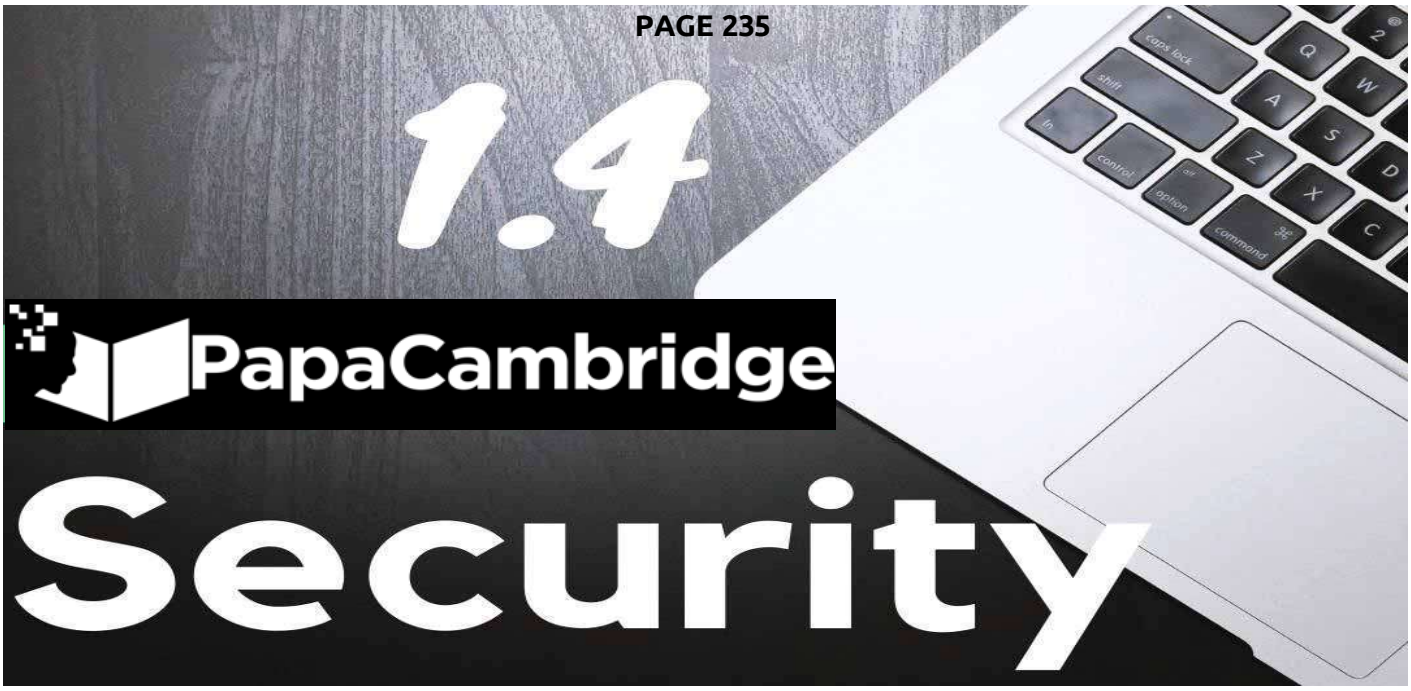


Chapter 4

1.4 Security aspects

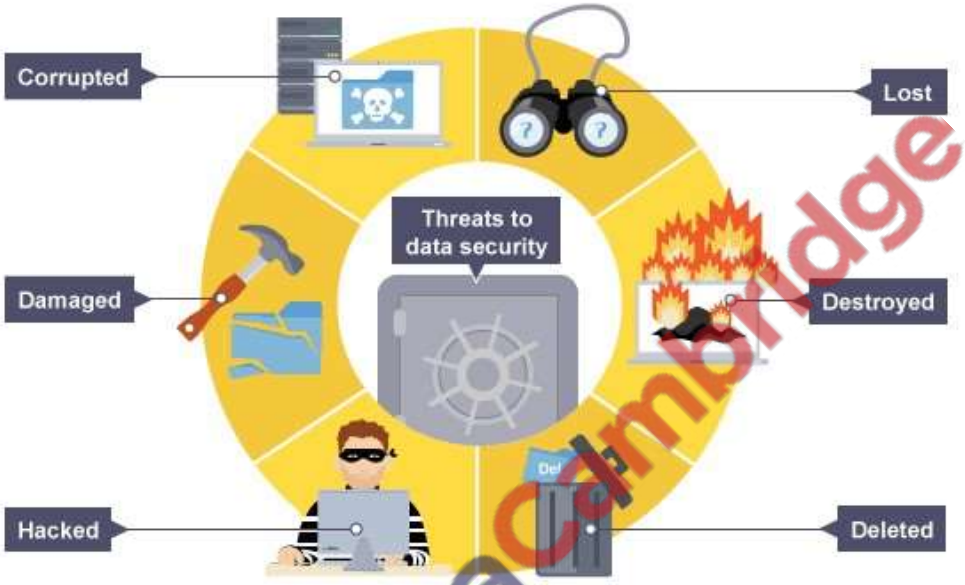
Learning Outcome	To Read	Have Read	To Revise	Have	Prepared
1.2.2: Security aspects					
Show understanding of the security aspects of using the Internet and understand what methods are available to help minimise the risks					
Show understanding of the Internet risks associated with malware, including viruses, spyware and hacking					
Explain how anti-virus and other protection software helps to protect the user from security risks (this also links into section 1.4 of the syllabus)					
1.4 Data integrity and security					
Show understanding of how data are kept safe when stored and transmitted, including: ○ use of passwords, both entered at a keyboard and biometric ○ use of firewalls, both software and hardware, including proxy servers ○ use of security protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) ○ use of symmetric encryption (plain text, cypher text and use of a key) showing understanding that increasing the length of a key increases the strength of the encryption					
Show understanding of the need to keep online systems safe from attacks including denial of service attacks, phishing, pharming					
Show understanding of the need to keep data safe from accidental damage, including corruption and human errors					
Show understanding of the need to keep data safe from malicious actions, including unauthorised viewing, deleting, copying and corruption					
Describe how the knowledge from 1.4.1, 1.4.2 and 1.4.3 can be applied to real-life scenarios including, for example, online banking, shopping					

Data Integrity and security

Data integrity refers to maintaining and assuring the accuracy and **consistency** of **data** over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves **data**.

Data security is about keeping data safe. Many individuals, small businesses and major companies rely heavily on their computer systems.

If the data on these computer systems is damaged, lost, or stolen, it can lead to disaster.



Loss of Data

Data loss is any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application. Data loss is also known as data leakage.

Reason	Pre-caution/ Method of Recovery
Accidental deletion	• Back-up • Saving on regular basis • Use of password so as unauthorised person can't delete data.
Hardware failure	• Back-up • UPS (to prevent loss of data from power failure) • Saving on regular basis • Parallel back-up hardware
Software failure	• Back-up • Saving on regular basis
Incorrect computer operation	• Back-up • Shut down computer properly • Remove external storage properly
Natural Disaster	• Back-up

PapaCambridge

Malware

Malware (malicious software) is specifically designed to disrupt or damage a computer system, such as a virus.

Malware, short for **malicious software**, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Computer virus is program or code that replicates itself and is designed to amend, delete or copy data and files on a user's computer without their consent.

Viruses are developed with intention to harm other computer data and programs.

Worms and Trojan horse are also types of virus.

A ***worm*** is a program that *actively* transmits itself over a network to infect other computers.

A **Trojan** horse is any program that invites the user to run it, concealing harmful or malicious code.

A **Trojan** horse is any program that invites the user to run it, concealing harmful or malicious code.

The **Trojan Horse** is a story from the Trojan War about the subterfuge that the Greeks used to enter the independent city of Troy and win the war. In the canonical version, after a fruitless 10-year siege, the Greeks constructed a huge wooden horse and hid a select force of men inside, including Odysseus. The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, ending the war.

PapaCambridge

Security Risk:

- Can delete or corrupt data and programs
- Can disrupt computer,
- Can cause computer stop working "hung"

Methods to remove risk

- Install antivirus
- Download data/programs only from authentic source
- Scan before opening email attachments or data from external source
- Install firewall

Spyware

Spyware/key-logging is software that monitors key presses on a user's keyboard, and relays the information back to the person who sent the software.

Spyware is a form of malware that hides on your device, monitors your activity, and steals sensitive information like bank details and passwords.

Security Risk:

- Transmits all data typed by user to the originator of spyware e.g. email/bank id and passwords, debit/credit card number etc.
- Can read cookies.
- Can change default web browser
- Can install other spyware

Methods to remove risk

- Install anti-spyware software
- Install firewall
- Use on-screen keyboard to type user id and passwords

War Driving

War driving is the act of searching for Wi-Fi wireless networks by a person usually in a moving vehicle, using a laptop or Smartphone. It is also known as **Access-Point Mapping.**

Security Risk

- Uses user's internet data/time
- May hack password and personal data

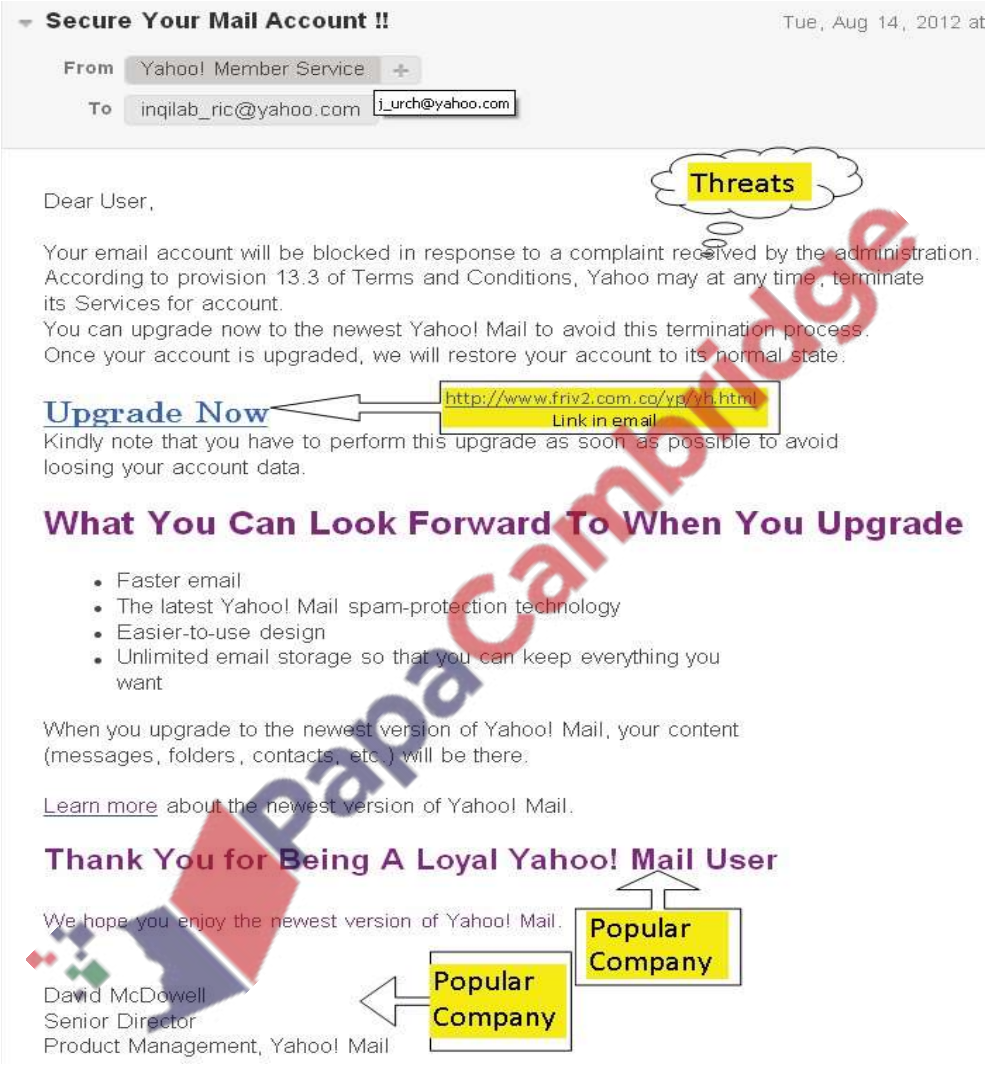
Methods to remove risk

- Use complex password
- Limit the number of users
- Firewall
- Use wired equivalent privacy (WEP) encryption

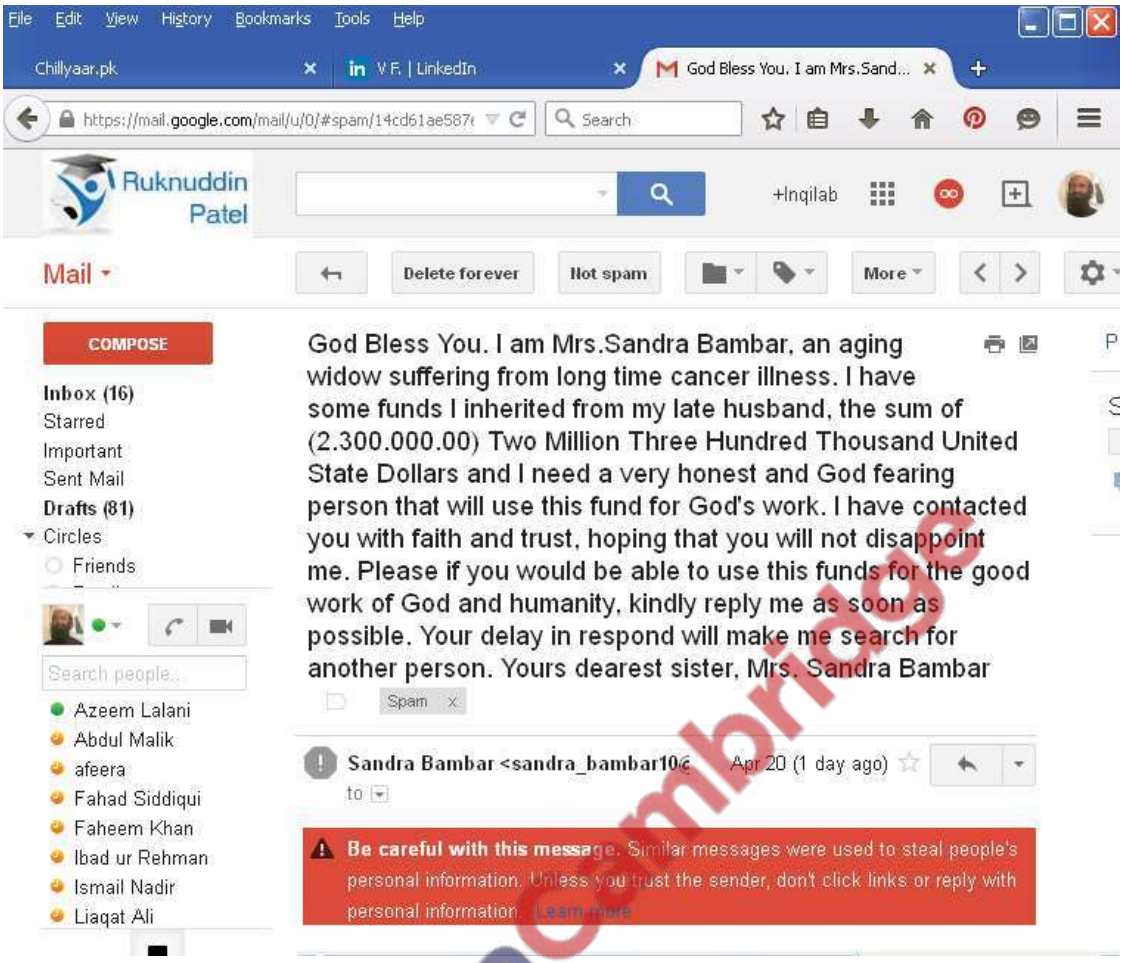
PapaCambridge

Phishing

Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.



PapaCambridge



Protection

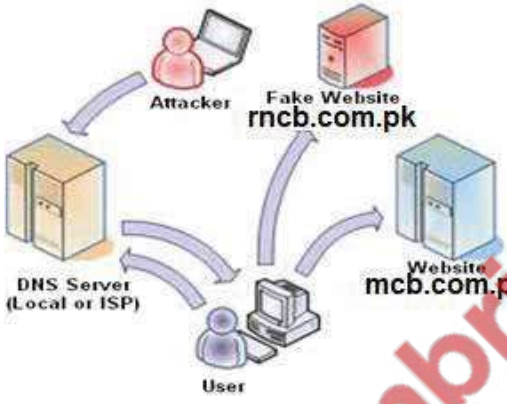
1. The most powerful weapon against phishing is common sense and the following rules that every user should oblige to.
2. If you are not a customer of the site delete the email immediately. Don´t click on the link or reply.
3. If you are a customer and you are not sure if the email is legit do one of the following:
   a) Contact the institute by phone or contact at the official website (do not use the email link of course) and ask if the mail is official.
   b) Instead of using the link provided open the website by typing in the official link there. The site should have news about the email on their starting page. (Most of the time). If not, use 3a to verify the email.

PapaCambridge

Pharming:

Pharming in Simple Steps:

- Hacker creates a fake website which appears similar to the original website.
- Hacker poisons the DNS servers thus domain names are resolved into fake IP address.
- User types the URL of the original website in the browser.
- The DNS server directs User to the fake website designed by hacker.
- User not knowing that it is a fake website, shares his confidential information such as login, password etc.
- Hacker gets the user confidential information from his fake web site and uses it to access the original website.
- Hacker exploits user's confidential information to his liking.



Protection

- Check the URL of any site that asks you to provide personal information. Make sure your session begins at the known authentic address of the site, with no additional characters appended to it.
- Use a trusted, legitimate Internet Service Provider. Rigorous security at the ISP level is your first line of defense against pharming.
- Check the certificate. It takes just a few seconds to tell if a site you land on is legitimate.
- Block suspicious Websites automatically

Identify fake website	
A	B

PapaCambridge

Hacking

Hacking is unauthorized use of computer and network resources.

The activity of breaking into a computer system to gain an unauthorized access is known as hacking. The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking.

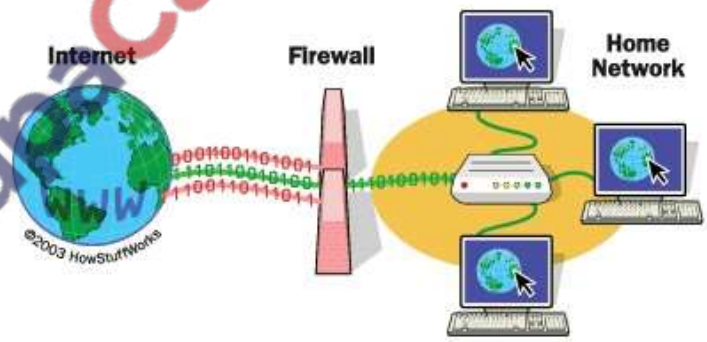
Protection:

- Make your passwords long and complicated, and with a good mix of letters and numbers, as well as utilizing case-sensitive letters. Don't use anything familiar, such as your birthday, your children's names or anything like that. If a hacker wants to attempt to break into your email accounts, at least make him work for it.
- Don't ever allow your browser to remember your passwords. True, it may be a bit of an inconvenience to enter your password every time you log in.
- Activate Firewall

Firewall

a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and un-trusted external network, such as the Internet.

Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.



