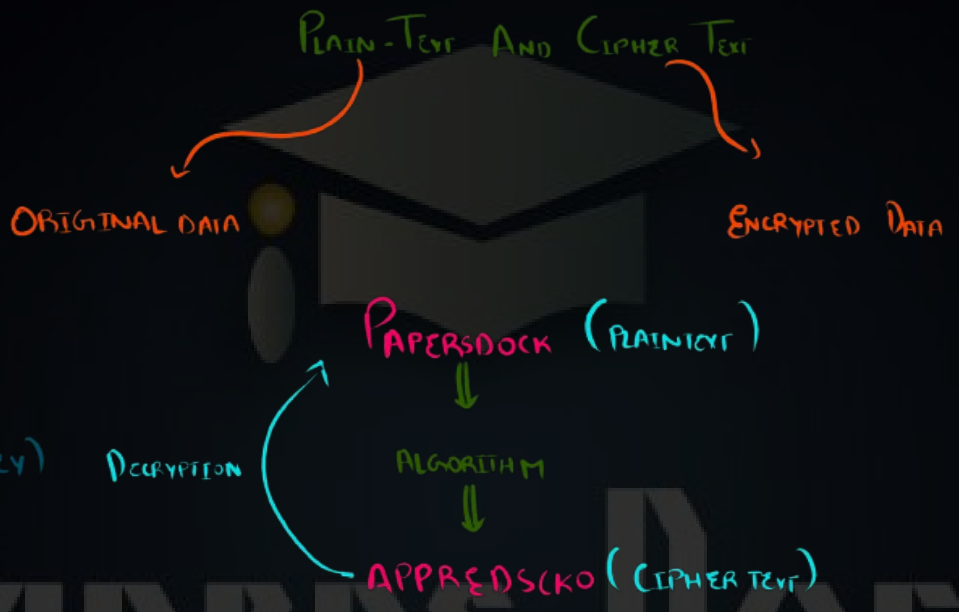
Security

COMPUTER SCIENCE 9618 PAPER 3

Security

Encryption: It alters data into a form that is unreadable by anybody for whom the data is not intended.
It does not stop the data from being intercepted, but it stops it from making any sense to hacker.

Process of turning plain text into cipher text.



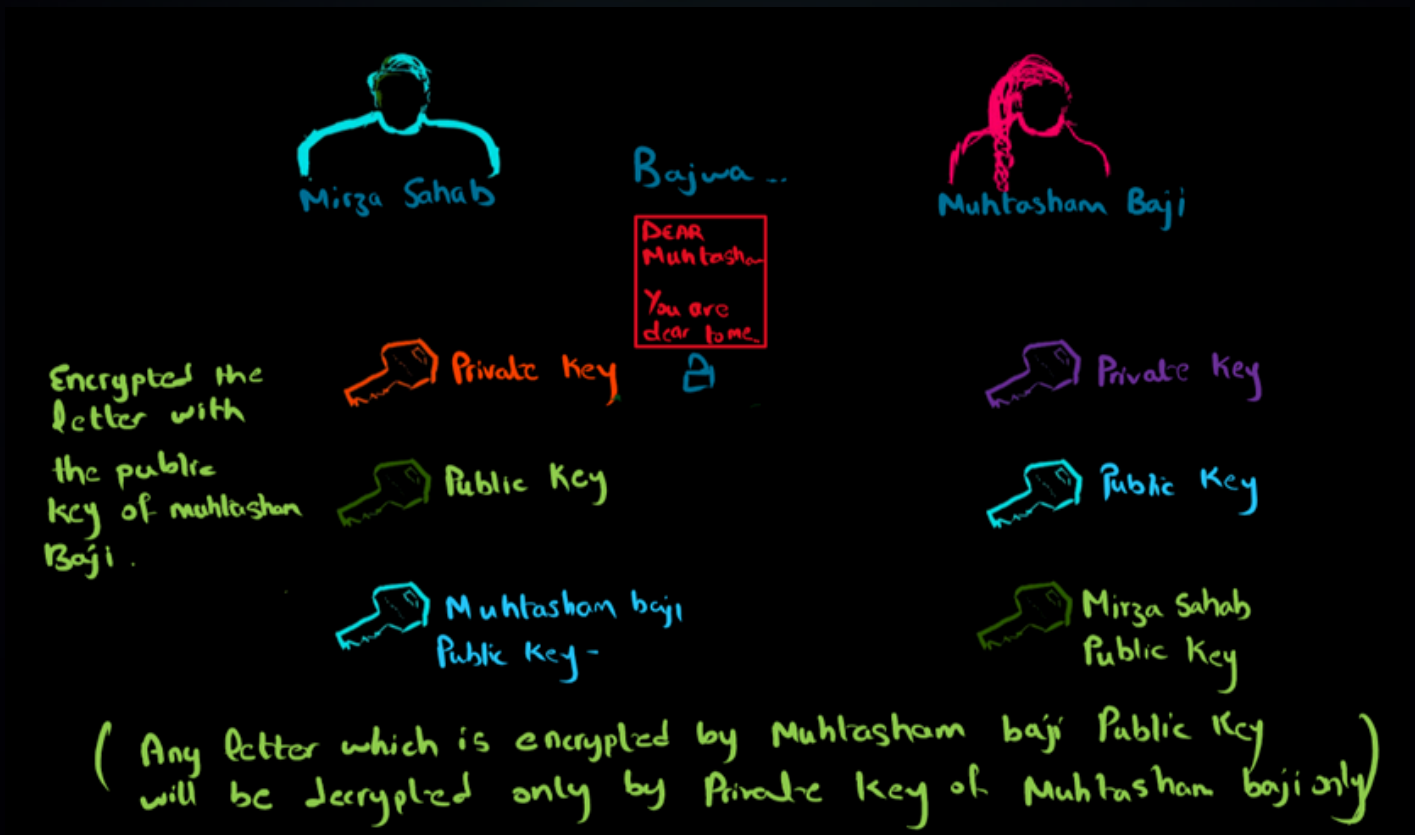
Types Of Encryption

Symmetric Encryption

Asymmetric Encryption

Symmetric Encryption

Asymmetric Encryption



Plain Text: Original Text.
Cipher Text: Encrypted version of the plain text.
Encryption: Process of turning plain text to cipher text.