Functions of firewall

- Monitors incoming and outgoing traffic
- checking whether incoming or outgoing data meets a given set of criteria
- if the data fails the criteria, the firewall will block the ‘traffic’ and give the user(or network manager) a warning that there may be a security issue
- logging all incoming and outgoing ‘traffic’ to allow later interrogation by the user(or network manager)

PapaCambridge

- criteria can be set to prevent access to certain undesirable sites; the firewall can keep a list of all undesirable IP addresses
- helping to prevent viruses or hackers entering the user's computer (or internal network)
- warning the user if some software on their system is trying to access an external data source (e.g. automatic software upgrade); the user is given the option of allowing it to go ahead or requesting that such access is denied.

It is often referred to in this case as a **GATEWAY**. Alternatively, the firewall can be software installed on a computer; in some cases, this is part of the operating system.

Limitations of firewall

- it cannot prevent individuals, on internal networks, using their own modems to bypass the firewall
- employee misconduct or carelessness cannot be controlled by firewalls (for example, control of passwords or use of accounts)
- users on stand-alone computers can chose to disable the firewall, leaving their computer open to harmful 'traffic' from the internet.
- All of these issues require management control or personal control (on a single computer) to ensure that the firewall is allowed to do its job effectively.

Proxy server

A proxy server is a dedicated computer system running on a network that acts as an intermediary between a client application, such as a Web browser, and a real server.

how proxy servers work:

When a proxy server receives a request for an Internet resource (such as a Web page), it looks in its local cache of previously pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

Functions of proxy servers include:

- allowing the internet 'traffic' to be filtered; they can block access to a website if necessary (similar type or reaction as a firewall)
- by using the feature known as a **CACHE**, they can speed up access to information from a website; when the website is first visited, the home page is stored on the proxy server; when the user next visits the website, it now goes through the proxy server cache instead, giving much faster access
- keeping the user's IP address secret – this clearly improves security
- acting as a firewall.

PapaCambridge

Security Certificates

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

https://www.us-cert.gov/ncas/tips/ST04-014

If an organization wants to have a secure web site that uses encryption, it needs to obtain a site, or host, certificate.

There are two elements:

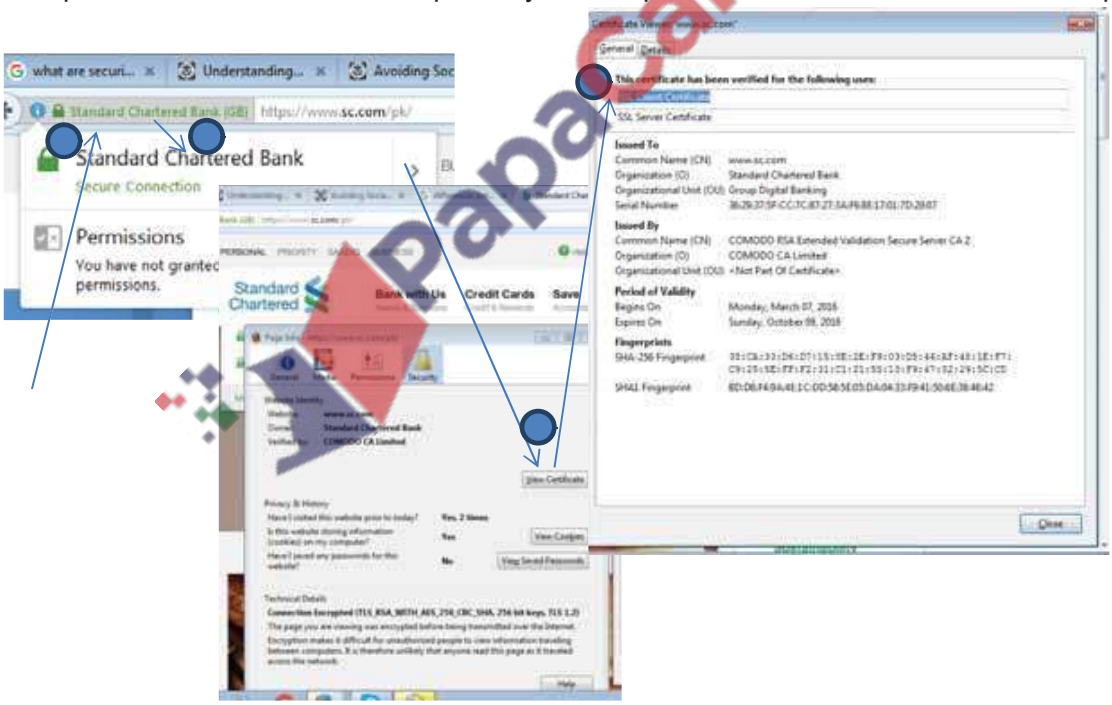
- a closed padlock,
- URL that begins with "https:" rather than "http:"

If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure web site, your browser will check the certificate for the following characteristics:

1. The web site address matches the address on the certificate
2. The certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority

If the browser senses a problem, it may present you with a dialog box that claims that there is an error with the site certificate.

If you have chosen not to trust the company who issued the certificate, or if the certificate has expired. You will usually be presented with the option to examine the certificate, after which you can accept the certificate forever, accept it only for that particular visit, or choose not to accept it.



Papa Cambridge

Security protocols

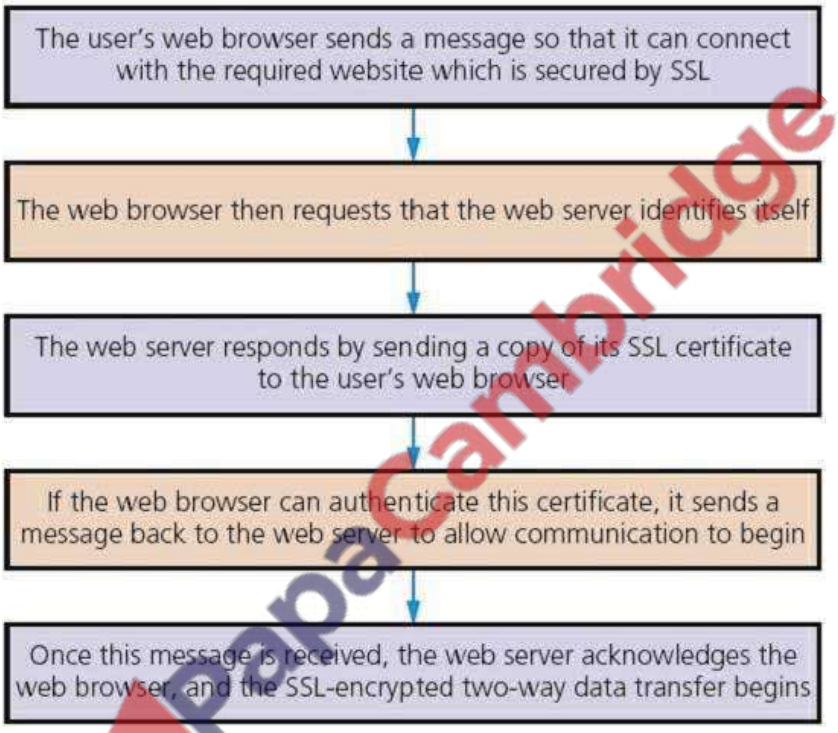
There are two forms of security protocols when using the internet:

• Secure Sockets Layer (SSL)

• Transport Layer Security (TLS).

SECURE SOCKETS LAYER (SSL) is a type of protocol (a set of rules used by computers to communicate with each other across a network). This allows data to be sent and received securely over the internet.

When a user logs onto a website, SSL encrypts the data – only the user's computer and the web server are able to make sense of what is being transmitted. A user will know if SSL is being applied when they see https or the small padlock in the status bar at the top of the screen. So what happens when a user wants to access a secure website and receive and send data to it?



TRANSPORT LAYER SECURITY (TLS) is similar to SSL but is a more recent security system. TLS is a form of protocol that ensures the security and privacy of data between devices and users when communicating over the internet. It is essentially designed to provide encryption, authentication and data integrity in a more effective way than its predecessor SSL.

When a website and client (user) communicate over the internet, TLS is designed to prevent a third party hacking into this communication causing problems with data security.

TLS is formed of two layers:

• Record protocol: this part of the communication can be used with or without encryption (it contains the data being transferred over the internet).

• handshake protocol: this permits the website and the client (user) to authenticate each other and to make use of encryption algorithms (a secure session between client and website is established).Only the most recent web browsers support both SSL and TLS which is why the older SSL is still used in many cases. But what are the main differences between SSL and TLS since they both effectively do the same thing?

• It is possible to extend TLS by adding new authentication methods.

• TLS can make use of **SESSION CACHING** which improves the overall performance 158 compared to SSL.

PapaCambridge

• TLS separates the handshaking process from the record protocol (layer) which holds all the data.

Session caching

When opening a TLS session, it requires a lot of computer time (due mainly to the complex encryption keys being used). The use of session caching can avoid the need to utilise so much computer time for each connection. TLS can either establish a new session or attempt to resume an existing session; using the latter can considerably boost system performance.

Summer 2015 P12

(a) State what is meant by the term SSL.

.....

.....

.....[1]

(b) The following stages take place when a user wishes to access a secure website.

Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you. [5]

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	
the web browser attempts to connect to a website which is secured by SSL	**1**
the web server sends the web browser a copy of its SSL certificate	
the web browser requests the web server to identify itself	
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	

Marking Scheme

(a) Any one from:
− Secure sockets layer − encrypts data being transmitted
− Use of https − use public and private keys [1]

(b) 1 mark for each number in the correct order, next to the correct stage.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	6
the web browser attempts to connect to a website which is secured by SSL	**1**
the web server sends the web browser a copy of its SSL certificate	3
the web browser requests the web server to identify itself	2
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	5
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	4

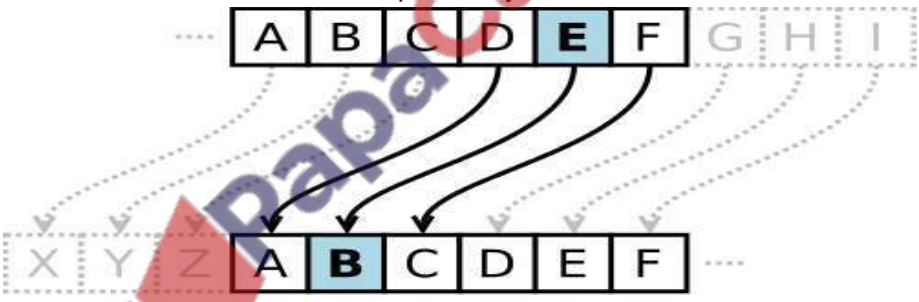
PapaCambridge

Caesar Cipher (Encryption)

The earliest known and simplest ciphers. The method is named after **Julius Caesar.**

It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.

For example, with a shift of -4, A would be replaced by X, D would become 4, and so on.



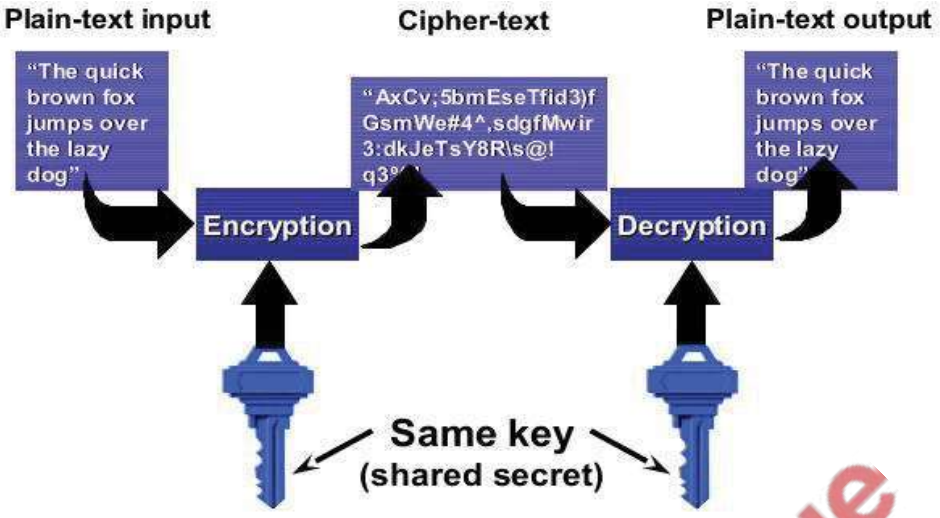
Encryption makes the data meaningless unless the recipient has the necessary decryption tools.

There are two types of encryption:

SYMMETRIC ENCRYPTION is a method of encryption in which one key is required to encrypt and decrypt the data.

ASYMMETRIC ENCRYPTION (also known as Public Key Encryption)is a method of encryption in which one key (public key) is required to encrypt and other key (private key) to decrypt the data.

Symmetric Encryption



KEY Distribution Problem:

In symmetric key encryption the sender has to supply the encryption key to the recipient. But this key could be hacked, which puts the security of the encrypted message at risk. This problem is known as key distribution problem.

ASYMMETRIC (PUBLIC KEY) ENCRYPTION

Public-key encryption is a cryptographic system that uses two keys

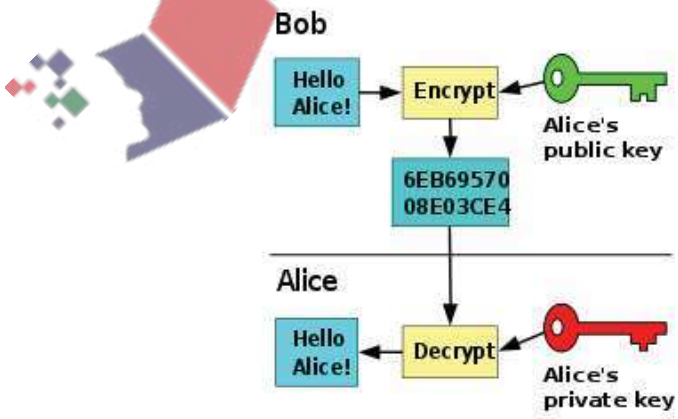
-- a *public key* known to everyone

-- and a *private* or *secret key* known only to the owner of the key.

If a message is encrypted by Public key it can only be decrypted by associated Private key.

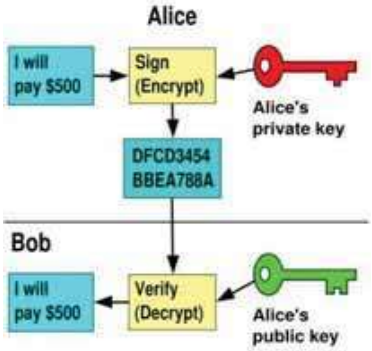
If a message is encrypted by private key it can only be decrypted by associated public key.

Example 1: *When Bob wants to send a secure message to Alice, he uses Alice's public key to encrypt the message. Alice then uses her private key to decrypt it.(To make not-understandable for others)*



PapaCambridge

Example 2: When Alice wants to ensure that the message is sent by her (to verify the sender and message is not altered, not to make message secure (not-understandable by others)),
she encrypts her message using her own private key.
Then the message is transmitted to Bob.
Bob decrypts the message using Alice's public key.
The decryption of message by Alice's public key confirms that this is Alice's message, and is without any alteration.



Example 3 (Exam style question): Bill, a manager of a company, sent an email with very sensitive information to a work colleague, Alison. However, Bill also accidentally sent it to everybody in the company.
Describe the method used that ensured only Alison was able to read the original contents of the email.

.....

.....

.....

.....

.....

.....[4]

Answer Key
Manager encrypts email using Alison's public key
Alison decrypts email his own private key

- Manager encrypts email
- using public key of colleague
- colleague decrypts email
- using his/her private key

Example 4 (Exam style question): Alexa sends an email to Beena. Explain how Beena can be sure that she has received a message that is authentic (not corrupted or tampered with) and that it came from Alexa.

.....

.....

.....

.....[2]

PapaCambridge

Answer Key

Alexa will encrypts her message using her own private key.
Beena will decrypts the message using Alexa's public key.
If message is decrypted by Alexa's public key, it shows that message is authentic (sent by Alexa and not tempered).

Digital certificates

Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible for issuing digital certificates.
It contains Name of certification authority, Public key of company and Expiry date.
The method of issuing a digital certificate is as follows:

1. A user starts an application for a digital certificate using their computer. On this computer a key pair is generated. This key pair consists of a public key and an associated private key.
2. The user submits the application to the CA. The generated public key and other application data are sent.
3. The key and data are encrypted using the CA's public key before sending to CA.
4. The CA creates a digital document containing all necessary data items and signs it using the CA's private key.
5. The CA sends the digital certificate to the individual.

HASHING ALGORITHM

The hashing algorithm takes a message or a key and translates it into a string of characters usually shown in hexadecimals essentially makes the message or key almost impossible to read 'meaningless' text. This is also known as message digest.

PapaCambridge

Authentication

Authentication means the receiver is certain who sent the cipher text.

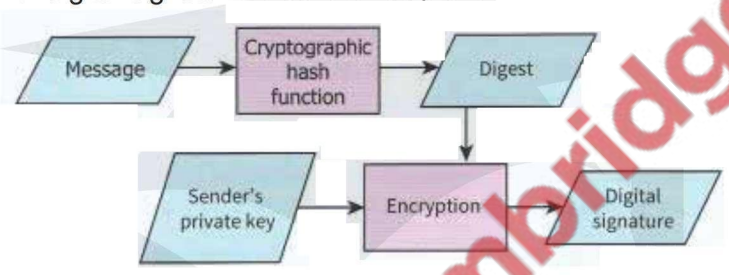
For authentication passwords, digital certificates and digital signatures are used/

Digital signature

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit.

How digital signature works

- Sender applies HASH algorithm on the message.
- Message digest is created.
- Sender encrypts the message digest using his own private key. This encrypted message digest is called Digital Signature.
- Plain text along with digital signature is sent to recipient.



Receiver receives both plain message and digital signature

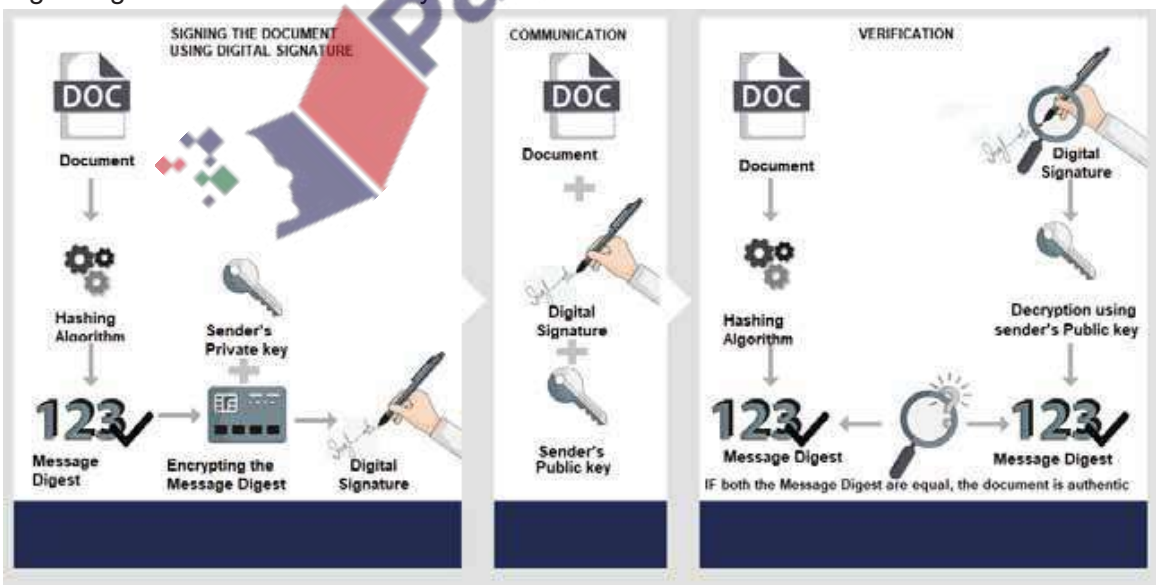
Receiver applies the same HASH algorithm on message and obtains message digest

Receiver then encrypts the receiving digital signature using sender's public key to obtain sender's message digest.

Receiver compares his own generated message digest with the sender's message digest.

If both matches then message is sent from the intended source.

Digital signature is used to identify the sender.



PapaCambridge

DENIAL OF SERVICE ATTACKS

A denial of service attack (DoS) is an attempt at preventing users from accessing part of a network, notably an internet server.

The attacker may be able to prevent a user from:

- accessing their emails
- accessing websites/web pages
- accessing online services (such as banking).

One method of attack is to flood the network with useless traffic.

When a user types in or clicks on a URL of a website (using their web browser), a request is sent to the internet server which contains the website or web page.

Obviously, the server can only handle a finite number of requests. So if it becomes overloaded by an attacker sending out thousands of requests, it won't be able to service the user's legitimate request. This is effectively a denial of service.

PapaCambridge

Specimen Paper 2015

Q1) In a simple symmetric encryption system, each letter of the alphabet is substituted with another.

The plain text message:

The Quick brown Fox jumps over a lazy dog.

becomes the cypher text message:

Zag towns jumpy Dmh coilv mwgu f bfke rmq

(a) (i) Convert these words to cypher text.

Computer Science

.....

..... [2]

(ii) Decode this cypher text message.

LFD Naflzgu

.....

..... [2]

(b) Both the person who sends the message and the person who receives it need to know what the substitution key is, and they need to keep this secret. A copy of the substitution key has been sent using SSL transmission.

Explain why this keeps the copy of the key secret during transmission.

.....

..... [2]

(d) A user downloads software from the Internet.

(i) State what should be part of the download to provide proof that the software is authentic?

.....[1]

(ii) Describe the process for ensuring that the software is both authentic and has not been altered.

.....

.....

.....

.....

.....

.....

.....[4]

PapaCambridge

(d)	**(i)**	digital signature
	(ii)	• software is put through hashing algorithm • hash total is encrypted with private key (digital signature) • software + encrypted hash / digital signature are sent • receiver is in possession of sender's public key • the received hash total / digital signature is decrypted with public key (SH) • the receiver hashes received software (RH) • If SH matches RH then software is authentic and has not been altered

Q 3) Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible for issuing digital certificates.

(a) Name **three** data items present in a digital certificate.

1 .....

2 .....

3 .....[3]

(b) The method of issuing a digital certificate is as follows:

1 A user starts an application for a digital certificate using their computer. On this computer a key pair is generated. This key pair consists of a public key and an associated private key.

2 The user submits the application to the CA. The generated .....**(i)** .....key and other application data are sent. The key and data are encrypted using the CA's .....**(ii)** .....key.
3 The CA creates a digital document containing all necessary data items and signs it using the CA's .....**(iii)** .....key.
4 The CA sends the digital certificate to the individual.
In the above method there are three missing words. Each missing word is either 'public' or 'private'.

State the correct word. Justify your choice.

(i) .....

Justification .....

.....[2]

(ii) .....

Justification .....

.....[2]

(iii) .....

Justification .....

.....[2]

(c) Alexa sends an email to Beena.

Alexa's email program:

• produces a message digest (hash)

• uses Alexa's private key to encrypt the message digest

• adds the encrypted message digest to the plain text of her message

• encrypts the whole message with Beena's public key

• sends the encrypted message with a copy of Alexa's digital certificate

Beena's email program decrypts the encrypted message using her private key.

(i) State the name given to the encrypted message digest.

.....[1]

PapaCambridge

(ii) Explain how Beena can be sure that she has received a message that is authentic (not corrupted or tampered with) and that it came from Alexa.

.....

.....

.....

.....[2]

(iii) Name **two** uses where encrypted message digests are advisable.

1 .....

2 .....[2]

(a)	Examples: Serial number Certificate Authority that issued certificate CA digital signature Name of company/organisation/individual/subject/owner owning Certificate 'Subject' public key Period during which Certificate is valid // some relevant date
(b) (i)	Public The individual keeps their private key private // the public key can be known by others (the public)
(ii)	Public The individual does not know the private key of the CA // the individual only knows the public key of the CA // only the CA can decrypt the packaged information
(iii)	Private 'Only' the CA's public key will allow decryption of the Certificate // proving the certificate was issued by the CA
(c) (i)	Digital signature
(ii)	Alexa's digital certificate (Includes) Alexa's public key Used to hash message received // produce message digest Generated hash compared to digital signature
(iii)	Examples: Financial transaction Legal document Software distribution

PapaCambridge

Q 4 a) The table below gives descriptions of three types of malware.

Description	Term
Malware that attaches itself to another program.	
Malware that redirects the web browser to a fake website.	
Email that encourages the receiver to access a website and give their banking details.	

Complete the table by adding the correct terms. [3]

(b) Ben wants to send a highly confidential email to Mariah so that only she can read it. Plain text and cipher text will be used in this communication.

(i) Explain the terms plain text and cipher text.

Plain text .....

.....

Cipher text .....

..... [2]

(ii) Explain how the use of asymmetric key cryptography ensures that only Mariah can read the email.

.....

.....

.....

.....

.....

.....

..... [4]

(a)

Description	*Term*
Malware which attaches itself to another program.	*VIRUS*
Malware designed to redirect the web browser to a fake website.	*PHARMING*
Email that encourages the receiver to access a website and give their banking details.	*PHISHING*

(b) (i) *Plain text is the original text*
Cipher text is the encrypted version of the plain text
(ii) *Asymmetric keys means that the key used to encrypt (public key) is different from the key used to decrypt (private key)*
Ben acquires Mariah's public key
Ben encrypts email …
using Mariah's public key
Ben sends encrypted email to Mariah
Mariah decrypts email …
Using her private key

PapaCambridge

Q 5) Anna has to send an email to Bob containing confidential information. Bob and Anna have never sent emails to each other before.
Bob and Anna both have public and private keys.
The first step is for Anna to request that Bob sends her one of his keys.

(i) State the key that Bob sends. .....[1]

(ii) Explain how Anna can be sure that it is Bob who has sent the key.

.....

.....

.....[2]

(iii) Anna has received the key from Bob.

The following incomplete table shows the sequence of actions between Anna and Bob to communicate the confidential information.

Complete the table. [4]

The person performing the action	What that person does
Anna	Requests Bob's <answer to **part (c)(i)**> key.
Bob	.....
Anna	.....
Anna	Sends the email to Bob.
Bob	.....

PapaCambridge

(i) public

(ii) Bob sends his digital certificate
Digital certificate contains Bob's public key
Successful decryption of certificate using CA's public key provides legitimacy
1 mark for any valid point – max 2

(iii)

The person performing the action	What that person does
Anna	Requests Bob's **public** key.
Bob	Sends Anna his public key.
Anna	Encrypts email with Bob's public key.
Anna	Sends the email to Bob.
Bob	Decrypts email. Using his private key.

Topical Questions from Past Papers

Winter 2014 P12

The following **five** statements about Internet security are incomplete:

(i) Illegal access to a computer system is known as < - - - - - - - - - >.

(ii) < - - - - - - - - - > are programs that self-replicate (copy themselves) and are designed to disrupt computer systems.

(iii) < - - - - - - - - -> is where a user is sent legitimate-looking emails; as soon as the email is opened and the recipient clicks on the embedded link, they are sent to a fake website.

(iv) Software that monitors key presses on a user's keyboard, and relays the information back to the person who sent the software, is known as < - - - - -- - - - >.

(v) < - - - - - - - - - > is malicious code or software installed on the hard drive of a user's computer or on a web server; the code or software will re-direct the user to a fake website without their knowledge.

Complete the **five** statements using words from the following list:

• Cookies• hacking • pharming • phishing• spam • spyware• viruses • web browsers

Summer 2014

The diagram below shows a number of descriptions and terms used in computer security. By drawing arrows, connect the correct description to the computer security term.

Program installed on a PC to gather data about the user. It monitors every key press and relays the data back to the home base.	Cookies
Junk (unsolicited) electronic mail advertising products and services sent to a general mailing list.	Phishing
Sending an email that claims to be from a legitimate company; the recipient is then directed to a bogus website where their personal details will be collected.	Pharming
Malicious code installed on a PC or on a server. This code directs users to a fraudulent website without their knowledge.	Spyware
Act of locating and possibly exploiting a wireless network by touring an area. This requires a laptop with relevant software and an antenna.	Spam
Information that a website stores about a user on the user's hard disk; this enables the website to remember details about the user when they next visit the website.	War-driving

PapaCambridge

Q3) Five security or data loss issues are shown on the left-hand side.
Five possible methods of data recovery or protection are shown on the right.
Draw a line to match each definition/description of Issues to the most appropriate Methods of Data Recovery.

Issues	Methods of Data Recovery
Data loss caused by hard disk head crash	Anti-spyware software
Hacking into files and changing or deleting data	Anti-virus software
Introduction of software that self-replicates and can cause data loss	Back-up files
Reading of illegally accessed documents	Encryption
Software that logs/records all key presses on your computer without you knowing	Passwords and a firewall

PapaCambridge

Winter 2014 P13

3 (a) Felipe wrote down the following three statements.
In **each** case, indicate whether the statement is true or false and give a reason for your choice.
"Encrypting data prevents it from being hacked"
TRUE/FALSE .....
Reason .....
.....
.....
"backing up data removes the risk of the data being infected by viruses"
TRUE/FALSE .....
Reason.....
.....
.....

"Wireless (Wi-Fi) networks are less secure than hard-wired systems"
TRUE/FALSE .....
Reason .....
.....
.....[3]

(b) Felipe uses Internet banking. When he logs on, the website asks for the 1st, 4th and 8th characters in his password. He selects the characters from drop-down boxes.

(i) State why drop-down boxes are used.
.....
.....[1]

(ii) Felipe is also asked to confirm the last date and time when he logged onto the website. State why he is asked to confirm this.
.....
.....[1]

(iii) When Felipe wishes to return to a previous page on this website, he clicks on the **View My Account** option rather than using the browser arrows. If he uses the browser arrows, he is logged out of the website.
Give a reason why the website does this.
.....
.....
.....[1]

a) FALSE – encryption only stops data being read / making sense (but does not prevent the act of hacking)
FALSE – data when backed up could still have the virus attached to it
– when the backed up data is re-loaded at a later date, the virus could be loaded again into the system together with the stored data
TRUE – tapping into a Wi-Fi network is relatively easy (even when the network is protected by passwords)
(b) (i) drop down boxes help defeat spyware / key logging software [1]
(ii) – to ensure that it was in fact Felipe who logged on last time [1]
– an additional authentication check
(iii) in case it is not Felipe who attempts to access the account[1]

PapaCambridge

Summer 2014

Q2) An encryption system gives each letter of the alphabet a value:
A = 1, B = 2, C = 3, …… , Y = 25, Z = 26.
Each letter is stored in a 12-bit binary register. The letter "S" (19th letter) is stored as:

2048	1024	512	256	128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	**1**	**0**	**0**	**1**	**1**

A 4-bit register is used to store the encryption key. This register shows how many places the bits are shifted to the left in the 12-bit register when it is encrypted. So,

8	4	2	1
0	**1**	**0**	**1**

means each bit in the 12-bit register is shifted 5 places to the left and the register now becomes:

2048	1024	512	256	128	64	32	16	8	4	2	1
0	0	**1**	**0**	**0**	**1**	**1**	0	0	0	0	0

Therefore, the letter "S" would be transmitted with the 4-bit register and the 12-bit register as follows:

0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	0

(a) "W" is the 23rd letter of the alphabet.
(i) Show how this letter would be stored in the 12-bit register before encryption:

(ii) The 4-bit register contains the following value:

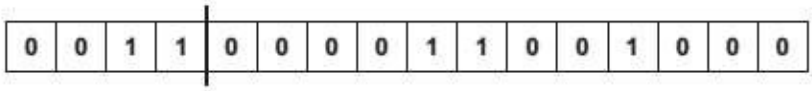
8	4	2	1
0	**1**	**1**	**0**

Show how the letter **"W"** is now stored in the 12-bit register in encrypted form:

[2]

PapaCambridge

(b) Find which letter of the alphabet has been encrypted here. (Show all your working.)



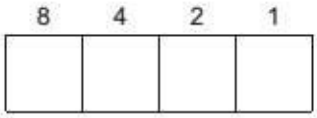
.....

.....

.....

..... [2]

(c) **(i)** What is the largest encryption key that can be stored in the 4-bit register?



(ii) Convert this into denary (base 10).

.....

(iii) If this encryption key were used, what problem would it cause?

.....

..... [3]

PapaCambridge

Winter 2010

Q3) (a) What is meant by a virus?

.....

.....

..... [2]

(b) What is meant by encryption?

.....

.....

..... [2]

(c) (i) A student wrote “I would make backup copies of my data to guard against viruses”.

Why is the student’s statement not necessarily true?

.....

.....

..... [2]

(ii) The same student also wrote “Encryption would stop a hacker accessing the data in my computer files”.

Why is the student’s statement incorrect?

.....

.....

..... [2]

Summer 2010

Q4) A company has set up an Internet website to sell their electrical goods online.

(a) Give two features you would expect to see on the website.

.....

.....

..... [2]

(b) Payments for goods can be made by credit/debit cards. Data from the cards is encrypted.

(i) What is encryption?

(ii) Why is data encrypted?

.....

.....

..... [2]

(c) Apart from credit card fraud, people have other fears about buying from the Internet.

Describe one of these fears.

.....

.....

..... [2]

Q5) The student is interested in how simple encryption could be applied to a text message. One of the simplest forms of encryption is a method of ‘substitution’ where each character has a unique substitute character.

The student uses this method with the following character substitutions:

Message character	A	B	C	D	E	F	G	H	I	J	K	L	M
Substitute character	P	L	F	N	O	C	Q	U	D	Z	V	G	I

Message character	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Substitute character	X	M	W	J	B	K	E	A	H	S	Y	R	T

Assume all messages are made up from the upper-case characters only.

Show the string after the message ATSEVEN is encrypted.

.....

.....

..... [2]

PapaCambridge

Q6) The encryption of data is widely used in computing.

(a) One application is online banking.

State two other applications where encryption is used.

Describe the reason for encrypting the data for each application.

Application 1.....

Reason.....

Application 2.....

Reason ..... [4]

(b) Explain the terms plain text and cipher text.

Plain text .....

Cipher text .....[2]

(c) Symmetric encryption uses a single key.

Explain how a message is encrypted and decrypted using symmetric encryption.

.....

.....

..... [2]

(d) Authorisation and authentication are processes designed to protect the computer system and data.

Give one technique used for each.

Authorisation .....

Authentication ..... [2]

PapaCambridge

Winter 2014 P13

1 Give, with reasons, **three** safety issues associated with the use of computers in the office.

1. .....
2. .....
3. .....[3]

Safety issues e.g.:

– electrocution from bare wires or spilling liquids on live equipment

– trip hazard due to trailing wires

– risk of heavy equipment falling from inadequate desks

– risk of fire if insufficient equipment ventilation or overloaded wall sockets [3]

Candidate Example Response

Question 5

Example Candidate Response – high	Examiner Comments
5 A music company wants to send a new music file to many radio stations. It will send the music file the day before the release date so that the radio stations can store the file ready for release. The music company does not want the radio stations to be able to open the music file until 09:00 on the release date. Identify **two** security measures **and** describe how each measure can be used to make sure the music file cannot be opened until the release date. Security measure 1 password Description The password will be sent out at 9AM (1) so people can't open it before. A password uses a combination of letters and numbers Security measure 2 Encryption Description Scramble up the data in the music using an encryption algorithm. The music company will ~~solve~~ send the encryption key at 9AM [4]	(1) It would be beneficial for candidates to state that this was 9am on the release date. **Total mark awarded = 4 out of 4**

How the candidate could have improved their answer

The candidate gave just enough of a reference to releasing the password and encryption key on the release data as they stated they could have been released at 9am. It would have been beneficial for the candidate to have stated that this was 9am on the release date.

Example Candidate Response – middle	Examiner Comments
5 A music company wants to send a new music file to many radio stations. It will send the music file the day before the release date so that the radio stations can store the file ready for release. The music company does not want the radio stations to be able to open the music file until 09:00 on the release date. Identify **two** security measures **and** describe how each measure can be used to make sure the music file cannot be opened until the release date. Security measure 1 The file can be secured by a password Description If the file is secured by a password other people won't be able to access it and the password can be given out sometime before the release (1) Security measure 2 The file can be encrypted ~~and then~~ Description The encrypted file could be de-crypted few moments before the release (2) [4]	(1) This timescale is too vague. The system will only work if the password is given out on the release date. (2) The candidate doesn't state how the file will be decrypted. **Total mark awarded = 2 out of 4**

How the candidate could have improved their answer

The candidate hasn't been specific enough in referring to when the password and decryption key could be given to the company. They stated that it could be some time before the release date, but the system would not work unless the password was given out on the release date.

PapaCambridge

Example Candidate Response – low	Examiner Comments
5 A music company wants to send a new music file to many radio stations. It will send the music file the day before the release date so that the radio stations can store the file ready for release. The music company does not want the radio stations to be able to open the music file until 09:00 on the release date. Identify **two** security measures **and** describe how each measure can be used to make sure the music file cannot be opened until the release date. Security measure 1 Pass code / Fingure scanner (1) Description If some has to open he or she use to open their fingure or enter code if it would be wrong an alarm would be start sounding Security measure 2 Timmer (2) Description Without the given time it would not be open or if some one tries to open it would give bug into his or her computer [4]	(1) The candidate is awarded a mark for passcode in reference to password. (2) The system described is not a viable system in the given scenario. **Total mark awarded = 1 out of 4**

How the candidate could have improved their answer

- The candidate was given the benefit of the doubt for the reference to the use of a passcode in place of a password. The remainder of the answer had no reference to sending out the password at the release date.
- The second system offered by the candidate was not a system that would be viable in this scenario.

Common mistakes candidates made in this question

Many candidates gave viable systems, such as password and encryption. Some candidates were not specific in how that system would work and when the password or encryption key would be sent to the company.

Example Candidate Response – low	Examiner Comments
6 Priya creates a website to sell her old comic books and superhero figures. (a) She uses HTML to create her website. The HTML she produces has both structure and presentation. Explain what is meant by HTML **structure** and **presentation**, include an **example** of each. Structure It is the lay-out of the program (1) ~~like colour of Heading of the~~ ~~and the colours of the website~~ like colours (2) Heading of website. Presentation It is the content which is writen in the program or the body of the program like style (3) and content writen in the program [4]	(1) The candidate cannot be awarded the mark for layout as they state it is the layout of the program. This is incorrect as it is the layout of the web page. (2) The first example given is an example of presentation and not structure. (3) The candidate is given the benefit of the doubt for their response that it is the style of the content. A mark is awarded for this. **Total mark awarded = 1 out of 4**

How the candidate could have improved their answer

- The candidate demonstrated misunderstanding; they thought the structure and presentation referred to the code for the web page, rather than the content of the actual webpage.
- The candidate also provided an incorrect example of structure. They should have stated an example such as where a paragraph of text was placed.