Public Key: Key widely available that can be used to encrypt messages that only the owner of the private key can decrypt.

Private Key: Key needed to decrypt the data that has been encrypted by a public key and is used in Asymmetric encryption, and is not shared.

What are the similarities and differences between public key and private key?

Similarities:

- Both used in asymmetric encryption.
- A pair of keys is required.
- One is used to encrypt data and the other is used to decrypt the data.
- Both use hashing algorithm.

Differences:

- Private key is only known to the owner of the key pair, while the public key can be distributed to anyone.
- When messages are sent to the owner of the public key, they are encrypted with the owner's public key so they can only be decrypted by the owner's private key.
- Message digests are encrypted with the private key of the sender to form a digital signature, while messages are encrypted with the public key of the receiver.

Question: Explain how private key and public key are used to ensure that Ali Wajid is the only person who receives this email.?

- Sender's computer will encrypt the email before sending it by receiver's public key.
- Receiver will decrypt the email when it is received by using receiver's private key.
- As the private key is only known to the receiver, so only they can understand.

Question: Explain how asymmetric encryption is used to ensure that the message remains private?

- The sender will encrypt the message with the receiver's public key.
- The receiver will decrypt the message with their private key, so the message will remain private.

Question: Explain how the use of asymmetric key cryptography ensures that only a particular person (Person A) can read the email?

- Asymmetric encryption means that the key used to encrypt (public key) is different from the key used to decrypt (private key).
- Sender will acquire Person A's public key.
- Sender will encrypt the email using Person A's public key.
- Sender will send the encrypted email to Person A.
- Person A will decrypt the email using their private key.

Question: Give reasons for using key cryptography ?

- To ensure the message is authentic and it came from a trusted source
- To ensure that only the intended receiver is able to understand the message
- To ensure the message has not been altered during transmission
- Non-repudiation, neither the sender or receiver can deny the transmission occurred

Question: Give two methods of Key Cryptography that can be used ?

- Symmetric
- Asymmetric

Question: State two difference between symmetric and asymmetric encryption ?

- Symmetric cryptography uses a single key to encrypt and decrypt messages, Asymmetric cryptography uses two.
- The symmetric key is shared, whereas with asymmetric, only the public key is shared (and the private key isn't).
- the risk of compromise is higher with symmetric encryption and asymmetric encryption is more secure.
- Symmetric cryptography is a simple process that can be carried out quickly, but asymmetric is much more complex, so slower.
- The length of the keys in symmetric encryption are (usually) shorter than those for asymmetric.

Protocols

Secure Socket Layer (SSL) Transport Layer Security (TLS)

Secure Socket Layer

When a user logs onto a website, SSL encrypts the data and only the client's computer and the webserver are able to make sense of what is being transmitted.

Describe what happens when setting up a secure connection using SSL (Secure Socket Layer)

1) Browser requests that the server identifies itself

2) Server sends a copy of its SSL certificate and its public key.

3) Browser checks the certificate against a list of trusted certificate authorities.

4) If the browser trusts the certificate, it creates, encrypts, and sends the server a symmetric session key using the server's public key.

5) Server decrypts the symmetric session key using its private key.

6) Server sends the browser an acknowledgment encrypted with the session key

Explain how the customer's browser and the server which is used to collect the payment will establish a secure connection by SSL:

- Browser requests that the server identifies itself.
- Server sends a copy of its SSL certificate, containing the public key.
- Browser checks the certificate against a list of trusted certificate authorities.
- If the browser trusts the certificate, a symmetric session key is created.
- This is done by the browser and encrypted using the server's public key and sent to the server.
- Server decrypts the symmetric session key using its private key.
- Server and browser now encrypt all transmitted data with the session key.

Transport Layer Security

- Recent security protocol.
- More secure than SSL.
- Only some browsers have the capability to support TLS.
- So that's why SSL is widely used.
- It provides encryption, authentication, and data integrity in a more effective way.

TLS is formed of two main layers:

- **Record Protocol:** Can be used with or without encryption, it contains the data being transmitted over the network.

- **Handshake Protocol:** Permits the webserver and client to authenticate each other and to make use of encryption algorithms.

Difference Between SSL And TLS

- It is possible to extend TLS by adding new authentication methods, unlike SSL.
- TLS can make use of session caching, which improves the overall performance of the communication when compared to SSL.
- TLS separates the handshaking protocol from the record protocol, where the data is held.

What is Session Caching?

- When opening a TLS session, a lot of time is required due to its complex cryptographic process.
- So the existing session can be used again because of session caching

What is the purpose of TLS?

- Purpose of TLS is to provide secure communication over a network.
- Maintains data integrity.
- Provides an additional layer of security.
- TLS provides improved security over SSL.
- It is composed of two layers: record protocol and handshake protocol.
- TLS protects information by using encryption.
- Also allows for authentication of servers and clients.