Common mistakes candidates made in this question

Candidates often used vague terms to describe each section, such as design, or the way the page looked. Both descriptions could have applied to either structure or presentation and not specifically to either one. Formatting could have been used for presentation, as this could specifically have referred to the formatting of text, which was the font, style, or colour of the text.

PapaCambridge

Question 6b

Example Candidate Response – high

(b) Priya uses cookies in her website.

Five statements are given about cookies.

Tick (✓) to show if the statement is **True** or **False**.

Statement	True (✓)	False (✓)
Cookies can be used to store a customer's credit card details	✓	
Cookies can be used to track the items a customer has viewed on a website	✓	
Cookies will corrupt the data on a customer's computer		✓
Cookies are downloaded onto a customer's computer	✓	
Cookies can be deleted from a customer's computer	✓	

[5]

Examiner Comments

1 The candidate provides five correct ticks.

Total mark awarded = 5 out of 5

How the candidate could have improved their answer

The candidate provided a model answer that could not be improved.

Example Candidate Response – middle

(b) Priya uses cookies in her website.

Five statements are given about cookies.

Tick (✓) to show if the statement is **True** or **False**.

Statement	True (✓)	False (✓)
Cookies can be used to store a customer's credit card details	✓	
Cookies can be used to track the items a customer has viewed on a website	✓	
Cookies will corrupt the data on a customer's computer		✓
Cookies are downloaded onto a customer's computer		✓
Cookies can be deleted from a customer's computer	✓	

[5]

Examiner Comments

1 The candidate provides an incorrect response for statement four.

Total mark awarded = 4 out of 5

How the candidate could have improved their answer

The candidate showed some understanding of the fact that cookies could be deleted from a computer. They needed to extend that understanding to have known that the cookies were downloaded onto the computer too, so that they could be deleted.

Example Candidate Response – low

(b) Priya uses cookies in her website.

Five statements are given about cookies.

Tick (✓) to show if the statement is **True** or **False**.

Statement	True (✓)	False (✓)
Cookies can be used to store a customer's credit card details	✓	
Cookies can be used to track the items a customer has viewed on a website	✓	
Cookies will corrupt the data on a customer's computer		✓
Cookies are downloaded onto a customer's computer		✓
Cookies can be deleted from a customer's computer		✓

[5]

Examiner Comments

1 The candidate shows limited understanding of the fact that cookies can be downloaded on to, and deleted from, a user's computer.

Total mark awarded = 3 out of 5

How the candidate could have improved their answer

The candidate didn't understand that cookies could be downloaded to a user's computer and therefore deleted from it as well.

Common mistakes candidates made in this question

Candidates appeared to understand how cookies could be used to store details and track browsing habits. It would have been beneficial for candidates to also have known how cookies were stored and whether they could be deleted.

PapaCambridge

Question 6ei

Example Candidate Response – high	Examiner Comments
(e) Priya is concerned about a denial of service attack (DoS) occurring on her webserver. (i) Explain what is meant by a denial of service attack. When a device (hacker) sends a large amount of requests to a webserver 1 at one time 2 over loading the web serve and potentially leading to the server crashing 3 or being extremely slow for other users trying to access the webserver 4 [4]	1 The first mark is awarded for the large number of requests sent. 2 The second mark is awarded for stating the requests are all sent at the same time. 3 The third mark is awarded for stating the server crashes. This is an acceptable way of stating it will timeout. 4 If the candidate is more specific and says that this denies people access, then a fourth mark could be awarded. **Total mark awarded = 3 out of 4**

How the candidate could have improved their answer

The candidate stated that the DoS would make the server extremely slow for others. If they had been more specific and said that this would have denied people access, then a fourth mark could have been awarded.

Example Candidate Response – middle	Examiner Comments
(e) Priya is concerned about a denial of service attack (DoS) occurring on her webserver. (i) Explain what is meant by a denial of service attack. It's when a user cannot access a part of the network, possibly an internet server 1 as can prevent the user from accessing their e-mails or online services. Via backing 2 the attacker can send millions of requests 3 which will clog up the process this prevents the website from serving the user's legitimate request 4 The ISP provides every webserver a specific data quota and can only handle a finite number of requests 5 the attacker can prevent other users from accessing the website [4]	1 The candidate needs to be more specific in their reference to the location of the attack. An Internet server is too vague and it needs to be a web server. 2 A mark is awarded for naming specific services that the user may be prevented from accessing. 3 A mark is awarded for reference to a high number of requests sent. 4 This repeats a mark of one gained earlier. 5 The candidate almost gains a mark here, as they state the server can only handle a finite number of requests, but they are missing the detail that this is why the server will struggle to handle the number of requests. **Total mark awarded = 2 out of 4**

How the candidate could have improved their answer

- The reference to the location of the attack being on an Internet server was too vague; it needed to be a web server. The candidate needed to be more specific in their reference to the location of the attack.
- In their last sentence, had the candidate expanded this to say that this was why the server would struggle with the number of requests, another mark could have been awarded.

PapaCambridge

Example Candidate Response – low	Examiner Comments
(e) Priya is concerned about a denial of service attack (DoS) occurring on her webserver. (i) Explain what is meant by a denial of service attack. it is occured when someone tries to hack your page or tries to produce virus in the page so that it couldnot be worked so with the help of Dos when ever it indicates that someone is hacking it gave the sign to the admin of page to prtech it or it is change on his page. 1 [4]	1 The candidate shows little understanding of a DoS attack. The candidate understands it to involve hacking and the use of viruses. **Total mark awarded = 0 out of 4**

How the candidate could have improved their answer

The candidate understood a DoS attack to involve hacking and viruses. It would have been beneficial for the candidate to have understood that there were other Internet risks not involved in this process.

Common mistakes candidates made in this question

This was a technical process that candidates had been asked to describe, so accuracy was important. A common error made by candidates was not providing enough notion that it was a high number of requests that were sent. Some candidates stated several requests or some requests.

Question 6eii

Example Candidate Response – high	Examiner Comments
(ii) Give **one** security device that can be used to help prevent a denial of service attack. Firewall 1 [1]	1 This is a suitable method of prevention. **Total mark awarded = 1 out of 1**

How the candidate could have improved their answer

The candidate provided a suitable security device and could not have improved their answer.

Example Candidate Response – middle	Examiner Comments
(ii) Give **one** security device that can be used to help prevent a denial of service attack. By having a long password to open it like [1]	1 This method of prevention will not stop a DoS. Also, it is not a device. **Total mark awarded = 0 out of 1**

How the candidate could have improved their answer

The candidate provided a method of security, but it would not have been suitable for a DoS attack. Also, it was not a device and the question had asked the candidate to provide a security device.

Example Candidate Response – low	Examiner Comments
(ii) Give **one** security device that can be used to help prevent a denial of service attack. IP Address 1 [1]	1 This is not a method of prevention. **Total mark awarded = 0 out of 1**

How the candidate could have improved their answer

The candidate gave an aspect that might have been involved in a DoS attack, but it was not a device that could gave helped prevent one. The candidate could have given firewall or proxy server.

Common mistakes candidates made in this question

Some candidates provided methods of security, but these were not security devices. The question specifically asked for a security device.

PapaCambridge

Example candidate response – high

1 (a) Four statements about cookies are shown in the table below.

Study each statement.

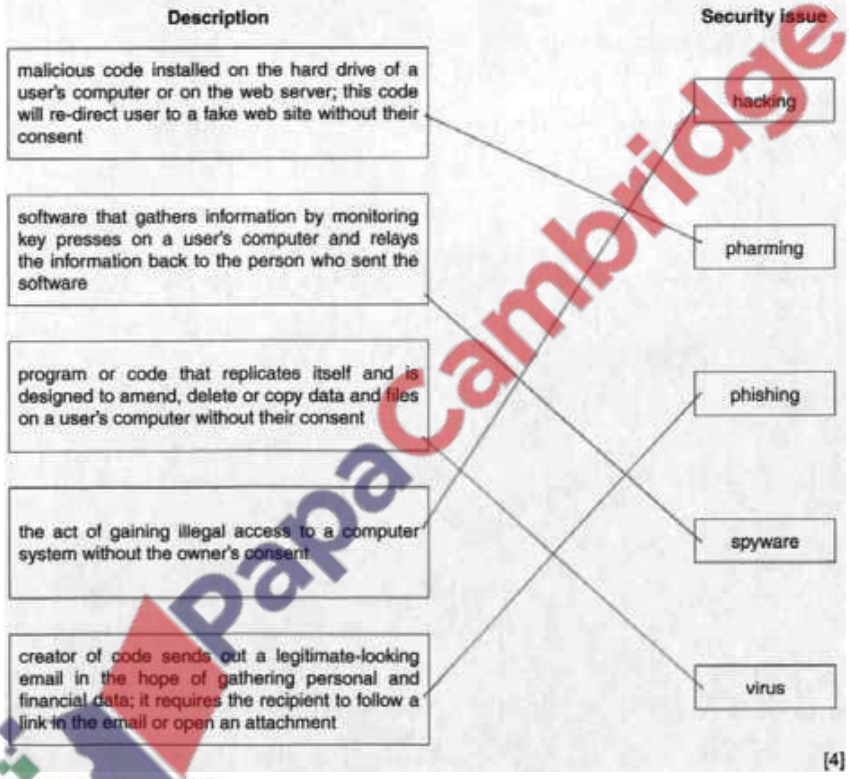
Tick (✓) to show whether the statement is true or false.

Statement	True	False
they are a form of spyware		✓
they are used only in advertising		✓
they are used to track browser use	✓	
they act in the same way as a virus		✓

[4]

(b) Five descriptions and five security issues are shown below.

Draw a line to connect each description to the correct security issue.



[4]

PapaCambridge

Examiner comment – high

This candidate was able to recognise which statements were true and false about cookies. No incorrect answers were given.

This candidate was able to match all the correct terms to the correct definitions. No terms were incorrectly matched.

Marks awarded for **1(a)** = 4 out of 4
Marks awarded for **1(b)** = 4 out of 4

Total mark awarded= 8 out of 8

Example candidate response – middle

1 (a) Four statements about cookies are shown in the table below.

Study each statement.

Tick (✓) to show whether the statement is true or false.

Statement	True	False
they are a form of spyware		✗
they are used only in advertising	✓	
they are used to track browser use	✓	
they act in the same way as a virus		✗

[4]

(b) Five descriptions and five security issues are shown below.

Draw a line to connect each description to the correct security issue.

Description	Security issue
malicious code installed on the hard drive of a user's computer or on the web server; this code will re-direct user to a fake web site without their consent	hacking
software that gathers information by monitoring key presses on a user's computer and relays the information back to the person who sent the software	pharming
program or code that replicates itself and is designed to amend, delete or copy data and files on a user's computer without their consent	phishing
the act of gaining illegal access to a computer system without the owner's consent	spyware
creator of code sends out a legitimate-looking email in the hope of gathering personal and financial data; it requires the recipient to follow a link in the email or open an attachment	virus

[4]

PapaCambridge

Examiner comment – middle

This candidate has made a common error in their answer to **1(a)**. It is a common error to think that cookies are only used in advertising. They can be used for many other reasons, such as retaining preferences for websites.

This candidate also managed to match all the correct terms to the definitions.

Marks awarded for **1(a)** = 3 out of 4
Marks awarded for **1(b)** = 4 out of 4

Total mark awarded = 7 out of 8

Example candidate response – low

1 (a) Four statements about cookies are shown in the table below.

Study each statement.

Tick (✓) to show whether the statement is true or false.

Statement	True	False
they are a form of spyware		✓
they are used only in advertising	✓	
they are used to track browser use	✓	
they act in the same way as a virus	✓	

[4]

(b) Five descriptions and five security issues are shown below.

Draw a line to connect each description to the correct security issue.

Description	Security issue
malicious code installed on the hard drive of a user's computer or on the web server; this code will re-direct user to a fake web site without their consent	hacking
software that gathers information by monitoring key presses on a user's computer and relays the information back to the person who sent the software	pharming
program or code that replicates itself and is designed to amend, delete or copy data and files on a user's computer without their consent	phishing
the act of gaining illegal access to a computer system without the owner's consent	spyware
creator of code sends out a legitimate-looking email in the hope of gathering personal and financial data; it requires the recipient to follow a link in the email or open an attachment	virus

[4]

PapaCambridge

Examiner comment – low

This candidate has made a common error in their answer to **1(a)**. It is a common error to think that cookies are only used in advertising. They also made the mistake of thinking that cookies act like a virus. Cookies are created to collect data, whereas a virus is created to corrupt data.

This candidate matched three definitions incorrectly. They mixed their understanding of the definitions of phishing, pharming and spyware; this is a common mistake to make.

Marks awarded for **1(a)** = 2 out of 4
Marks awarded for **1(b)** = 2 out of 4

Total mark awarded = 4 out of 8

Example candidate response – high

4 **(a)** State what is meant by the term SSL.

Secure Socket Layer is a program which helps users be able to use secure applications on the internet and be able to browse safely/securely [1]

(b) The following stages take place when a user wishes to access a secure website.

Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	6
the web browser attempts to connect to a website which is secured by SSL	1
the web server sends the web browser a copy of its SSL certificate	3
the web browser requests the web server to identify itself	2
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	5
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	4

[5]

PapaCambridge

Examiner comment – high

In part **(a)** this candidate correctly states that SSL is secure sockets layer.

In part **(b)** they manage to get the correct sequence of events when a person uses a secure website.

Marks awarded for **(a)** = 1 out of 1
Marks awarded for **(b)** = 5 out of 5

Total mark awarded = 6 out of 6

Example candidate response – middle

4 **(a)** State what is meant by the term SSL.

Secure Socket Layer.
Which aware the user that the web pages
are secure. It can be seen in the ~~bar~~ URL. [1]

(b) The following stages take place when a user wishes to access a secure website.

Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	6
the web browser attempts to connect to a website which is secured by SSL	1
the web server sends the web browser a copy of its SSL certificate	3
the web browser requests the web server to identify itself	4
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	5
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	2

[5]

PapaCambridge

Examiner comment – middle

In part **(a)** this candidate correctly states that SSL is secure sockets layer.

In part **(b)** they mix up stages 2 and 4 in the sequence. The browser needs the server to identify itself before it can carry out any further stages.

Marks awarded for **4(a)** = 1 out of 1
Marks awarded for **4(b)** = 3 out of 5

Total mark awarded = 4 out of 6

Example candidate response – low

4 **(a)** State what is meant by the term SSL.

Server Securing Log

.....[1]

(b) The following stages take place when a user wishes to access a secure website.

Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	4
the web browser attempts to connect to a website which is secured by SSL	**1**
the web server sends the web browser a copy of its SSL certificate	3
the web browser requests the web server to identify itself	2
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	6
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	5

[5]

PapaCambridge

Examiner comment – low

In part **(a)**, the candidate gives an incorrect response from the definition of SSL. It was a good attempt, but not correct.

In part **(b)**, the candidate starts the sequence correctly but then gets the last three stages in the incorrect order. The web browser needs to check the certificate is trustworthy before it will share the encrypted data.

Marks awarded for **4(a)** = 0 out of 1
Marks awarded for **4(b)** = 2 out of 5

Total mark awarded = 2 out of 6

Past Papers

Q 1) Summer 2015 P11

4 Choose **six** correct terms from the following list to complete the spaces in the paragraphs below:

• encryption	• file name	• firewall
• HTML tags/text	• IP address	• protocol
• proxy server	• SSL certificate	• web server name

A user enters a URL. The web browser breaks up the URL into **three** components:
1 .....
2 .....
3 .....
The web server returns the selected web page.
The web browser reads the ..... from the selected page and shows the correctly formatted page on the user's screen.
A ..... is used between the user's computer and the network to examine the data traffic to make sure it meets certain criteria.
To speed up the access to the web pages next time, a ..... is used between the computer and web server; this device uses a cache to store the website home page after it has been accessed for the first time. [6]

Examiner's Comments on Question 4

The full range of marks were awarded to candidates for this question. It was clear some candidates knew the process and gained full marks, but most candidates achieved two or three marks.

6 (a) Viruses, pharming and phishing are all examples of potential Internet security issues. Explain what is meant by each of these **three** terms.
Virus: .....
.....
Pharming: .....
.....
.....
Phishing: .....
.....
.....[6]

(b) An online bank requires a client to supply an 8-digit code each time they wish to access their account on the bank's website.
Rather than ask the client to use a keyboard, they are requested to use an on-screen keypad (shown on the right) to input the 8-digit code.
The position of the digits on the keypad can change each time the website is visited.
The client uses a mouse or touch screen to select each of the8 digits.

2	**5**	**1**
6	**8**	**3**
9	**0**	**4**
	7	

(i) Explain why the bank has chosen to use this method of entering the 8 digits.
.....
.....
.....
..... [2]

(ii) Name and describe **another** measure that the bank could introduce to improve the security of their website.
Name: .....
Description: .....
.....
.....
..... [2]

PapaCambridge

Examiner's Comments on Question 6 (a) and (b)

In part (a) many candidates answered the section about viruses very well. Many candidates were not precise in their response for phishing and pharming and some candidates confused the two, mistaking one for the other.

In part (b)(i) most candidates gained just one of the two marks. This was normally for an answer that included reference to the prevention of key loggers picking up key presses. Candidates were not precise enough in their answer to gain two marks. Many candidates referred to stopping a person looking over their shoulder and seeing the password. This answer was often imprecise. Candidates provided some good security measures and descriptions in part (b)(ii). A wide range of knowledge was demonstrated by candidates in this area with most giving a good description for the security measure. Chip and Pin, security protocols such as SSL and encryption were the more common responses.

Q 2) Summer 2015 P12

1 (a) Four statements about cookies are shown in the table below.

Study each statement.

Tick (✓) to show whether the statement is true or false.

Statement	True	False
they are a form of spyware		
they are used only in advertising		
they are used to track browser use		
they act in the same way as a virus		

b) Five descriptions and five security issues are shown below.

Draw a line to connect each description to the correct security issue.

Description	Security issue
Malicious code installed on the hard drive of a user's computer or on the web server; this code will re-direct user to a fake web site without their consent	Hacking
Software that gathers information by monitoring key presses on a user's computer and relays the information back to the person who sent the software	Pharming
Program or code that replicates itself and is designed to amend, delete or copy data and files on a user's computer without their consent	Phishing
The act of gaining illegal access to a computer system without the owner's consent	Spyware
Creator of code sends out a legitimate-looking email in the hope of gathering personal and financial data; it requires the recipient to follow a link in the email or open an attachment	Virus

Examiner's comments on Questions 1(a) and 1(b)

In part (a) the full range of marks were awarded with most candidates gaining three or four marks. The most common error was candidates mistaking cookies for being spyware.

In part (b) the full range of marks were awarded and candidates displayed a good level of knowledge of security issues. The most common error was candidates confusing the definition of phishing and pharming

4 (a) State what is meant by the term SSL.

.....
.....
.....[1]

(b) The following stages take place when a user wishes to access a secure website.
Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you. [5]

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	
the web browser attempts to connect to a website which is secured by SSL	**1**
the web server sends the web browser a copy of its SSL certificate	
the web browser requests the web server to identify itself	
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	

Examiner's comments on Questions 4(a) and 4(b)

Most candidates gained a mark for their answer to part (a). This was mainly through stating Secure Sockets Layer as the full name for SSL. Those candidates that did not provide the name, but instead gave a description of SSL involving encryption and web servers also gained a mark.
In part (b) the full range of marks were awarded with many candidates demonstrating a good level of knowledge of secure websites. The most common error was the confusion of steps 2 and 3.

Q 3) Winter 2015 P12

1 There are a number of security risks associated with using the Internet.
Name **three** of these risks. For each, state why it is a risk and describe how the risk can be minimised.