Application of TLS

- Online Banking
- Private Email
- Online Shopping
- Online Messaging

What are the problems that SSL and TLS can overcome?

- Security: e.g., alteration of transmitted messages.
- Privacy: e.g., only the intended receiver can view data.
- Authentication: e.g., trust in the other party.

What are the problems that SSL and TLS can overcome?

- Security: e.g., alteration of transmitted messages.
- Privacy: e.g., only the intended receiver can view data.
- Authentication: e.g., trust in the other party.

There are certain security parameters that are agreed on between server and client during handshake ?

1) Which protocol will be used?

- As there are a number of different versions of the two protocols.

2) Session ID

- Uniquely identifies a related series of messages between server and client.

3) Session type

- Reusable or not.

4) Encryption method

- Asymmetric/Symmetric.

5) Authentication method

- Use of digital certificate or use of digital signature.

Describe the purpose of the secure sockets layer(SSL) and Transport Layer Security (TLS) protocols ?

- The SSL and TLS protocols provide communications security over the internet
- they provide encryption
- They enable two parties to identify and authenticate each other
- and communicate with confidentiality and integrity.

Explain how SSL/TLS protocols are used when a client-server communication is initiated?

- An SSL/TLS connection is initiated by an application
- which becomes the client
- The application which receives the connection becomes the server
- Every new session begins with a handshake (as defined by the (SSL/TLS) protocols)
- The client requests the digital certificate from the server and the server sends the digital certificate to the client
- The client verifies the server's digital certificate
- and obtains the server's public key
- The encryption algorithms are agreed
- The symmetric session keys are generated

Digital Signature And Digital Certificate

There is a letter that Mirza Sahab has written for Muhtasham Baji

Abba ji prepared a hate letter and threw that love letter in bin

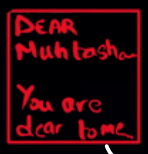
Sends this letter as Mirza Sahab to Muhtasham

Mirza Sahab Confused

Abba Rock
Mirza Shock

Problem : The receiver can not make sure that the message / data is altered

Solution

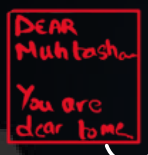


Hashing Algorithm Produces Hash Key Known As Digest

Encrypts Digest (Hash Key) (5F) with Mirza (Sender) Private Key

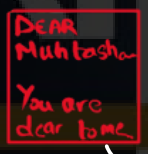
Encrypts the letter with public key of Muhtasham baji

Sends Encrypted Letter and the Encrypted Digest



Decrypts the letter with her Private Key.

Muhtasham Baji now have two things. Decrypted letter and Hash Key Decrypted by Public Key of Mirza



Pass the same letter in the same hashing algorithm

Makes her own new Hash key by using the letter

New Hash Key = Decrypted Hash Key

Means No Alteration

- Sender hashes the letter with the agreed hashing algorithm
- which provides hash key
- That hash key is encrypted with sender's private key
- Sender sends encrypted letter with hash key known as message digest
- Receiver already has public key of sender (from the digital certificate)
- Receiver decrypts the hash key with public key of sender.
- Receiver after decrypting that letter, passes that letter to same hashing algorithm.
- If decrypted hash key and new hash key done by receiver is same then the letter is authentic.

What is the difference between digital certificate and digital signature?

- Certificate is obtained from an issuing authority
- Signature created from a message

- Certificate provides authentication of owner
- Signature used to authenticate message that are sent by the owner

- Certificate remains unchanged while it is valid
- New signature is created for every message

- Only signature makes use of private key and does not provide information
- Only certificate provides extra information and does not use private key

Question: What is the purpose of digital signature?

- To ensure a document is authentic/came from a trusted source
- To ensure a document has not been altered during transmission
- Non-repudiation

Is the assurance that someone cannot deny the validity of something.

Explain how a digital signature is produced before the message is sent ?

- The message is hashed with the agreed hashing algorithm
- to produce a message digest
- The message digest is then encrypted with the sender's private key to form the digital signature

Explain how the digital signature can be checked on receipt to ensure that the message has not been altered during transmission?

- The message together with the digital signature is decrypted using the receiver's private key
- The digital signature received is decrypted with the sender's public key to recover the message digest sent
- The decrypted message received is hashed with the agreed hashing algorithm to reproduce the message digest of the message received
- The two message digests are compared
- if they are the same the message has not been altered and if they are different the message has been altered

Describe what is meant by a digital certificate?

- A digital certificate is an electronic document.
- Used to authenticate the identity the online identity of an individual/organization.
- Typically issued by a CA.
- For example: it contains information identifying a website owner/individual and a public key.

Question: How digital certificate is obtained?

- Enquiry made to Certificate Authority (CA)
- Enquirer's details checked by CA
- If enquirer details verified by CA then public key is agreed
- CA creates/issues certificate that includes the enquirer's public key
- Encrypting data sent by CA with the CA's public key

Question: Explain the role of a digital certificate in creating a digital signature ?

- The digital certificate provides the public key
- that can be used to validate the private key associated with the organisation/website/digital signature.

Verification → Working of digital signature

Privacy → Encryption working

Question: Explain how Asymmetric Encryption is used to ensure that it is a verified message?

- The sender creates the message digest
- Receiver recreates the message digest
- If both copies of the message digest match, then the message has not been altered.

Question: Explain how asymmetric encryption uses the contents of digital certificate to ensure that the message has not been altered during transmission?