Security risk 1: .....
Why it is a risk: .....
.....
How to minimize the risk:.....
.....
Security risk 2: .....
Why it is a risk: .....
.....
How to minimize the risk: .....
.....
Security risk 3: .....
Why it is a risk: .....
.....
How to minimize the risk: .....
..... [9]

PapaCambridge

Examiners' Comments Question 1

Most candidates were able to accurately name three different security risks. Many candidates were able to describe why they were a risk, but some candidates did not provide clear detail in their answer for this section. These candidates were vague in their response and not specific in the detail. Candidates need to make sure they are specific in their answers, clearly demonstrating their understanding.

Some candidates did not give an accurate enough response for minimising the security risk, for example installing most software will not ensure the risk in minimised. The software needs to be run in order to minimise the risk.

Q 4) Winter 2015 P13

4 (b) The four statements below refer to firewalls and proxy servers. Study each statement. Tick (9) the appropriate column(s) to indicate whether the statement refers to a firewall and/or a proxy server. [4]

Statement	**Firewall**	**Proxy server**
Speeds up access of information from a web server by using a cache		
Filters all Internet traffic coming into and out from a user's computer, intranet or private network		
Helps to prevent malware, including viruses, from entering a user's computer		
Keeps a list of undesirable websites nd IP addresses		

(c) Explain **three** ways of preventing **accidental** loss or corruption of data.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

3 .....

.....

.....

..... [6]

Examiners' Comments Question 4 (a), (b) and (c)

In part (a)(i) many candidates confused free software with freeware or shareware, providing an incorrect answer. In part (a)(ii) most candidates were able to pick up marks by describing areas that might be covered in ethics. Most candidates missed providing detail about ethics being used to regulate or govern the use of computers.

In part (b) many candidates did not identify that some statements could apply to both a firewall and a proxy server. Most ticked only one.

In part (c) many candidates did not consider the question thoroughly and realise that it was asking about accidental damage and not malicious damage. Many candidates wrote about malicious damage such as viruses. Some candidates could correctly identify some methods such as creating a back-up. Candidates need to understand a clearer distinction between what causes accidental damage and what causes malicious damage.

PapaCambridge

10 Choose **five** correct terms from the following list to complete the spaces in the sentences below:

- cypher text
- encryption algorithm
- encryption key
- firewall
- plain text
- proxy server
- symmetric encryption

..... is a security system.
It uses the same ..... to encrypt and decrypt a message.
Before encryption, the message is called ..... .
The ..... processes the original message. The output is known as ..... . [5]

Examiners' Comments Question 10

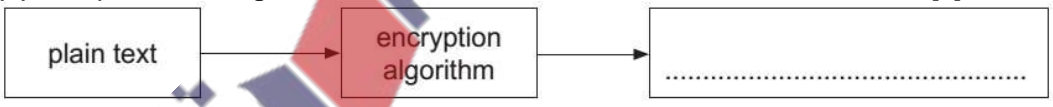
Some candidates were able to provide the correct missing terms, many confused plain text and cypher text, or encryption key and encryption algorithm.

Q 5) Winter 2015 P11

3 (a) Three statements about cookies are shown below.
Study each statement. Tick to show whether the statement is true or false. [3]

Statement	True	False
Cookies can destroy or modify data in a computer without the user's knowledge		
Cookies generate website pop-ups		
Cookies allow a website to detect whether a viewer has viewed specific web pages		

6 (a) State what is meant by encryption.
.....
..... [1]
(b) State what is meant by symmetric encryption.
.....
..... [1]
(c) Complete the diagram: [1]



Examiners' Comments Question 6(a) (b) and (c)

In part (a) many candidates were able to demonstrate that they could provide a definition of encryption.
In part (b) many candidates were not able to accurately describe symmetric encryption. Many gave a second similar definition of encryption, rather than referring to the fact that symmetric encryption uses the same key to encrypt and decrypt text.
In part (c) most candidates correctly identified the next stage of the process.

13 Identify which **five** computer terms are being described below.
(a) A system designed to prevent unauthorised access to or from a private network or intranet; it examines all data traffic to and from the network and filters out anything that does not meet certain criteria.
..... [1]
(b) Software that can be used on a trial basis before buying the full version; it often does not include all the features of the full version or has a time limit before it stops working.
.....[1]

PapaCambridge

(c) A protocol for transmitting private documents via the Internet; it uses two keys to encrypt the data – a public key and a private key.

.....[1]

(d) A standard adopted by the electronic music industry for controlling devices that produce music, such as synthesisers and sound cards.

..... [1]

(e) A device that allows audio signals to be converted into electrical signals which can be interpreted by a computer after being converted into digital signals.

.....[1]

Examiners' Comments Question 13(a) (b) (c) (d) and (e)

Many candidates were able to gain at least two or three marks in this section. Some confused shareware for freeware or free software, demonstrating they were unsure of their knowledge in this area.

Q 6) Summer 2016 P11 & P13

6 Secure socket layer (SSL) is used in the security of information on Internet websites.

(a) State how it is possible for a user to know that a website is secure by looking at the web address.

.....

..... [1]

(b) Describe **three** of the stages a web browser goes through to detect whether a website is secure.

1 .....

.....

.....

2 .....

.....

.....

3 .....

.....

..... [3]

Examiner Report Question 6(a) and (b)

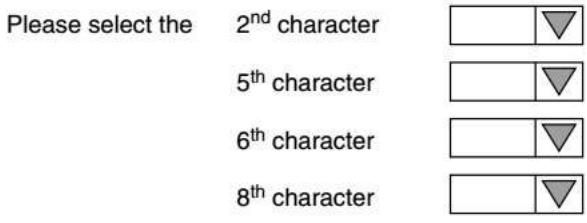
In part (a) most candidates correctly identified that the http in the address would have https if the website is secure. Some candidates were awarded a mark if they fully explain that a padlock is also present to identify the security of the website.

In part (b) very few candidates were able to describe three stages of the process. Many candidates incorrectly referred to a request being sent to the website to identify itself, and that the website sends the SSL certificate. They must recognise it is the role of the web server to do this and not the website.

PapaCambridge

8 A bank offers an online service to its customers. The bank has developed a "*SafeToUse*" systemthat asks each customer to enter four randomly chosen characters from their password each time they log in.

The customer selects these four characters from drop-down boxes. For example:



[2]

(a) (i) Explain why it is more secure to use drop-down boxes rather than entering characters using a keyboard.

.....

.....

.....[2]

(ii) Give a reason why the system asks for four characters chosen at random.

.....

.....[1]

(b) Biometrics is an additional form of security.

Give two examples of biometrics.

1 .....

2 ..... [2]

Examiner Report Question 8 (a)(i), (ii) and (b)

In part (a)(i) many candidates recognised that the method would protect against ley logging software. Few candidates were able to expand this point to advise this is because drop down boxes cannot be recorded as a key press on a keyboard.

In part (a)(ii) some candidates were able to recognise that this kind of method would mean that it would be very difficult for a hacker to get the password in a single time of hacking, that it would take several times of hacking or observations to be able to attempt to gain the full password. Many candidates were not able to recognise this and repeated or reworded answers given in part (a)(i).

In part (b) many candidates were able to identify suitable examples of biometric devices. Some candidates did not give accurate and technical names for a biometric device. The most common error was describing a retina/iris scanner as an eye scanner.

PapaCambridge

10 Six security issues and six descriptions are shown below.
Draw a line to link each security issue to its correct description.[5]

URL	Description
Pharming	illegal access to a computer system without the owner's consent or knowledge
Phishing	software that gathers information by monitoring key presses on a user's keyboard; the data is sent back to the originator of the software
Viruses	malicious code installed on the hard drive of a user's computer or on a web server; this code will re-direct the user to a fake website without the user's knowledge
Hacking	creator of code sends out a legitimate-looking email in the hope of gathering personal and financial information from the recipient; it requires the user to click on the link in the email or attachment
Spyware	a message given to a web browser by a web server; it is stored in a text file; the message is then sent back to the server each time the browser requests a page from the server
Cookies	program or code that replicates itself; designed to amend, delete or copy data or files on a user's computer; often causes the computer to crash or run slowly

PapaCambridge

Examiner Report Question 10
Most candidates were able to match the correct term with the correct definition. The most common errors were the confusion of the terms Phishing and Pharming, and cookies and spyware.

Q 7) Summer 2016 P12

8 (c) Security of data is very important.

Three security issues are viruses, pharming and spyware.

Explain what is meant by each issue.

Viruses: .....

.....

.....

Pharming: .....

.....

.....

.....

Spyware: .....

.....

.....[6]

(d) Describe **three** tasks carried out by a firewall.

1 .....

.....

2 .....

.....

3 .....

.....

.....[3]

Examiner Report Question 8(a), (b), (c) and (d)

In part (a) a number of candidates only gained a single mark for the question. This is because they only joined each type to a statement using a single line. Candidates are reminded that when the question requires candidates to draw lines (not a line) this means that multiple lines may go from a term to a statement.

In part (b) some candidates were able to describe a range of ethical issues in a good amount of detail. A number of candidates were vague and repetitive in their descriptions and were not able to gain marks for this.

In part (c) many candidates were able to gain at least one mark for each term. Some candidates were vague in their response and gave little accurate detail about each term. Pharming was often confused with a description on Phishing. Virus sometimes did not include a reference to the program or software being what is self-replicating.

In part (d) some candidates had a clear understanding of the role of a firewall. Many candidates gave vague descriptions that did not fully detail the role of a firewall. Candidates must make sure that their descriptions display a good level of knowledge and are not a vague generic description.

PapaCambridge

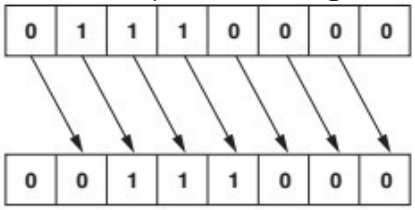
Q 8) Winter 2016 P12

5 A computer uses an 8-bit register.
The 8-bit register contains binary integers.
(a) Write the denary (base 10) value represented by:

128	64	32	16	8	4	2	1
0	1	1	1	0	0	0	0

.....[1]

(b) All the bits in the register are shifted **one** place to the **right** as shown below.



Write the denary number that is represented after this shift.
.....[1]

(c) State the effect the shift to the right had on the original denary number from **part (a)**.
.....[1]

(d) The original number in **part (a)** is shifted **three** places to the **right**.

(i) Show the new binary number: [1]

(ii) Write the equivalent denary number.
.....[1]

(e) Describe the problems that could be caused if the original binary number in **part (a)** is shifted **five** places to the **right**.
.....
.....
.....
.....
.....[2]

Examiner Report

In parts **(a)** and **(b)** most candidates could provide a correct conversion from binary to denary.
In part **(c)** many candidates could identify the effect that the shift had on the number. Some candidates were too vague in their response stating the number had merely decreased.
In parts **(c)** and **(d)** most candidates could perform the shift and convert it to the correct denary value.
In part **(e)** most candidates could not accurately explain the effect of the shift. They were not able to express that the right most bit would be lost from the register, making the number inaccurate.

PapaCambridge

9 (a) Explain what is meant by a denial of service attack.

.....

.....

.....

.....[2]

(b) Name and describe **two other** potential security threats when using the Internet.

Security threat 1 .....

Description .....

.....

.....

Security threat 2 .....

Description .....

.....

..... [4]

Examiner Report

In part **(a)** very few candidates could provide an accurate description of a denial of service attack. Many just stated that it denies the user of a service, which was not accurate enough for a mark.

In part **(b)** some candidates could identify and describe further security threats. Some candidates mistakenly identified security measures rather than security threats. Candidates must make sure they thoroughly read the question.

Q 9) Winter 2016 P11& 13

2 Name each of the potential security issues described in the **five** statements below: [5]

Statement	**Security issue**
The act of gaining unauthorised access to a computer system	.....
Program code that can replicate itself with the intention of deleting or corrupting files stored in a computer	.....
A small file sent by a web server to a web browser; every time the user visits the website, data about user preferences is collected	.....
The act of illegally changing the source code of a program so that it can be exploited for another use	.....
Malicious code installed on a user's hard drive or a web server which redirects the user to a fake website without their knowledge	.....

Examiner Report

Some candidates could correctly identify all five potential security issues. Most candidates could identify hacking and virus. Many could identify pharming, but some incorrectly identified this as phishing or spam. Many candidates did not correctly identify cookies or cracking.

PapaCambridge

4 The Henslows Diner is a local restaurant.

(c) The Henslows Diner stores personal data on a computer. This computer is connected to the Internet to allow the data to be backed up.

There is currently one security method in place to protect the data on the computer from unauthorised access. This is a password.

Give **two** other security methods that could be added to improve the security of the data.

Describe how each method will keep the data safe.

Security method 1 .....

Description .....

.....

.....

Security method 2 .....

Description .....

.....

.....[4]

Examiner Report

In part **(a)** many candidates answered this question well, providing two reasonable disadvantages of using a keyboard.

In part **(b)** some candidates could provide two reasonable benefits. Most candidates tried to turn the disadvantages into a benefit, which provided some good answers. Candidates need to make sure that they provide benefits relating to the context they are given. Some candidates provided a benefit that was not relevant to the context they had been given.

In part **(c)** some candidates could gain marks for identifying a security method. Many candidates did not get a mark for describing how the security method kept the data safe. Most candidates stated that it does keep the data safe by stopping unauthorised access, but did not describe how it did this. The most common error from candidates was reference to anti-virus as a method of security for preventing unauthorised access. This could be a reasonable answer to preventing data from being corrupted, but the question specifically asked for security methods about preventing unauthorised access.

10 (d) When sending this data, security is very important. Data are sent over the Internet using Transport Layer Security (TLS) protocol.

Name the **two** layers that make up TLS.

1 .....

2 ..... [2]

Examiner Report

In part **(a)(i)** many candidates incorrectly transcribed the value 431 as though it was a hexadecimal value. Candidates must read the question to correctly establish what the value is, in this case it was a denary value.

In part **(a)(ii)** most candidates could correctly provide a hexadecimal conversion, some from follow through from part **(a)(i)**.

In part **(b)** some candidates could provide a full answer gaining 3 marks. Some candidates did not provide any working out, so could not gain full marks. Candidates are reminded to provide full working out when the question asks to show working.

In part **(c)** most candidates could provide the full version of the acronym for MAC and IP. Some candidates gained marks by explaining what a MAC address or an IP address is.

In part **(d)** very few candidates could correctly identify either layer of TLS.

PapaCambridge

Q 10) March 2017 India

4 A simple symmetric encryption system is used to encrypt messages. Each letter of the alphabet is substituted by another letter.

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Cypher text

v	p	n	a	q	b	r	u	z	s	c	o	y	k	w	f	x	i	e	m	d	j	t	l	h	g

(a) Convert the following plain text to cypher text.
Plain text: **d a t a s e c u r i t y**
Cypher text: .....[2]

(b) A new cypher text is created by shifting each letter of the alphabet **five** places to the right. Show the new cypher text below.

Plain text

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

New cypher text

[2]

(c) State, giving a reason, which cypher text would be more secure.

.....

.....

.....

..... [2]

Examiner Report
(a) Most candidates correctly converted the plain text to cypher text using the symmetric encryption shown.
(b) Some candidates correctly shifted the plain text five places to the right. Common errors included incorrectly shifting the text to the left or incorrectly shifting the cypher text rather than the plain text.
(c) Most candidates correctly identified the cypher text given in **part (a)** as the more secure.

5 Give the meaning of the following terms.

HTML .....

.....

http .....

.....

https .....

..... [3]

Examiner Report
This was generally well answered.

PapaCambridge

9 Passwords are used to keep data safe.
Explain the differences between a *text-based password* and a *biometric password*.

.....
.....
.....
.....
.....
.....
.....[4]

Examiner Report
Most candidates gave an appropriate example of a biometric password and stated that a text based password consisted of characters. Better candidates then went on to describe what was different, for example 'biometric passwords are unique to a person and cannot be shared'.

Q 11) Summer 2017 P11

7 Six security terms and **six** statements are listed below.
Draw a line to match the security term with the most appropriate statement. [5]

Security term	Statement
Encryption	Provides a secure connection between web browsers and websites allowing secure transmission of private data.
Secure Socket Layer (SSL)	Computer that acts as an intermediary between a web browser and the Internet.
Pharming	Legitimate-looking email is sent in the hope of gathering personal information; it requires the user to click on a link in the email.
Phishing	Uses rules and criteria, set by the user, to help protect a network or system from unauthorised access.
Firewall	Malicious code installed on the hard drive of a user's computer; this code will redirect the user to a fake website without the user's knowledge.
Proxy server	Scrambles data for secure transmission.

PapaCambridge

Examiner Comment on Q 7
Many candidates correctly match all six terms and definitions. The most common incorrect answers were theconfusion of phishing and pharming, and firewall and proxy server.

Q 12) Summer 2017 P12

8 A company has a number of offices around the world.

(a) Data is transmitted between the offices over the Internet. In order to keep the data safe the company is using Secure Socket Layer (SSL) protocol and a firewall at each office.

Explain how SSL protocol and a firewall will keep the company's data safe.

SSL protocol .....

.....

.....

Firewall .....

.....

..... [4]

(b) A company stores personal details of its customers on a computer system behind a firewall.

Explain, with reasons, what else the company should do to keep this data safe.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[6]

Examiner Comment on Q 8(a)

Some candidates understood that the SSL protocol uses encryption, few candidates provided further detailthan this. Some candidates misunderstood the question and described what SSL is used for.Some candidates understood that a firewall acts as a filter, few candidates provided further detail than this.Many candidates were vague and inaccurate with their description.

It would be beneficial for candidates to have an accurate and more in-depth understanding of SSL andfirewalls.

Examiner Comment on Question 8(b)

Many candidates provided a range of methods that could be used to keep the data safe. It would bebeneficial for candidates to understand that methods such as anti-virus and anti-malware software can helpprevent data being affected, but they do not fully prevent data being affected.

11 A company sells smart phones over the Internet.

Explain how the information stored on the company's website is requested by the customer, sent to the customer's computer and displayed on the screen.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[7]

PapaCambridge

Examiner Comment on Q 11
Candidates found this question challenging. Some candidates described using a web browser and entering aURL, but after this their answer lacked detail of the process involved. It would be beneficial for candidates tohave a greater understanding of how data is retrieved for a web page, and how it is displayed on the user'sscreen. Some candidates misunderstood the question and described the operations of security certificates.

Q 13) Winter 2017 P12

5 Raj is using the Internet to do some online shopping. He visits a website that tells him that it use s cookies.

(a) Explain what is meant by the term **cookies**.

Method 1 .....

.....

.....

.....

.....

.....

..... [4]

(b) Give **two** examples of the use of cookies.

Example 1 .....

.....

.....

Example 2 .....

.....

.....[2]

10 (a) Describe what is meant by Transport Layer Security (TLS).

.....

.....

.....

.....

.....

..... [3]

(b) Name **three** different applications of TLS.

1 .....

2 .....

3 ..... [3]

PapaCambridge

Q 14) Winter 2017 P13

7 Six statements about firewalls are shown.

Tick (✓) to show whether each statement is true or false. [6]

Statement	True (✓)	False (✓)
Firewalls can monitor incoming and outgoing traffic.		
Firewalls operate by checking traffic against a set of rules.		
Firewalls cannot block access to a certain website.		
Firewalls can be software and hardware.		
Firewalls can act as intermediary servers.		
Firewalls can block unauthorised traffic.		

8 (a) Data is valuable. It needs to be kept secure and it can easily be damaged.