- Sender's message is encrypted with receiver's public key which is provided by the digital certificate of the receiver.
- Agreed hashing algorithm mentioned in digital certificate is used on the message to produce the message digest.
- The message digest is then encrypted with sender's private key to provide a digital signature.
- Both the encrypted message and the digital signature are sent.
- The message is decrypted with receiver's private key.
- Sender's digital signature is decrypted with sender's public key (which is provided by the digital certificate of sender) to obtain the message digest.
- Using the same hashing algorithm the receiver recreates the message digest.
- The two message digests are compared. If they are same, then the message is not altered.

Quantum Cryptography

Quantum Physics : Is the study of matter and energy at its most fundamental

Photons : Are the smallest possible packets of electromagnetic energy and they carry visible light

Knowledge Only No Need To Memorize

A Quantum Computer is a new type of computer that uses the rules of quantum physics to solve problems much faster than regular computers. Instead of using tiny switches that are either on (1) or off (0) like normal computers, quantum computers use qubits, which can be both 1 and 0 at the same time. Scientists are exploring different ways to build these computers, such as using tiny superconducting circuits or trapped atoms. Although still in development, quantum computers could help solve big problems in science, medicine, and security in the future.

Due to advancement in technologies, the concept of quantum computers have been introduced which will easily be able to crack all the encryption keys.

Fight Quantum With Quantum

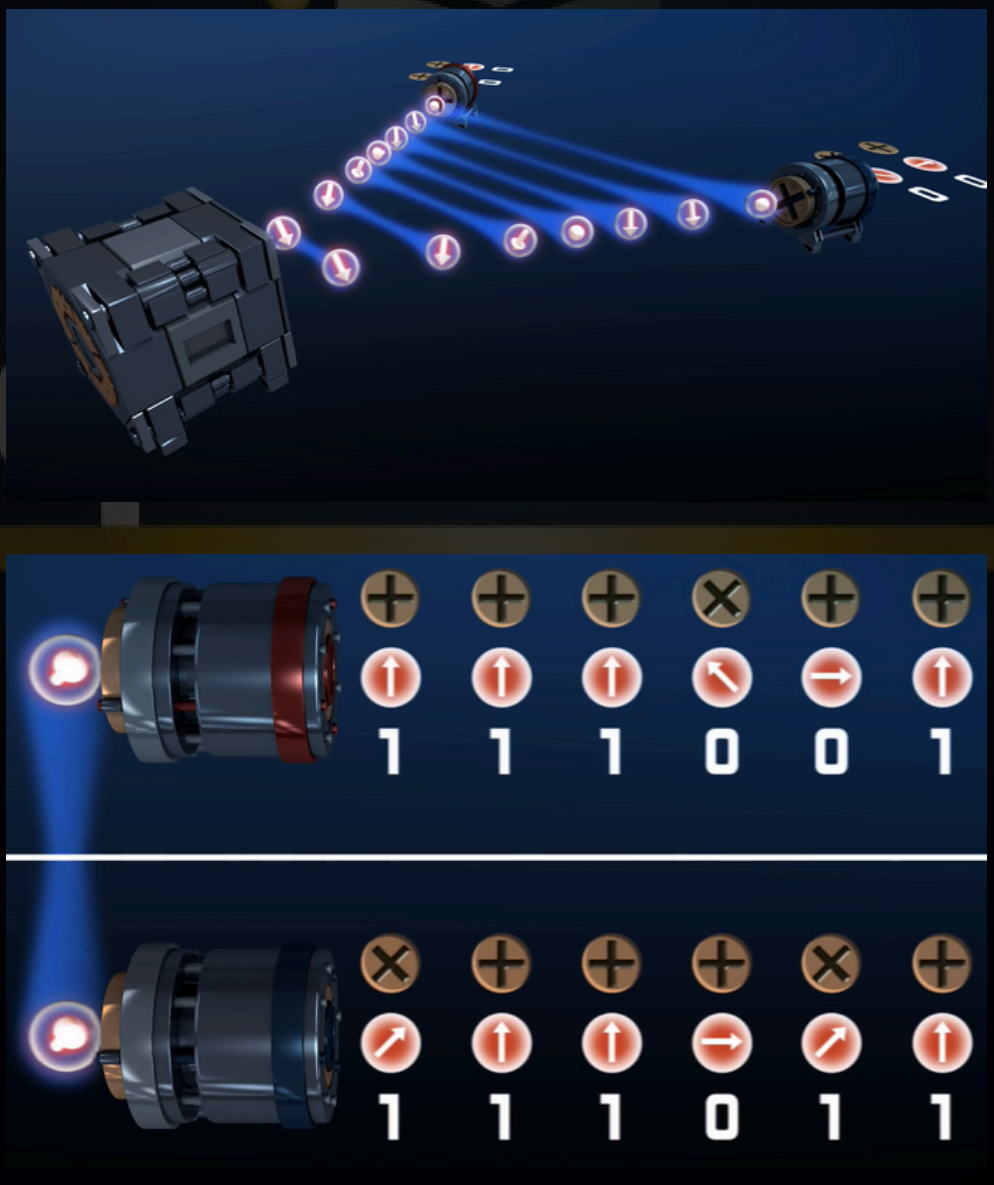
Problem

- Random numbers generation of the code can easily be broken by Quantum Computers.
- Current key distribution techniques will not stand up to a quantum computer.

Solution

- QKD (Quantum Key Distribution

Explanation




ALICE
0 0 0 0 0 1 1 1 1 1 0 0 1 1 0 0 1 0 1 1 1 0 0 1 0 0 1 0 0 0
BOB
1 0 0 0 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 0 1 1 0 0


ALICE
0 0 0 1 1 0 0 1 1 1 0 1 1 1 0 0 0
BOB
0 0 0 1 1 0 0 1 1 1 0 1 1 1 0 0 0


ALICE
0 0 0 1 1 0 0 1 1 1 1 0 0 0
BOB
0 0 0 1 1 0 0 1 1 1 1 0 0 0
SECURE ENCRYPTION KEY


ALICE
QUANTUM KEY GENERATOR
BOB
EAVESDROPPER

- The sender generates photons using a light source.
- Photons are polarized randomly using one of four possible orientations.
- The polarization determines the bit value (0 or 1).
- The photons travel through a fiber optic cable to the receiver.
- The receiver uses a random beam splitter (filter) to measure the photons.
- There are two types of filters: rectilinear (|, —) and diagonal (/,).
- The receiver sends back the sequence of filters used.
- The sender compares this with the original polarization sequence.
- Only correctly measured bits are kept to form the encryption key.
- Incorrectly measured bits are discarded.
- If an eavesdropper intercepts, the quantum state changes, making spying detectable.
- Once synchronized, the encryption key is used for secure communication.

Purpose Of Quantum Cryptography

- To produce a virtually unbreakable encryption system and send virtually un-hackable secure messages
- using the laws principles of quantum mechanics and properties of photons
- Detects eavesdropping
- because the properties of photons change
- To protect the security of data transmitted over fibre optic cables
- To enable the use of longer keys.

Benefits Of Quantum Cryptography

- Any eavesdropping can be identified (as the state will be changed)
- Integrity of the key once transferred can be guaranteed (cannot be copied and decrypted at a later date)
- more secure and longer keys can be exchanged
- Almost unhackable
- The performance of Quantum cryptography is continuously improved

Drawbacks Of Quantum Cryptography

- Limited range
- Requires dedicated fibre (optic) line and specialist hardware
- Cost of dedicated fibre (optic) line and specialist hardware is expensive
- Polarization of light may be altered whilst travelling down fibre optic cables
- Lacks many vital features such as digital signature, certified mail, etc.
- Error rates are relatively high as technology is still being developed.
- Allows criminals and terrorists to hide their communication

Security

Question 1

8 Martha wants to send a private message to Joshua over the Internet.

(a) Martha and Joshua's computers have already exchanged digital certificates.

Identify **three** items that could be contained in a digital certificate.

1 .....

.....

2 .....

.....

3 .....

.....

[3]

(b) Joshua and Martha's digital certificates are used to ensure that Martha's message has not been altered during transmission.

Explain how asymmetric encryption uses the contents of the digital certificates to ensure that the message has not been altered during transmission.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question 2

6 Anita is studying computer science and she is confused about some of the computer security terminology as some of the words are similar.

Anita wants to know the similarities (features that are the same) and differences (features that are different) between some of the terms.

(a) Give the similarities **and** differences between a **public key** and a **private key**.

Similarities .....

.....

.....

.....

.....

Differences .....

.....

.....

.....

.....

[4]

(b) Give the similarities **and** differences between a **digital certificate** and a **digital signature**.

Similarities .....

.....

.....

.....

.....

Differences .....

.....

.....

.....

.....

[4]

Question 3

7 Sam wants to send confidential data to an organisation. He has already received the organisation's digital certificate. The organisation has asked him to make sure that the message containing the confidential data is encrypted and is sent with a digital signature.

(a) Explain the process the organisation followed to obtain its digital certificate.

.....

.....

.....

.....

.....

..... [3]

(b) Identify **two** items included in the organisation's digital certificate that will be used when sending the message. Give a reason why each item is required.

Item 1 .....

Reason .....

.....

Item 2 .....

Reason .....

.....

[4]

(c) Identify **two** other items included in the organisation's digital certificate.

.....

.....

.....

..... [2]

(d) Explain how the digital signature for Sam's message is produced.

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 4

5 **(a)** Wiktor is an employee of a travel agent. He uses asymmetric encryption to send confidential information to his manager.

Fill in the spaces with an appropriate term to complete the descriptions.

Asymmetric encryption uses different ..... for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into ..... using his manager's ..... key. When the manager receives the message, it is decrypted using her ..... key.

When the manager replies, the message is encrypted using Wiktor's ..... key, and when Wiktor receives the message, it is decrypted into ..... using his ..... key. [5]

(b) When customers pay for their travel booking online, a secure connection is established using Secure Socket Layer (SSL).

Explain how the customer's browser and the server used to collect the payment will establish a secure connection.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question 5

5 Sanjeet is a member of the public, and he wants to send a private message to a government department.

(a) Explain how asymmetric encryption is used to ensure that the message remains private.

.....

.....

.....

..... [2]

(b) When the government department replies to Sanjeet, it needs to send a verified message.

Explain how asymmetric encryption can be used to ensure that it is a verified message.

.....

.....

.....

.....

.....

..... [2]

Question 6

8 Digital certificates are used in internet communications. A Certificate Authority (CA) is responsible for issuing a digital certificate.

(a) Identify **two** data items present in a digital certificate.

1 .....

2 .....

[2]

(b) The following paragraph describes how a digital signature is produced. Complete the paragraph by inserting an appropriate term in each space.

A ..... algorithm is used to generate a message digest from the plain text message. The message digest is ..... with the sender's ..... .

[3]

Question 7

1 **(a)** The following incomplete table shows descriptions relating to the security of data transmission.

Complete the table with the appropriate terms.

	Description	Term
A	The original data to be transmitted as a message	.....
B	An electronic document from a trusted authority that ensures authentication	.....
C	An encryption method produced by a trusted authority that can be used by anyone	.....