Give three different ways that data can be accidentally damaged.

1 .....

.....

2 .....

.....

3 .....

..... [3]

(b) The Secure Socket Layer (SSL) protocol can be used to securely transmit data in online banking.

State three other different applications that use SSL.

Application 1 .....

Application 2 .....

Application 3 .....[3]

(c) Online banking is increasing in popularity.

Online banking can be a risk as it can raise a number of security issues. SSL can be used as a security method to make online banking safer.

Identify and describe three other security methods that could be used to make online banking safer.

Security method 1 .....

.....

.....

.....

Security method 2 .....

.....

PapaCambridge

.....

.....

Security method 3 .....

.....

.....

..... [6]

Q 15) March 2018 P12 (India)

2 David has installed anti-virus software on his computer.

(a) State **three** tasks carried out by anti-virus software. [3]

Task 1 .....

.....

Task 2 .....

.....

Task 3 .....

.....

(b) David is still concerned that his computer might get infected by a computer virus.

State three other ways in which David can reduce the risk of his computer getting a computer virus

.

1 .....

.....

2 .....

.....

3 .....

.....[3]

Comments on Question 2

(a) Many candidates answered this question well. Most candidates provided information about the virus scanner identifying and removing viruses. It would be encouraging to see candidates begin to provide understanding beyond this about the role of anti-virus software.

Some candidates demonstrated a misconception that anti-virus software will stop any viruses being downloaded. It would be helpful if candidates understood that this is not the case.

(b)Most candidates demonstrated a good level of knowledge for this question. The most common responses were the use of a firewall and to only download from trusted sources.

Some candidates repeated a solution already given in part 2(a) about using anti-virus software to scan the computer. It would be helpful if candidates understood that if this has already been provided as a solution, no marks can be awarded for further elaboration when other alternatives have been requested.

PapaCambridge

Q 16) Summer 2018 P11

10 (c) When a customer enters the website, a message is displayed:

"RockICT makes use of cookies. By continuing to browse you are agreeing to our use of cookies."

Explain why the music company uses cookies.

.....

.....

.....

.....[2]

(d) The music company is concerned about the security of its website.

The company uses a proxy server as part of its security system.

Describe the role of a proxy server in the security system.

.....

.....

.....

.....

.....

.....

.....

.....[4]

Q 17) Summer 2018 P12

12 (a) Selma has some important personal information that she needs to email to her employer. She wants to make sure that if the personal information is intercepted, it cannot be understood.

(i) State how Selma could email her personal data more securely.

..... [1]

(ii) Describe how your chosen solution works.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

PapaCambridge

(b) Selma wants to make sure that the information received is correct.
A parity check can be used to detect errors.
Describe another error detection method that can be used to check the information received is correct.

Error detection method .....

Description .....

.....

.....

.....

.....

.....

.....

..... [3]

Q 18) Winter 2018 P12

4 (a) Identify **three** security issues that can put a computer system at risk.

Security issue 1 .....

Security issue 2 .....

Security issue 3 .....[3]

(b) Explain how a firewall can help to protect a computer system from security issues.

.....

.....

.....

.....

.....

.....

.....[4]

PapaCambridge

Q 19) Winter 2018 P13

6 Sarah stores data electronically. Describe three methods that she could use to avoid loss of stored data.

Method 1 .....

....

.....

.....

.....

Method 2 .....

.....

.....

.....

.....

Method 3 .....

.....

.....

.....

..... [6]

Q 20) March 2019 P12

7 Arya regularly uses the Internet as a research tool for her school projects.

Identify **and** describe **three** risks to Arya's computer when she is using the Internet for research.

Risk 1 .....

Description .....

.....

.....

Risk 2 .....

Description .....

.....

.....

Risk 3 .....

Description .....

.....

..... [6]

PapaCambridge

Q 21) Summer 2019 P11

4 (a) Lola is concerned about the risks to her computer when using the Internet.

She wants to use some security methods to help protect her computer from the risks.

Identify a security method she could use for each of the following risks. Each security method must be different. Describe how each security method will help protect Lola's computer.

(i) Computer virus

Security method .....

Description .....

.....

.....

..... [3]

(ii) Hacking

Security method .....

Description .....

.....

.....

..... [3]

(iii) Spyware

Security method .....

Description .....

.....

.....

..... [3]

(b) Lola is also concerned that the data she stores could be subject to accidental damage or accidental loss.

(i) State **three** ways that the data Lola stores could be accidentally damaged or accidentally lost.

1 .....

.....

2 .....

.....

3 .....

..... [3]

(ii) Give **two** methods that Lola could use to help keep her data safe from accidental damage or accidental loss.

1 .....

.....

PapaCambridge

2 .....

..... [2]

6 A law company holds a lot of sensitive data about its clients.

(a) It currently requires employees to enter a username and a password to log-in to an account. Each password must be 8 letters. The company wants to increase the security of the log-in system.

Identify **two** improvements the company could use to make the log-in system more secure.

Explain how each improvement increases security.

Improvement 1 .....

.....

Explanation .....

.....

.....

Improvement 1 .....

.....

Explanation .....

.....

..... [4]

8 An art gallery has a website that is used to display and sell art.

(a) The gallery uses Secure Socket Layer (SSL) to provide a secure connection when selling art.

Describe the process of SSL and how it provides a secure connection.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

PapaCambridge

(b) The art gallery also uses a firewall. **Six** statements are given about firewalls.

Tick (✓) to show if the statement is **True** or **False**. [6]

Statement	**True** (✓)	**False** (✓)
Firewalls are only available as hardware devices		
Firewalls allow a user to set rules for network traffic		
Firewalls will automatically stop all malicious traffic		
Firewalls only examine traffic entering a network		
Firewalls encrypt all data that is transmitted around a network		
Firewalls can be used to block access to certain websites		

(c) The art gallery is concerned about computer ethics relating to its website.

Explain what is meant by computer ethics **and** why the art gallery is concerned about computer ethics.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Q 22) Summer 2019 P12

5 A music company wants to send a new music file to many radio stations. It will send the music file the day before the release date so that the radio stations can store the file ready for release. The music company does not want the radio stations to be able to open the music file until 09:00 on the release date.

Identify **two** security measures **and** describe how each measure can be used to make sure the music file cannot be opened until the release date.

Security measure 1 .....

Description .....

.....

.....

Security measure 2 .....

Description .....

.....

..... [4]

PapaCambridge

6 Priya creates a website to sell her old comic books and superhero figures.

(b) Priya uses cookies in her website. **Five** statements are given about cookies.

Tick (✓) to show if the statement is **True** or **False**. [5]

Statement	**True (✓)**	**False (✓)**
Cookies can be used to store a customer's credit card details		
Cookies can be used to track the items a customer has viewed on a website		
Cookies will corrupt the data on a customer's computer		
Cookies are downloaded onto a customer's computer		
Cookies can be deleted from a customer's computer		

(e) Priya is concerned about a denial of service attack (DoS) occurring on her web server.

(i) Explain what is meant by a denial of service attack.

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Give **one** security device that can be used to help prevent a denial of service attack.

..... [1]

Q 23) Winter 2019 P13

1 A library has a system that allows customers to check out the books that they want to borrow. Each book has a barcode that can be used to identify the book.

(b) The data stored by the library is archived at the end of each day. The archive is held on a server in the library office. The data is encrypted with an 8-bit key. As some of the data is confidential, the library wants to make the encryption more secure.

(i) State how the library could make the encryption more secure.

.....

..... [1]

(ii) The term used to describe data before it is encrypted is plain text.

State the term used to describe encrypted data.

..... [1]

PapaCambridge

6 Jesse is taking his Computer Science examination. He answers five questions about ethics.

(a) For the first question, he writes the answer:

"This type of software can be copied and shared without the permission of the owner."

State what Jesse is describing.

..... [1]

(b) For the second question, he writes the answer:

"With this type of software, the owner still retains the copyright for the software, but he gives away copies of it for free."

State what Jesse is describing.

..... [1]

(c) For the third question, he writes the answer:

"This type of software is often a trial version of the full software. To use the full version the user normally needs to pay a fee."

State what Jesse is describing.

..... [1]

(d) For the fourth question, he writes the answer:

"This is when a person copies another person's computer program and tries to claim it as his own."

State what Jesse is describing.

..... [1]

(e) For the fifth question, he writes the answer:

"This is the legal protection that a person can obtain, to provide protection against his work being stolen."

State what Jesse is describing.

..... [1]

8 A company discovers malware on its network.

Explain **two** ways that the malware could have been introduced to the company's network.

.....

.....

.....

.....

.....

.....

.....

..... [4]

PapaCambridge

Q 24) Winter 2019 P12

7 Gerald uses a keyboard to enter a website address into the address bar of his browser.

(c) The website Gerald visits uses https. Explain what is meant by https.

.....

.....

.....

.....

.....

..... [3]

10 Data is valuable to a company.

(a) Companies use error detection methods to make sure that data is accurate.

One error detection method is the use of a check digit.

Explain what is meant by a check digit and how it is used to detect errors.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) Companies can use a range of security methods to keep their data secure.

Identify **two** security methods that a company can use to keep their data secure **and** explain how each method can keep the data secure.

Security method 1 .....

.....

.....

.....

.....

.....

Security method 2 .....

.....

.....

.....

.....

..... [6]

PapaCambridge

Q 25) March 20 P12

2 A school network is used to transmit and store data about students.

(c) Data is encrypted using 128-bit symmetric encryption before it is transmitted.

(i) Explain what is meant by encryption.

.....

.....

.....

..... [2]

(ii) State how the strength of the encryption can be improved.

.....

..... [1]

(d) Describe how the school could prevent the loss of stored data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

8 A student website provides research support and software downloads.

(a) Students use a browser to access the web pages. Explain the role of a browser in this process.

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

PapaCambridge

(b) The website owners are worried about a denial of service (DoS) attack.

Explain the term denial of service attack.

.....

.....

.....

.....

.....

..... [3]

(c) The website owners are also concerned about the ethical issues of copyright and plagiarism.

(i) State what is meant by the term copyright.

.....

..... [1]

(ii) State what is meant by the term plagiarism.

.....

..... [1]

Q 26) Summer 20 P12

3 A company collects and stores data about its customers. The data is stored on a server in the company's office. The data is transmitted to cloud storage to create a back-up.

The data is encrypted using symmetric encryption before it is sent to the cloud storage.

(a) Describe how the data is encrypted.

.....

.....

.....

.....

.....

.....

.....

.....

[4]

(b) Give **three other** methods that can be used to secure the data in the office.

Method 1 .....

.....

Method 2 .....

.....

Method 3 .....

..... [3]

PapaCambridge

5 Meena uses a browser to research information for her business.

(a) Give **three** functions of a browser.

1 .....

2 .....

3 ..... [3]

(b) Meena buys products for her business using the Internet.

The Transport Layer Security (TLS) protocol is used for transferring data when she buys products.

One layer of the TLS protocol is the handshake layer.

(i) Describe the purpose of the handshake layer.

.....

.....

.....

..... [2]

(ii) Identify the other layer of the TLS protocol.

..... [1]

(iii) Identify another protocol that can be used to transfer data securely.

..... [1]

(c) Meena visits a website to buy products for her business.

The browser uses a small file to store the details of the products she views. This allows the website to display advertisements for other products she may like.

The small file also stores her log-in details.

Give the name of this type of file.

..... [1]

10 Uma is concerned about risks that she may encounter when using the Internet.

Two of the risks she is concerned about are phishing and pharming.

(a) Give **one** similarity and **two** differences between phishing and pharming.

Similarity .....

.....

.....

Difference 1 .....

.....

.....

Difference 2 .....

.....

..... [3]

PapaCambridge

(b) Identify **two** other risks that Uma could encounter when using the Internet.

Risk 1 .....

Risk 2 ..... [2]

(c) Uma uses a firewall to secure the data on her computer.

(i) Uma tells her friend that a firewall can only be software-based.

Tick (✓) to show whether Uma is **Correct** or **Incorrect**. [1]

☐ **Correct**

☐ **Incorrect**

(ii) Describe how the firewall helps to keep Uma's data secure.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Q 27) 15a Summer 20 P11

7 Hans has a website selling comic books. Customers can create an account to buy the comic books.
Customers enter a username and password to log in to their account.
(a) Customers may worry about keylogging software being used to gain unauthorised access to their account.
(i) Describe how keylogging software can be used to gain unauthorised access to a customer's account.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Identify a feature that Hans can add to the website to limit the threat of keylogging software.

..... [1]

PapaCambridge

(b) Hans makes sure data transmission for his website is secure.
(i) State how customers can check that the personal details they enter into the website will be transmitted securely.

.....
..... [1]

(ii) Explain how a customer's browser checks that the website is secure.

.....
.....
.....
.....
.....
.....
.....
..... [4]

28) Winter 20 P12

1 (d) Tina will use the TLS protocol in her website when selling tickets to people for different charity events. This makes sure that their personal data is transmitted securely.

(i) Identify the **two** layers that are present in the TLS protocol.

Layer 1 .....

Layer 2 ..... [2]

(ii) Explain how data is sent securely using the TLS protocol.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... [6]

(e) Tina is concerned about security threats to her web server.

(i) Identify **three** security threats to her web server that Tina might be concerned about.

1 .....

2 .....

3 ..... [3]

PapaCambridge

(ii) Tina installs a proxy server to help protect her website from security threats.

Describe how the proxy server will help protect the website.

.....

.....

.....

.....

.....

.....

.....

..... [4]

3 Alessandro has some important data stored on his computer.

He is concerned about accidental damage to his data.

(a) (i) Identify **three** ways that the data could be accidentally damaged.

1 .....

2 .....

3 ..... [3]

(ii) State what Alessandro could do to make sure that he can retrieve his data if it is accidentally damaged.

.....

Q 29) Winter 20 P13

4 Eugene has a web server that stores his online shopping website.
Customers access the website using a browser.

(a) Describe how the webpages are requested and displayed on the customer's computer.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) State **three** online security threats to Eugene's web server.

Threat 1 .....

Threat 2 .....

Threat 3 ..... [3]

PapaCambridge

6 Elsa writes a paragraph in an examination about encryption.
There are several terms missing from the paragraph.
Complete the paragraph using the list of given terms. Not all terms may need to be used.
Some terms may be used more than once.

• algorithm	• alphanumeric	• cookie
• cypher	• key	• padlock
• plain	• word processed	

The data is encrypted using a ..... . This is an ..... that is used to scramble the data. The data before encryption is known as ..... text. When the data has been encrypted it is known as ..... text. To read the encrypted data it needs to be decrypted using a ..... . [5]

13 Phishing and pharming are two security issues a user should be aware of when using the Internet.

(a) State **one** similarity between phishing and pharming.

.....

..... [1]

(b) Explain **two** differences between phishing and pharming.

Difference 1 .....

.....

.....

Difference 2 .....

.....

..... [2]

Q 30) March 21 P12

2 (c) Users can buy the high definition photographs from the website. When a user buys a high definition photograph, a Secure Socket Layer (SSL) connection is created.

(i) Give **one** benefit of using an SSL connection.

.....

..... [1]

(ii) Explain how the SSL connection is created.

.....

.....

.....

.....

.....

.....

.....

..... [4]

PapaCambridge

6 Hacking is one type of Internet risk used to obtain personal data that is stored on a computer.

(a) Explain how a firewall can help prevent hacking.

.....
.....
.....
.....
.....
.....
.....
..... [4]

(b) Identify and describe **two** other types of internet risk that are used to obtain personal data.

Internet risk 1 .....
Description .....
.....
.....
.....
Internet risk 2 .....
Description .....
.....
.....
..... [6]

PapaCambridge

Marking Scheme

Q 1) Summer 2015 P11

4 1 mark per correct word

1 protocol
2 web server name
3 file name

accept these three items in any order

HTML tags/text

firewall

proxy server

6 (a) virus

any **two** from:

- program/software that replicates/copies itself
- can delete or alter files/data stored on a computer
- can make the computer "crash"/run slow

pharming

any **two** from:

- malicious code/software installed on a user's hard drive/actual web server
- this code redirects user to a fake website (without their knowledge)
- to obtain personal/financial information/data

phishing

any **two** from:

- legitimate-looking emails sent to a user
- as soon as recipient opens/clicks on link in the email/attachment …
- … the user is directed to a fake website (without their knowledge)
- To obtain personal/financial information/data

(b) (i) Any **two** from:

- spyware/key logging software can only pick up key presses
- using mouse/touchscreen means no key presses to log
- the numbers on the key pad are in random/non-standard format, which makes it more difficult to interpret

PapaCambridge

(ii) **1** mark for name and **1** mark for description

any **one** from:

chip and PIN reader
– only the user and the bank know which codes can be generated

request user name
– additional security together with password/PIN

anti-virus
– removes/warns of a potential virus threat which can't be passed on to customers

firewall
– (helps) to protect bank computers from virus threats and hacking

encryption
– protects customer data by making any hacked information unreadable

security protocol
– governs the secure transmission of data

Biometric
– to recognise user through the use of, e.g. facial/retina/finger print

Alerts
– users IP/MAC address is registered and user is alerted through, e.g. SMS if account is accessed through an unregistered address

PapaCambridge

Q 2) Summer 2015 P12

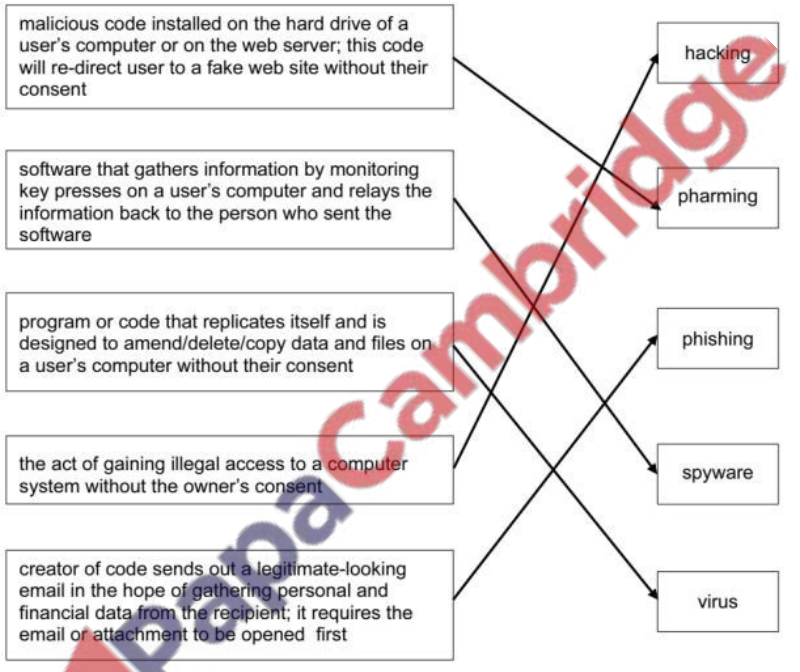
Page 2	Mark Scheme	Syllabus	Paper
	Cambridge O Level – May/June 2015	2210	12

1 **(a)** 1 mark per correctly placed tick

Statement	True	False
they are a form of spyware		✓
they are used in advertising only		✓
they are used to track the browsing of a user	✓	
they act in the same way as a virus		✓

[4]

(b)



4/5 matches – 4 marks
3 matches – 3 marks
2 matches – 2 marks
1 match – 1 mark

[4]

PapaCambridge

Page 5	Mark Scheme	Syllabus	Paper
	Cambridge O Level – May/June 2015	2210	12

4 **(a)** Any **one** from:

- secure sockets layer
- encrypts data being transmitted
- use of https
- use public and private keys