[3]

(b) **(i)** Explain the purpose of a digital signature.

.....

.....

.....

..... [2]

(ii) Describe how a digital signature is produced for transmission with the message.

.....

.....

.....

.....

.....

.....

..... [3]

Question 8

(b) A customer downloads a new educational software package from the company.

Explain how the customer's and the company's computers use a hashing algorithm to assure the customer that:

- the software has come from the company (is authentic) and
- no one has altered it.

.....

.....

.....

.....

.....

.....

.....

.....[4]

Question 9

5 Katarina works for a company specialising in the sale of computer parts and accessories. She works in the London office and her colleague Lucy works in the Hong Kong office. Katarina emails confidential information to Lucy so that only Lucy can read the information.

(a) Explain how public and private keys are used to ensure that only Lucy has a readable copy of the confidential information.

.....

.....

.....

.....

.....

.....

.....

.....[4]

(b) Julio is buying items from the online shop. He already has an account with the shop.

Explain how the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) helps to keep Julio's confidential information secure.

.....

.....

.....

.....

.....

.....[3]

Question 10

6 **(a)** The following table shows descriptions and terms relating to data transmission security.

Add appropriate descriptions and terms to complete the table.

	Description	Term
A	The result of encryption that is transmitted to the recipient.	.....
B	The type of cryptography used where different keys are used; one for encryption and one for decryption.	.....
C	....	**Digital certificate**
D	....	**Private key**

[4]

(b) The sequence of steps 1 to 7 describes what happens when setting up a secure connection using Secure Socket Layer (SSL).

Four statements are missing from the sequence.

A	If the browser trusts the certificate, it creates, encrypts and sends the server a symmetric session key using the server's public key.
B	Server sends the browser an acknowledgement, encrypted with the session key.
C	Server sends a copy of its SSL Certificate and its public key.
D	Server decrypts the symmetric session key using its private key.

Write **one** letter (**A** to **D**) in the appropriate space to complete the sequence.

1. Browser requests that the server identifies itself.
2. .....
3. Browser checks the certificate against a list of trusted Certificate Authorities.
4. .....
5. .....
6. .....
7. Server and browser now encrypt all transmitted data with the session key.

[3]

Question 11

(c) 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.

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	....

[4]

Question 12

(c) Digital certificates are used in internet communications. A Certificate Authority (CA) is responsible for issuing a digital certificate.

The digital certificate contains a digital signature produced by the CA.

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

1 .....

2 .....

3 .....

[3]

(ii) Describe how the digital signature is produced by the CA.

.....

.....

.....

.....

.....

.....[3]

(iii) Give the reason for including a digital signature in the digital certificate.

.....

.....[1]

Question 13

4 The Secure Socket Layer (SSL) protocol and its successor, the Transport Layer Security (TLS) protocol, are used in Internet communications between clients and servers.

(a) (i) Define the term **protocol**.

.....

.....

.....

..... [2]

(ii) Explain the purpose of the TLS protocol.

.....

.....

.....

.....

.....

..... [3]

(b) A handshake process has to take place before any exchange of data using the TLS protocol. The handshake process establishes details about how the exchange of data will occur. Digital certificates and keys are used.

The handshake process starts with:

- the client sending some communication data to the server
- the client asking the server to identify itself
- the server sending its digital certificate including the public key.

Describe, in outline, the other steps in the handshake process.

.....

.....

.....

.....

.....

..... [3]

(c) Give **two** applications where it would be appropriate to use the TLS protocol.

1 .....

.....

2 .....

.....

[2]

Question 14

2 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]

(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]

Question 15

(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]

Question 16

4 Both clients and servers use the Secure Socket Layer (SSL) protocol and its successor, the Transport Layer Security (TLS) protocol.

(a) (i) What is a protocol?

.....

.....

.....

..... [2]

(ii) Name the client application used in this context.

..... [1]

(iii) Name the server used in this context.

..... [1]

(iv) Identify **two** problems that the SSL and TLS protocols can help to overcome.

1 .....

2 ..... [2]

(b) Before any application data is transferred between the client and the server, a handshake process takes place. Part of this process is to agree the security parameters to be used.

Describe **two** of these security parameters.

1 .....

.....

.....

.....

2 .....

.....

.....

..... [4]

(c) Name **two** applications of computer systems where it would be appropriate to use the SSL or TLS protocol. These applications should be different from the ones you named in **part (a)(ii)** and **part (a)(iii)**.

1 .....

.....

2 .....

..... [2]

Question 17

(c) Explain the following terms:

Encryption .....

.....

.....

.....

Public key .....

.....

.....

.....[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]

Question 18

8 **(a)** Describe the purpose of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

.....

.....

.....

.....

..... [2]

(b) Explain how SSL/TLS protocols are used when a client-server communication is initiated.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 19

8 A message is to be sent securely. Software uses a key to encrypt the message before it is sent.

(a) **(i)** Give **two** reasons for using key cryptography.

1 .....

.....

2 .....

.....

[2]

(ii) Give **two** methods of key cryptography that can be used.

1 .....

2 .....

[2]

(b) When there is a secure exchange of key(s), the message is sent.

The use of quantum cryptography is being considered for the secure exchange.

(i) State **two** possible benefits of using quantum cryptography.

1 .....

.....

.....

2 .....

.....

.....

[2]

(ii) State **two** possible drawbacks of using quantum cryptography.

1 .....

.....

.....

2 .....

.....

.....