[1]

(b) 1 mark for each number in the correct order, next to the correct stage.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	6
the web browser attempts to connect to a web site which is secured by SSL	***(1)***
the web server sends the web browser a copy of its SSL certificate	3
the web browser requests the web server to identify itself	2
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	5
the web browser checks whether the SSL certificate is trustworthy; if it is then the web browser sends a message back to the web server	4

[5]

PapaCambridge

Q 3) Winter 2015 P12

1 1 mark for each risk + 1 mark for corresponding reason why it is a risk and 1 mark f of minimisation

Risk: hacking
Reason: illegal/unauthorised access to data
deletion/amendment of data
Minimised: use of passwords/user ids
use of firewalls
encrypt data/encryption

Risk: virus
Reason: can corrupt/delete data
cause computer to crash/run slow
can fill up hard drive with data
Minimised: use of /run anti-virus (software)
do not download software or data from unknown sources

Risk: spyware/key logging (software)
Reason: can read key presses/files/monitors on a user's computer
Minimised: use of/run anti-spyware (software)
use data entry methods such as drop-down boxes to minimise risk

Risk: phishing
Reason: link/attachments takes user to fake/bogus website
website obtains personal/financial data
Minimised: do not open/click emails/attachments from unknown sources
some firewalls can detect fake/bogus websites

Risk: pharming
Reason: redirects user to fake/bogus website
redirection obtains personal/financial data
Minimised: only trust secure websites, e.g. look for https
check the URL matches the intended site

Risk: credit card fraud/identity theft
Reason: loss of money due to misuse of card/stealing data
Minimised: set passwords
encrypt data/encryption

Risk: cracking
Reason: illegal/unauthorised access to data
Minimised: setting strong passwords
encrypt data/encryption

Papacambridge

Q 4) Winter 2015 P13

(b) 1 mark for each CORRECT row

Statement	Firewall	Proxy server
Speeds up access of information from a web server by using a cache		✓
Filters all Internet traffic coming into and out from a user's computer, intranet or private network	✓	✓
Helps to prevent malware, including viruses, from entering a user's computer	✓	
Keeps a list of undesirable websites and IP addresses	✓	✓

(c) **one** mark for method + **one** mark for linked reason (maximum 6 marks)

– back up files…
– …on a regular basis / to another device / to the cloud

– set data to read only…
– …to prevent accidental editing

– save data on a regular basis…
– …to prevent loss / corruption of data in unexpected shutdown / failure

– use correct shut down / start up procedures…
– …to prevent damage to components / stored files

– use correct procedures before disconnecting portable storage device…
– …to prevent damage to device / data corruption

– keep storage devices in a safe place…
– …away from fire hazards

10 symmetric encryption

encryption key

plain text

encryption algorithm

cypher text

PapaCambridge

Q 5) Winter 2015 P11

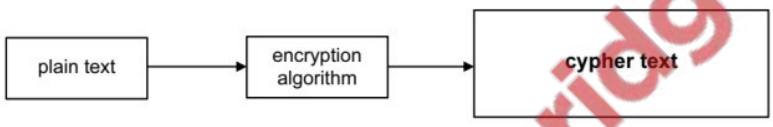
3 **(a)**

Statement	True	False
Cookies can destroy or modify data in a computer without the user's knowledge		✓
Cookies generate website pop-ups		✓
Cookies allow a website to detect whether a viewer has viewed specific web pages	✓	

6 **(a)** Any **one** from:
- jumbling up/scrambling characters so that message makes no sense
- requires an encryption key to encrypt data
- need decryption key to decipher encrypted message

(b) Uses the same key to encrypt and decrypt message

(c) 1 mark for correct name in box



Q 6) Summer 2016 P11 & P13

6 **(a)** Any **one** from:
- protocol ends in "s"
- use of http**s**

(b) Any **three** from:
- requests web server to identify itself/view the (SSL) certificate
- receives a copy of the (SSL) certificate, sent from the webserver
- checks if SSL certificate is authentic/trustworthy
- sends signal back to webserver that the certificate is authentic/trustworthy
- starts to transmit data once connection is established as secure
- if website is not secure browser will display an open padlock/warning message

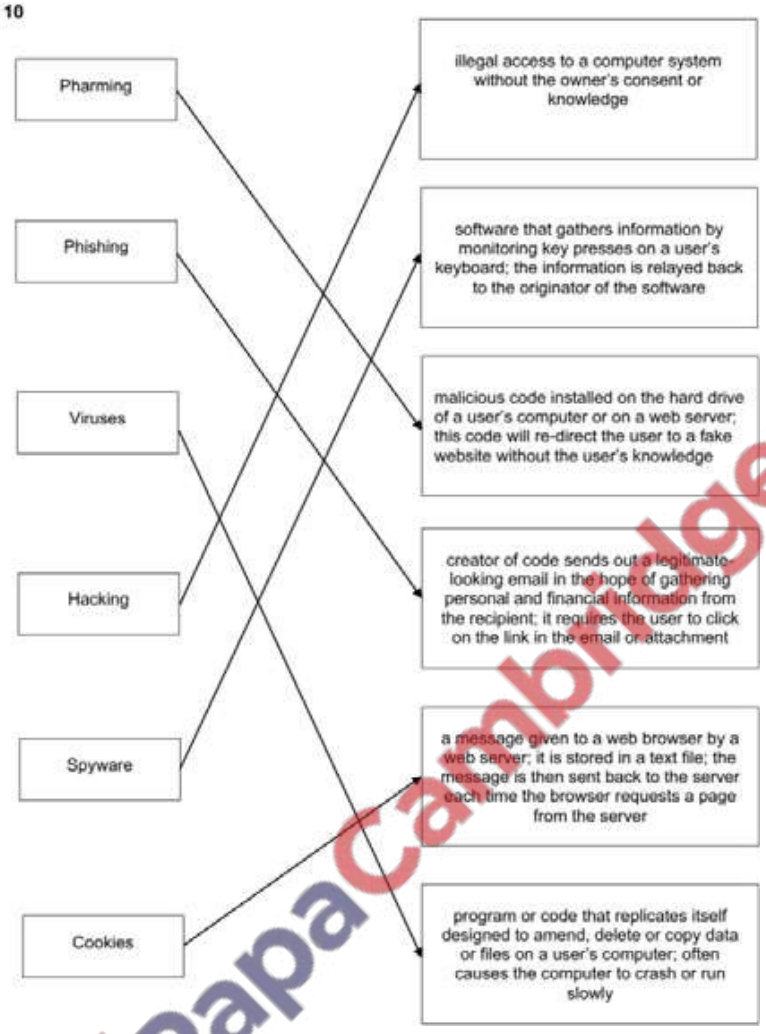
8 **(a)** **(i)** Any **two** from:
- to protect against key logging software/spyware
- can stop key presses being recorded
- can stop key presses being relayed
- drop down boxes cannot be recorded as key presses
- drop down boxes can be placed in different location on the screen each time (to overcome screen capture issues)

(ii) Any **one** from:
- hacker never finds all characters on the first hack
- makes it more difficult for hackers to find the order of the characters
- hacker needs to hack the system several times to gain the whole password
- shoulder surfing will not give person full password

(b) Any **two** from:
- fingerprint scanner
- face recognition software
- retina scanner/iris scanner
- voice recognition software

PapaCambridge

10



PapaCambridge

Q 7) Summer 2016 P12

(c) **2** marks for each term described

Viruses:
- program/software/file that replicates (copies) itself
- intends to delete or corrupt files//fill up hard disk space

Pharming:
- malicious code stored on a computer/web server
- redirects user to fake website to steal user data

Spyware:
- monitors and relays user activity e.g. key presses//key logging software
- user activity/key presses can be analysed to find sensitive data e.g. passwords [6]

(d) Any **three** from:
- examines/monitors traffic to and from a user's computer and a network/Internet
- checks whether incoming and outgoing traffic meets a given set of criteria/rules
- firewall blocks/filters traffic that doesn't meet the criteria/rules
- logs all incoming and outgoing traffic
- can prevent viruses or hackers gaining access
- blocks/filters access to specified IP addresses/websites
- warns users of attempts by software (in their computer) trying to access external data sources (e.g. updating of software) etc. // warns of attempted unauthorised access to the system [3]

Q 8) Winter 2016 P12

Page 4	Mark Scheme	Syllabus	Paper
	Cambridge IGCSE – October/November 2016	0478	12

5 **(a)** 112 [1]

(b) 56 [1]

(c) divided by 2 // value 112 was halved // multiplied by 0.5 [1]

(d) **(i)**

0	0	0	0	1	1	1	0

[1]

(ii) 14 [1]

(e) Any **two** from:
- run out of places to the right of register / at the end of register
- right-most 1 would be lost
- number would become 3 instead of 3.5
- loss of precision

[2]

PapaCambridge

9 **(a)** Any **two** from:

- a large number of requests are sent to the network/server all at once
- designed to flood a network/server with useless traffic/requests
- the network/server will come to a halt/stop trying to deal with all the traffic/requests
- prevents users from gaining access to a website/server

[2]

(b) 1 mark for each security threat and 1 mark for matching description

Security threat	Description
Viruses	– software that replicates – causes loss/corruption of data // computer may "crash"/run slow
Hacking/cracking	– illegal/ unauthorised access to a system/data
Phishing	– a link/attachment sends user to fake website (where personal data may be obtained)
Pharming	– malicious code installed on user's hard drive / computer – user is redirected to a fake website (where personal data may be obtained)
Spyware/key logger	– send/relay key strokes to a third party

[4]

Q 9) Winter 2016 P11& 13

2
- Hacking
- Virus
- Cookies
- Cracking
- Pharming

[5]

4

(c) 1 mark for security measure, 1 mark for description.

Any **two** from:

- Encryption
- If the data is accessed or stolen it will be meaningless

- Biometric device
- Can help prevents unauthorised access to the system (only award once)

- Firewall
- Can alert to show unauthorised access attempt on the system
- Can help prevent unauthorised access to the system (only award once)
- Can help protect against viruses and malware entering the system

- Anti-spyware
- Can stop the keys being logged that, when analysed, would reveal the password to the data

[4]

10

(d)
- record (layer)
- handshake (layer)

[2]

PapaCambridge

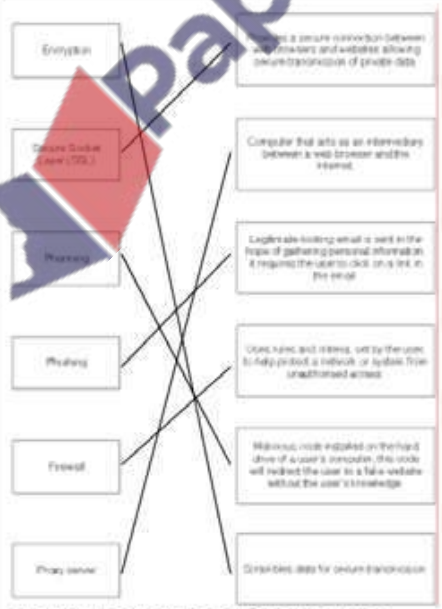
Q 10) March 2017 India

Question	Answer	Marks
4(a)	∞ a v m v e q n d i z m h (2 marks, 1 for each correct word)	2
4(b)	v w x y z a b c d e f g h i j k l m n o p q r s t u 2 marks ∞ shift right ∞ all characters shifted five places	2
4(c)	∞ the first cypher ∞ cannot deduce rest of cypher having identified some characters/more random substitution	2

Question	Answer	Marks
5	HTML – HyperText Markup Language / language used to create web pages http – hypertext transfer protocol / protocol used by web browsers https – hypertext transfer protocol secure / secure protocol used by web browsers	3

Question	Answer	Marks
9	Any **four** from, must include at least **one** difference: Text based password ∞ (a minimum number of) characters that can be typed at a keyboard ∞ set / can be changed by the user Biometric password ∞ a stored physical measurement e.g. fingerprint ∞ that is compared to a previously scanned human measurement Difference ∞ text based passwords are easier to hack than biometric passwords ∞ biometric passwords are unique to that person/cannot be shared	4

Q 11) Summer 2017 P11

Question	Answer	Marks
7	 1 mark for correct line till 5 marks given.	5

PapaCambridge

Q 12) Summer 2017 P12

Question	Answer	Marks
8(a)	2 marks for SSL, 2 marks for Firewall **SSL protocol** **Two** from: ∞ uses encryption ∞ encryption is asymmetric / symmetric / both ∞ makes use of (public and private) keys ∞ data is meaningless (without decryption key / if intercepted) **Firewall** **Two** from: ∞ helps prevent unauthorised access // helps prevent hacking ∞ checks that data meets criteria // identifies when data does not meet criteria ∞ acts as a filter for (incoming and outgoing) data // blocks any unacceptable data //allows acceptable data through	4

Question	Answer	Marks
8(b)	**Six** from: Encrypt the data … … so it cannot be understood by those not entitled to view it Password protected / biometrics … … to help prevent unauthorised access Virus checking software … … helps prevent data corruption or deletion … identifies / removes a virus in the system … scans a system for viruses Spyware checking software … … helps prevent data being stolen/copied/logged … scans a system for spyware Drop-down input methods / selectable features … … to reduce risk of spyware / keylogging Physical method e.g. locked doors / CCTV timeout / auto log off … to help prevent unauthorised access Network / company policies // training employees … to educate users how to be vigilant Access rights … … allows users access to data that they have permission to view … prevents users from accessing data that they do not have permission to view	6

PapaCambridge

Question	Answer	Marks
11	**Seven** from: **Requested** ∞ a web browser is used ∞ user enters the URL / web address (into the address bar) // clicks a link containing the web address // clicks an element of the webpage ∞ the URL / web address specifies the protocol ∞ protocols used are Hyper Text Transfer Protocol (HTTP) / Hyper Text Transfer Protocol Secure (HTTPS) **Sent** ∞ the URL / web address contains the domain name ∞ the Internet Service Provider (ISP) looks up the IP address of the company ∞ the domain name is used to look up the IP address of the company ∞ the domain name server (DNS) stores an index of domain names and IP addresses ∞ web browser sends a request to the web server / IP address **Received** ∞ Data for the website is stored on the company's web server ∞ webserver sends the data for the website back to the web browser ∞ web server uses the customer's IP address to return the data ∞ the data is transferred into Hyper Text Mark-up Language (HTML) ∞ HTML is interpreted by the web browser (to display the website)	7

Q 13) Winter 2017 P12

Question	Answer	Marks
5(a)	Any **four** from: ∞ Data / files ∞ Stored in a text file ∞ Downloaded to a user's computer when a website is visited // webserver sends to web browser ∞ Stored on a user's computer ∞ Stored by a browser ∞ Detected by the website when it is visited again	4
5(b)	Any **two** from: e.g. ∞ To store personal information/data ∞ To store login details ∞ To save items in an online shopping basket ∞ To track/save internet surfing habits // to track website traffic ∞ To carry out targeted advertising ∞ To store payment details ∞ To customise a webpage // to store user preferences ∞ Store progress in online games/quizzes	2

Question	Answer	Marks
6	1 mark for each correct term, in this order: ∞ Interrupt ∞ Compiler ∞ ALU/Arithmetic and Logic Unit ∞ ARQ/Automatic repeat request	4

PapaCambridge

10(a)	Any **three** from: ∞ It is a (security) protocol ∞ It encrypts data (sent over the web/network) ∞ It is the updated version of SSL ∞ It has two layers ∞ It has a handshake layer ∞ It has a record layer	3
10(b)	1 mark for each correct application, examples could include: ∞ Online banking ∞ Online shopping // Online payment systems ∞ Email ∞ Cloud based storage ∞ Intranet/extranet ∞ VPN ∞ VoIP ∞ Instant messaging (IM) // social networking	3

Q 14) Winter 2017 P13

Question	Answer	Marks
7	1 mark for each correct tick **Statement** / **true (✓)** / **false (✓)** Firewalls can monitor incoming and outgoing traffic. / ✓ / Firewalls operate by checking traffic against a set of rules. / ✓ / Firewalls cannot block access to a certain website. / / ✓ Firewalls can be software and hardware. / ✓ / Firewalls can act as intermediary servers. / / ✓ Firewalls can block unauthorised traffic. / ✓ /	6

Question	Answer	Marks
8(a)	Any **three** from: – Human error (e.g. deleting/overwriting data) – Physical damage – Power failure/surge – Hardware failure – Software crashing	3
8(b)	Any **three** from: – Online shopping // Online payment systems // Online booking – Email – Cloud based storage – Intranet/extranet – VPN – VoIP // video conferencing – Instant messaging (IM) // social networking // online gaming	3

PapaCambridge

Question	Answer	Marks
8(c)	1 mark for identifying, 1 mark for description – Strong password – To make it difficult to hack an account – Biometric device – To use data that is difficult to fake as a password – TLS // Encryption – To make data meaningless if intercepted – To encrypt data that is exchanged (TLS only) – More secure than SSL (TLS only) – Anti-spyware (software) – To find and remove any spyware that is installed on a computer – To help stop key loggers recording key presses – Firewall – To help prevent unauthorised access to an account – Blocks any requests that do not meet/match the criteria – Authentication (card reader at home)/mobile security code app/two-step verification – To add another level of identification of the user – Use of drop-down boxes (or equivalent) – So key loggers cannot record the key presses – Proxy server – To divert an attack away from the main system	6

Q 15) March 2018 P12 (India)

Question	Answer	Marks
2(a)	Any **three** from: Scans files for viruses // detects/identifies a virus Can constantly run in background Can run a scheduled scan Can automatically updating virus definitions Can quarantine a virus Can delete a virus Completes heuristic checking Notifies user of a possible virus	3

Question	Answer	Marks
2(b)	Any **three** from: Use a firewall Use of a proxy server Do not use / download software / files from unknown sources Do not share external storage devices / USB pens Do not open / take care when opening attachments / link Do not connect computer to network / use as stand-alone computer Limiting access to the computer	3

Question	Answer	Marks
3(a)	Byte 3 // 10110100	1
3(b)	Odd parity used Counted / added the number 1's // Most Bytes have an odd number of 1's Byte 3 has an even number of 1's // Byte 3 didn't follow odd parity	3

Q 16) Summer 2018 P11

10(c)	Any **two** from e.g. : – To store items that a customer has added to an online shopping basket – To store a customer's credit card details – To store log-in details – To track what product a customer browses // Track music preferences – Targeted advertising // making recommendations – Personalises/customises the experience – Shows who are new and returning customers – To speed up log-in times – To speed up/allow single click purchases – Improves the experience	2

PapaCambridge

Question	Answer	Marks
10(d)	Any **four** from: – Prevents direct access to the **webserver** // Sits between **user** and **webserver** – If an attack is launched it hits the proxy server instead // can be used to help prevent DDOS // help prevent hacking of **webserver** – Used to direct invalid traffic away from the webserver – Traffic is examined by the proxy server // Filters traffic – If traffic is valid the data from the webserver will be obtained by the user – If traffic is invalid the request to obtain data is declined – Can block requests from certain IP addresses	4

Q 17) Summer 2018 P12

12(a)(i)	Encryption	1

12(a)(ii)	Any **five** from: – Her personal details before encryption is the plain text – The plain text/her personal details is encrypted using an encryption algorithm – The plain text/her personal details is encrypted using a key – The encrypted text is cypher/cipher text – The key is transmitted **separately** (from the text) – The key is used to decrypt the cypher text (after transmission)	5
12(b)	Any **three** from a single error method: – Checksum – Calculation carried out on data – (checksum/calculated) value sent with data – recalculated after transmission **and** compared to original – If they do not match an error is present – ARQ – uses acknowledgment **and** timeout – A request is sent with data to acknowledge all data is received – Acknowledgement sent back to say all data is received – If no acknowledgement is received in a time frame an error in transmission detected / data automatically resent.	3

Q 18) Winter 2018 P12

Question	Answer	Marks
4(a)	**Three** from: ∞ Malware ∞ Virus // No antivirus ∞ Denial of service ∞ Spyware // No antispyware ∞ Phishing // opening unknown links/emails ∞ Pharming // opening unknown links/emails (only award once for this alternative) ∞ Hacking/cracking/unauthorised access // No/weak password // No/weak firewall ∞ Downloading/Using unknown software ∞ Not updating software ∞ Physical issue e.g. computer/door left unlocked	3
4(b)	**Four** from: ∞ It examines/monitors/filters traffic into **and** out of a computer ∞ It allows a user to set criteria/rules for the traffic ∞ It checks whether the traffic meets the criteria/rules ∞ It blocks any traffic that does not meet the criteria/rules // Blocks unauthorised access ∞ It warns a **user** of any unauthorised software/access/unauthorised outgoing traffic ∞ It keeps a log of all traffic (that can be examined)	4

PapaCambridge

Q 19) Winter 2018 P13

Question	Answer	Marks
6	1 mark for method name, 1 mark for description e.g. **Backups** ∞ Make a copy of the data ∞ Copy stored away from main computer ∞ Data can be restored from backup **Anti-virus** ∞ Scans computer for viruses ∞ Software to detect/remove viruses ∞ Can prevent data being corrupted by viruses **Firewall** ∞ Hardware or software that monitors network traffic ∞ To help prevent hackers gaining access / deleting data **Password/Biometrics** ∞ To help protect files / computer from unauthorised access **Restricted access** ∞ To stop users downloading/installing software that could harm **Verification** ∞ Message e.g. to ask if definitely want to delete **Physical methods** ∞ Locks/alarms/CCTV to alert/deter unauthorised access	6

Q 20) March 2019 P12

7	For each of **three** risks Naming the risk – 1 mark, describing the risk – 1 mark: – Hacking ... – ... when a person tries to gain unauthorised access to a computer system – ... data can be deleted/corrupted by hacker – Malware ... – ... a software program designed to damage data / disrupt the computer system – ... replicates itself and fills the hard disk – Virus ... – ... a program that replicates itself to damage / delete files NOTE: Multiple kinds of malware can be awarded if listed and given a matching description e.g. trojan horse, worm	6

Q 21) Summer 2019 P11

4(a)(i)	1 mark for security method, 2 marks for description **Anti-virus (software) // Anti-malware (software)** • Scans the computer system (for viruses) • Has a record of known viruses • Removes/quarantines any viruses that are found • Checks data before it is downloaded • ... and stops download if virus found/warns user may contain virus **Firewall // Proxy server** • Monitors traffic coming **into and out of** the computer system • **Checks** that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist	3

PapaCambridge

4(a)(ii)	1 mark for security method, 2 marks for description **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i)** **Passwords** • Making a password stronger // by example • Changing it regularly • Lock out after set number of attempts // stops brute force attacks // makes it more difficult to guess **Biometrics** • Data needed to enter is unique to individual • ... therefore very difficult to replicate • Lock out after set number of attempts **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • ... making it more difficult for hacker to obtain it • Data has to be entered into the same system • ... so if attempted from a remote location, it will not be accepted	**3**
4(a)(iii)	1 mark for security method, 2 marks for description **Anti-spyware software // Anti-malware (software)** • Scans the computer for spyware • Removes/quarantines any spyware that is found • Can prevent spyware being downloaded **NOTE: Anti-malware (software) cannot be awarded if already given in 4(a)(i)** **Drop-down boxes // onscreen/virtual keyboard** • Means key logger cannot collect data // key presses cannot be recorded • ... and relay it to third party **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • ... making it more difficult for hacker to obtain it • Data has to be entered into the same system • ... so if attempted from a remote location, it will not be accepted **NOTE: Cannot be awarded if already given in 4(a)(ii)** **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i) or 4(a)(ii)**	**3**
4(b)(i)	**Three** from: • Human error e.g. accidentally deleting a file • Hardware failure • Physical damage e.g. fire/flood • Power failure // power surge • Misplacing a storage device	**3**
4(b)(ii)	**Two** from: • Back data up • Use surge protection • Keep data in a fireproof / waterproof / protective case • Use verification methods (for deleting files) • Following correct procedure e.g. ejecting offline devices / regularly saving	**2**

PapaCambridge

6(a)	**Four** from (max 2 marks per improvement): • Make the password require more characters • Makes the password harder to crack/guess • More possible combinations for the password • Make the password require different types of characters • Makes the password harder to crack/guess • More possible combinations for the password • Use a biometric device • Hard to fake a person's biological data // data is **unique** • Two-step verification // Two factor-authentication • Adds an additional level to hack • Have to have the set device for the code to receive it • Drop-down boxes // onscreen keyboard • To prevent passwords being obtained using keylogger • Request random characters • Won't reveal entire password • Set number of password attempts • Will lock account if attempting to guess • Will stop brute-force attacks	4

8(a)	**Six** from: • SSL is a (security) protocol • It encrypts any data that is sent • It uses/sends digital certificates … • … which is sent to the (buyer's/user's) browser // requested by (buyer's/user's) browser • … that contains the gallery's public key • … that can be used to authenticate the gallery • Once the certificate is authenticated, the transaction will begin	6

8(b)	1 mark for each correct tick. **Statement** / **True (✓)** / **False (✓)** Firewalls are only available as hardware devices — False (✓) Firewalls allow a user to set rules for network traffic — True (✓) Firewalls will automatically stop all malicious traffic — False (✓) Firewalls only examine traffic entering a network — False (✓) Firewalls encrypt all data that is transmitted around a network — False (✓) Firewalls can be used to block access to certain websites — True (✓)	6
8(c)	**Four** from: • A set of guidelines • Rules/laws that govern the use of computers / by example • Tell people how to behave when using computers // helps keep users safe when using computers // by example • **Art gallery** could be subject to plagiarism / intellectual property theft • **Art gallery** could **copyright** their work (to make it illegal to steal it)	4

PapaCambridge

Q 22) Summer 2019 P12

<table>
<tr><td>5</td><td>– Password protection
– Password is released on the release date

– Encryption
– Encryption key is released on the release date</td><td>4</td></tr>
<tr><td>6(a)</td><td>Structure
– This is the layout of the web page
– e.g. placing an image alongside some text // example of tag, such as

Presentation
– This is the formatting/style of the web page
– e.g. the colour that is applied to some text // example of tag, such as <font-color></td><td>4</td></tr>
<tr><td>6(b)</td><td>1 mark per each correct row.

<table><tr><th>Statement</th><th>True (✓)</th><th>False (✓)</th></tr><tr><td>Cookies can be used to store a customer's credit card details</td><td>✓</td><td></td></tr><tr><td>Cookies can be used to track the items a customer has viewed on a website</td><td>✓</td><td></td></tr><tr><td>Cookies will corrupt the data on a customer's computer</td><td></td><td>✓</td></tr><tr><td>Cookies are downloaded onto a customer's computer</td><td>✓</td><td></td></tr><tr><td>Cookies can be deleted from a customer's computer</td><td>✓</td><td></td></tr></table></td><td>5</td></tr>
<tr><td>6(c)</td><td>– Several/multiple bits are transmitted at a time/simultaneously
– Several/multiple wires are used
– Data is transmitted in both directions …
– … at the same time/simultaneously</td><td>4</td></tr>
<tr><td>6(d)</td><td>One from:
– Uniform resource locator
– The website's address
– User friendly version of the IP address</td><td>1</td></tr>
<tr><td>6(e)(i)</td><td>Four from:
– Designed to deny people access to a website
– A large number/numerous requests are sent (to a server) …
– … all at the same time
– The server is unable to respond/struggles to respond to all the requests
– The server fails/times out as a result</td><td>4</td></tr>
<tr><td>6(e)(ii)</td><td>One from:
– Proxy server
– Firewall</td><td>1</td></tr>
</table>

PapaCambridge

Q 23) Winter 2019 P13

1(b)(i)	∞ Increase the length of the key // make key 12-bit, etc.	1
1(b)(ii)	∞ Cypher text	1

Question	Answer	Marks
1(b)(iii)	**Six** from: ∞ The system could use odd or even parity ∞ A parity bit is added ∞ The data is checked to see if it has incorrect/correct parity // by example ∞ If parity is correct no error is found ∞ An acknowledgement is sent that data is received correctly ∞ The next packet of data is transmitted ∞ If incorrect parity is found an error has occurred ∞ A signal is sent back to request the data is resent ∞ The data is resent until data is received correctly/timeout occurs	6

Question	Answer	Marks
6(a)	∞ Free software	1
6(b)	∞ Freeware	1
6(c)	∞ Shareware	1
6(d)	∞ Plagiarism // Intellectual property theft	1
6(e)	∞ Copyright	1

Question	Answer	Marks
8	**Four** from: ∞ A hacker could have hacked the network … ∞ … and downloaded the malware onto the network ∞ Clicking a link/attachment/downloaded a file from an email/on a webpage … ∞ … the malware could have been embedded into the link/attachment/file ∞ Opening an infected software package … ∞ … this would trigger the malware to download onto the network ∞ Inserting an infected portable storage device … ∞ … when the drive is accessed the malware is downloaded to the network ∞ Firewall has been turned off … ∞ … so malware would not be detected/checked for when entering network ∞ Anti-malware has been turned off … ∞ … so malware is not detected/checked for when files are downloaded	4

Q 24) Winter 2019 P12

Question	Answer	Marks
7(c)	**Three** from: ∞ Hypertext Transfer Protocol Secure // It is a protocol … ∞ … that is a set of rules/standards ∞ Secure version of HTTP ∞ Secure website // secures data ∞ Uses TLS / SSL ∞ Uses encryption	3

PapaCambridge

Question	Answer	Marks
10(a)	**Four** from: ∞ Validation method ∞ Used to check data entry ∞ Digit is calculated from data // by example ∞ Digit is appended / added to data ∞ Digit is recalculated when data has been input ∞ Digits are compared ∞ If digits are different, error is detected // If digits match, no error is detected	4
10(b)	**Six** from (maximum three marks per security method): ∞ Firewall … ∞ … Monitors the traffic ∞ … **Blocks** any traffic that doesn't meet the **criteria / rules** ∞ (Strong) password // biometric … ∞ … Data cannot be accessed without the use of the password / bio data ∞ … Prevent brute force attacks ∞ Encryption … ∞ … Data will be scrambled ∞ … **Key** is required to decrypt the data ∞ … If data is stolen it will be meaningless ∞ Physical security methods … ∞ … The physical security will need to be overcome ∞ … This can help deter theft of the data ∞ Antispyware … ∞ … will remove any spyware from system ∞ … will prevent data being relayed to a third party	6

Q 25) March 20 P12

Question	Answer	Mark
2(c)(i)	Any **two** from: • Scrambles data • … making it meaningless/unintelligible • Uses an algorithm / key • Data / plain text is changed to cipher text	2
2(c)(ii)	Any **one** from: • Increase the length of the key // use more than 128 bits • Uses a more complex encryption algorithm	1

PapaCambridge

Question	Answer	Mark
2(d)	Any **six** from (max **four** for identification of method only): • Backups • … if data is lost can be replaced • Install antivirus // Anti malware • … **detects/deletes viruses** that could **corrupt/delete** data • Install firewall • … helps prevent hackers gaining access **and** deleting/corrupting data • Password / Biometrics • Two factor authentication // two-step verification • … helps prevent unauthorised access **and** the deletion/corruption of data • Access rights • … helps prevent users accessing data they should not see **and** deleting it • Network/usage policy • … gives users guidance on data use // by example • Surge protection // Uninterrupted power supply (UPS) • … prevents loss of data that has not been saved • … prevents damage to hardware (that stores data) • Physical method // by example • … helps prevent unauthorised access **and** the deletion/corruption of data	6

Question	Answer	Mark
8(a)	Any **five** from: • **Sends** the URL of the website • … to a DNS to find the IP address • Connects to the webserver (using the IP address) … • … using HTTP / HTTPS • Renders/Translates the HTML • Runs active/client-side scripts built into webpages • **Manages** SSL/TLS certificate process • Stores/retrieves cookies	5
8(b)	Any **three** from: • **Webserver** is sent multiple requests // Requests flood the **webserver** … • … at the **same** time • **Webserver** crashes / runs slow • Designed to prevent access to e.g. a website // Stops legitimate requests being processed/serviced	3
8(c)(i)	• A **law/legislation** that requires permission to use intellectual property / other people's work	1
8(c)(ii)	Any **one** from: • To claim other's work as your own • To use other people's work without consent / acknowledgement • Theft of intellectual property	1

PapaCambridge

Q 26) Summer 20 P12

Question	Answer	Marks
3(a)	Any **four** from: – Encryption key is used – Encryption algorithm is used – Encryption key / algorithm is applied to plain text – … to convert it into cypher text – Same key is used to encrypt and decrypt the text	4
3(b)	Any **three** from: – Firewall – Password – Proxy server – Physical methods (by example e.g. CCTV, Locks) – Access rights – Asymmetric encryption – Disconnect from network	3

Question	Answer	Marks
5(a)	Any **three** from: – Convert HTML code – Display web pages – Check if a website is secure – Request web pages from a web server – Send URL/domain name – Runs active script – Store history/favourites/bookmarks – Create tabs	3

2210/12 Cambridge O Level – Mark Scheme PUBLISHED May/June 2020

Question	Answer	Marks
5(b)(i)	– Carries out authentication of server and client – Handles encryption algorithms / keys	2
5(b)(ii)	– Record layer	1
5(b)(iii)	Any **one** from: – SSL – HTTPS	1
5(c)	– Cookies	1

Question	Answer	Marks
10(a)	**One** mark for similarity, **two** marks for differences Similarity: – Both are designed to steal personal data – They both pose as a real company/person Differences: – Pharming uses malicious code installed on hard drive – Phishing is in form of an email – Phishing requires use to follow a link / open an attachment	3
10(b)	– Virus – Malware	2
10(c)(i)	– Incorrect	1
10(c)(ii)	Any **four** from: – Can help prevent hacking – Can monitor incoming and outgoing traffic – Can set criteria / rules are set for traffic – Can check whether traffic meets / defies criteria rules – Can rejects any traffic that does not meet / defies criteria	4

PapaCambridge

Q 27) 15a Summer 20 P11

7(a)(i)	Any **four** from: – Keylogger is downloaded without knowledge (by example) – Keylogger records key presses – Data is relayed back to third party – Data is analysed // Patterns in data could reveal log-in details … – … details can then be used to log into the account	4
7(a)(ii)	Any **one** from: – Use drop-down boxes for password – Two-step verification (by example) – Partial password requests – Onscreen / virtual keyboard	1
7(b)(i)	Any **one** from: – Look for locked padlock / green padlock – Check for https	1
7(b)(ii)	Any **four** from: – requests web server to identify itself // request to view the (SSL) certificate – receives a copy of the (SSL) certificate, sent from the webserver – checks if (SSL) certificate is authentic/trustworthy – sends signal back to webserver that the certificate is authentic/trustworthy	4

28) Winter 20 P12

1(d)(i)	– Handshake (layer) – Record (layer)	2

1(d)(ii)	Any **six** from: – **Client/browser** requests secure **connection** to server – **Client/browser** requests the **server** to identify itself – **Server** provides a digital certificate – **Client/browser** validates the certificate – **Client/browser** send signal **back to server** (to begin transmission) – Session caching can be used – A session key is generated – Encryption method is agreed // data is encrypted	6
1(e)(i)	Any **three** from: – Hacking – Denial of service (DoS) attack – Virus – Malware NOTE: Three different type of malware can be awarded	3
1(e)(ii)	Any **four** from: – Acts as a firewall – Monitor/filters/examines incoming **and** outgoing traffic – Rules/criteria for traffic can be **set** // blacklist/whitelist **set** – Blocks any traffic that does not meet criteria … – … and can send a warning message **to the user** – Stop the website failing in a DoS attack // DoS attack hits the proxy server and not the webserver	4

3(a)(i)	Any **three** from: – Loss of power/electricity – Spillage of liquids – Flood – Fire – Human error – Hardware failure – Software failure NOTE: Three different types of human error can be awarded e.g. accidental deletion, not saving data, incorrect shutdown procedure	3
3(a)(ii)	– Create a backup	1

PapaCambridge

3(b)	Max **three** from: – Solid state drive – Non-volatile – Secondary storage – Flash memory – Has no mechanical/moving parts – Uses transistors – … and cells that are laid out in a grid – Uses control gates and floating gates – Can be NAND/NOR (technology) – Use EEPROM technology Max **two** from: – Stores data by flashing it onto the chips – Data stored by controlling the flow of electrons **through/using transistors/chips/gates** – The electric current reaches the control gate and flows through to the floating gate to be stored – When data is stored the transistor is converted from 1 to 0	**4**

3(c)	**One** mark for each correct row:	**6**

Statement	Blu-ray (✓)	CD (✓)	DVD (✓)
A type of optical storage	✓	✓	✓
Has the largest storage capacity	✓		
Can be dual layer	✓		✓
Read using a red laser		✓	✓
Has the smallest storage capacity		✓	
Stores data in a spiral track	✓	✓	✓

Q 29) Winter 20 P13

4(a)	Any **four** from: – Browsers sends URL to DNS – … using HTTP – DNS finds matching IP addresses for URL – … and sends IP address to web browser – Web browser sends request to IP address/web server for web pages – Web pages are sent from web server to browser – Browser renders HTML to display web pages – Any security certificates are exchanged/authenticated // SSL/HTTPS is used to secure the data – … encrypting any data sent	**4**

4(b)	Any **three** from: – Hacking – Denial of service (DoS) – Malware – Virus NOTE: three suitable types of malware can be awarded	**3**

6	– Key // Algorithm – Algorithm // Key (must be opposite of first one) – Plain – Cypher – Key // Algorithm	**5**

PapaCambridge

13(a)	Any **one** from: – Both are designed to steal/collect personal data – Both pretend to be a real company – Both use fake websites	1
13(b)	– Phishing involves use of an email whereas pharming involves installing malicious code – Phishing involves clicking a link or an attachment whereas pharming creates a redirection	2

Q 30) March 21 P12

2(c)(i)	– Data if intercepted cannot be understood // Data is **encrypted** // Data is **scrambled** // uses keys to **encode/decode** data	1
2(c)(ii)	**Four** from: – Uses (digital) **certificates** – ….requested from web server by browser/client // browser/client asks web server to identify itself – Server send SSL/digital signature to browser/client – Client and server agree on encryption method to use – … that contains the server's public key – Browser checks **authenticity of certificate**… – … then session key is generated – … the transaction will begin // sends signal to server to start transmission	4
6(a)	Any **four** from: – Monitors incoming and outgoing traffic – Allows the **setting** of criteria/blacklist/whitelist/by example – Blocks access to signals that do not meet requirements/criteria/blacklist/whitelist … – … sends signal to warn the user – Restrict access to specific applications – Blocks entry/exit by specific ports	4
6(b)	**One** mark for risk, **two** marks for description – Phishing – **Legitimate looking email** sent to user – Clicking on **link/attachment** takes user to fake website – Pharming – Software is installed on user's computer – Redirects (correct URL) to different/fraudulent website – Spyware (accept keylogger but do not award for MP3) – Software is installed on user's computer – Records key strokes // keylogger – Transmits data to third part for analysis	6

PapaCambridge