[2]

Question 20

7 A digital signature is used to validate the authenticity of an electronic message.

In order to produce a digital signature, a digital certificate is required.

(a) State how a digital certificate is obtained.

.....

.....

.....

.....

.....

..... [3]

(b) (i) Explain how a digital signature is produced before the message is sent.

.....

.....

.....

.....

.....

.....

.....

..... [3]

(ii) Explain how the digital signature can be checked on receipt to ensure that the message has not been altered during transmission.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 21

6 A message is encrypted using a private key and sent to an individual using asymmetric encryption.

(a) State what is meant by a **private key**.

.....

.....

.....

..... [2]

(b) Describe the process of asymmetric encryption.

.....

.....

.....

..... [2]

(c) Explain how a digital signature is used to verify a message when it is received.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 22

6 **(a)** State **two** differences between symmetric and asymmetric encryption.

.....

.....

.....

..... [2]

(b) Explain the process by which an organisation may acquire its digital certificate.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question 23

9 **(a)** Encryption is used to alter data into a form that makes it meaningless if intercepted.

Describe the purpose of asymmetric key cryptography.

.....

.....

.....

..... [2]

(b) Identify **two** benefits and **two** drawbacks of quantum cryptography.

Benefit 1 .....

.....

Benefit 2 .....

.....

Drawback 1 .....

.....

Drawback 2 .....

.....

[4]

Question 24

5 **(a)** Encryption is used to scramble data to make it meaningless if intercepted.

Describe the purpose of quantum cryptography.

.....

.....

.....

..... [2]

(b) Explain the differences between symmetric and asymmetric cryptography when encrypting and decrypting data.

.....

.....

.....

.....

.....

..... [3]

Question 25

7 **(a)** Describe what is meant by a digital certificate.

.....

.....

.....

.....

.....

..... [3]

(b) Explain the role of a digital certificate in creating a digital signature.

.....

.....

.....

..... [2]

Question 26

4 Sheila has a customer called Fred. Fred wants to send Sheila a confidential document as part of a transaction.

Explain how Fred uses asymmetric encryption to send his document securely.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answers

Answer 1

8(a)	Any **three** from: • a hashing algorithm • a public key • serial number • dates valid	**3**
8(b)	Any **six** from: • Martha's message is encrypted using Joshua's public key (provided by Joshua's digital certificate). • Martha's hashing algorithm is used on the message to produce the message digest. • The message digest is then encrypted with Martha's private key to provide a digital signature. • Both the encrypted message and the digital signature are sent. • The message is decrypted with Joshua's private key. • Martha's digital signature is decrypted with Martha's public key (provided by the Martha's digital certificate) to obtain the message digest. • Martha's hashing algorithm (provided by the Martha's digital certificate) recreates the message digest from the decrypted message. • The two message digests are compared, if they are the same then the message should be authentic/has not been tampered.	**6**

Answer 2

6(a)	**Three** marks similarities, **three** marks differences max 4 Similarities: any **three** from Both used in <u>asymmetric</u> … encryption … as a pair of keys is required … one is used to encrypt the data/message and the other is used to decrypt the data/message Both hashing algorithms Differences: any **three** from Private key **only** known to owner of the key pair …The public key can be distributed to anyone When messages are sent to the owner of a public key, they are encrypted with the **owners public key** …so they can only be decrypted by the **owner's private key** Message digests are encrypted with the **private key of the sender** to form a digital signature … messages are encrypted with the **public key of the receiver**	**4**

6(b)	**Three** marks similarities, **three** marks differences max 4 Similarities: any **three** from Both used for authentication Both are unique to the **owner/subject** Include / use owner's public key include / make use of hash algorithm Differences: any **three** from Certificate obtained from issuing authority … signature created from a message Certificate provides authentication of owner …Signature used to authenticate messages that are sent by the owner Certificate remains unchanged whilst it is valid …new signature created for every message Only certificate provides extra information Only signature makes use of a private key	**4**

Answer 3

7(a)	Any **three** from Applied to an issuing certificate authority / CA … with some proof of identity … (for example) name of organisation / address of organisation etc … so their identity can be checked by an organisational registration authority / ORA … so that a digital certificate will only be issued to a trusted organisation	**3**
7(b)	**one** mark for item, **one** mark for reason; must relate to item Max 4 Item: public key Reason: to encrypt / decrypt data Item: agreed encryption/hashing algorithm Reason: to produce hash total / message digest	**4**
7(c)	Any **two** from Serial number Name of subject/organisation Date valid from/to Signature to verify it came from the issuers Name of issuer Purpose of the public key Thumbprint algorithm Thumbprint/fingerprint for the hash CA digital signature	**2**
7(d)	Any **four** from Message is put through agreed hashing / encryption algorithm … to produce a hash total / message digest then the message digest / hash total is encrypted … with Sam's private key … … this is now his digital signature	**4**

Answer 4

5(a)	**1 mark** per bullet point ∞ Keys ∞ Cipher text ∞ Manager's public and private keys in correct spaces ∞ Wiktor's public and private keys in correct spaces ∞ Plain text Asymmetric encryption uses different **keys** for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into **cipher text** using his manager's **public** key. When the manager receives the message, it is decrypted using her **private** key. When the manager replies, the message is encrypted using Wiktor's **public** key, and when Wiktor receives the message, it is decrypted into **plain text** using his **private** key.	**5**
5(b)	**1 mark** per bullet point (**max 6**) ∞ Browser requests that the server identifies itself ∞ Server sends a copy of its (Digital) Certificate ∞ … containing its public key ∞ Browser checks the certificate ∞ …against a list of trusted Certificate Authorities ∞ If the browser trusts the certificate ∞ … a symmetric session key is created ∞ …this is (by the browser) encrypted using the server's public key and sent to the server ∞ Server decrypts the symmetric session key ∞ … using its private key ∞ Server and browser now encrypt all transmitted data with the session key	**6**

Answer 5

5(a)	**1 mark** per bullet point ∞ Sanjeet's computer/software encrypts the message with the government department's public key ∞ The government department's computer/software decrypts the message with their private key	**2**
5(b)	**1 mark** per bullet point (max 2) ∞ The government department's computer/software creates the message digest ∞ Sanjeet's computer/software recreates this message digest ∞ If both copies of the message digest match the message has been verified	**2**

Answer 6

8(a)	**1 mark** per bullet point to **max 2** • Serial number • Identification of Certificate Authority (that issued the certificate) • Version (number) • Valid from // start date • Valid to // end date • Subject name (name of user/owner/computer/network device) • Subject's public key • Hashing algorithm • Algorithm used to create signature • Algorithm used to hash certificate • Hashed certificate	**2**
8(b)	**1 mark** for each correct term A **hashing** algorithm is used to generate a message digest from the plain text message. The message digest is **encrypted** with the sender's **private key**.	**3**

Answer 7

1(a)	1 mark per correct row **A** — The original data to be transmitted as a message — **Plain text** **B** — An electronic document from a trusted authority that ensures authentication — **Digital certificate** **C** — An encryption method produced by a trusted authority that can be used by anyone — **Public key**	**3**
1(b)(i)	1 mark per bullet point to **max 2** • To ensure a document is authentic // came from a trusted source • To ensure a document has not been altered during transmission • Non repudiation	**2**
1(b)(ii)	1 mark per bullet point to **max 3** • The message is hashed with the agreed hashing algorithm … • … to produce a message digest • The message digest is encrypted with the sender's private key… • … so the digital signature can be decrypted with sender's public key	**3**

Answer 8

6(b)	**1** mark per bullet to max **4** ∞ software is put through a hashing algorithm by the company ∞ hash total is encrypted with the company's private key ∞ company sends software and encrypted hash ∞ customer is in possession of company's public key (from the digital certificate) ∞ customer decrypts the received hash with public key ∞ customer hashes the received software with the hash algorithm (from the digital certificate) ∞ if decrypted hash and the software hash match, the software has come from the company/is authentic and has not been altered.	**4**

Answer 9

5(a)	**1** mark per bullet to max **4** • Katarina's computer/software encrypts the email before she sends it • using Lucy's public key • Lucy's computer/software decrypts the email when it is received • using Lucy's private key • As the private key is known only to Lucy, only she can understand the email	**4**
5(b)	**1** mark per bullet to max **3** • Julio's computer/software checks the digital certificate of the online shop's website • If digital certificate is invalid his computer/software rejects website • If valid a session is created/the transaction can continue • The encryption algorithms to be used are agreed • The session keys to be used are generated • The (session) key is used to encrypt the data sent	**3**

Answer 10

6(a) 1 mark for each term/description

	Description	Term
A	**The result of encryption that is transmitted to the recipient**	Cipher text
B	**The type of cryptography where different keys are used, one for encryption and one for decryption.**	Asymmetric or Public key
C	Electronic document used to prove the ownership of a public key // Electronic document used to prove that the data is from a trusted source	**Digital certificate**
D	Key needed to decrypt data that has been encrypted by a public key // Key needed to encrypt data so that it that can be decrypted by a public key // the key used in asymmetric encryption which is not shared	**Private key**

6(b)	1 mark for **C** in the correct place 1 mark for **A** followed by **D** in any position 1 mark for **D** followed by **B** in any position 1 Browser requests that the server identifies itself **2 C** 3 Browser checks the certificate against a list of trusted Certificate Authorities **4 A** **5 D** **6 B** **7** Server and Browser now encrypt all transmitted data with the session key

Answer 11

2(c)(i)	public	**1**
2(c)(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	**2**
2(c)(iii)	**The person performing the action** / **What that person does** Anna – Requests Bob's **public** key. Bob – Sends Anna his public key. 1 Anna – Encrypts email with Bob's public key. 1 Anna – Sends the email to Bob. Bob – Decrypts email. 1 Using his private key. 1	**4**

Answer 12

2(c)(i)	(Certificate) serial number 1 Certificate Authority (that issued certificate) 1 Valid date(s) // Date of expiry 1 Subject name (name of user/owner, computer, network device) 1 Subject public key 1 Version (Number) 1 Hashing algorithm (data or signature) 1 **max 3**	**3**
2(c)(ii)	CA uses hashing algorithm .. 1 To generate a message digest from the particular certificate 1 Message digest is encrypted with CA's private key 1	**3**
2(c)(iii)	Need to know that the certificate is genuine (and has not been altered) // Authenticate or verify it (came from the CA)	**1**

Answer 13

4(a)(i)	A (known) set of rules 1 Agreed/standard method for data transmission // governs how two devices communicate 1	**2**
4(a)(ii)	**Max 2 marks** for purpose: ∞ Purpose of TLS is to provide for secure communication (over a network) ∞ maintain data integrity ∞ additional layer of security **Max 2 marks** for further explanation from: ∞ TLS provides improved security over SSL ∞ TLS is composed of two layers / record protocol and handshake protocol ∞ TLS protects this information by using encryption ∞ Also allows for authentication of servers and clients	**Max 3**
4(b)	∞ The client validates (the server's) TLS Certificate ∞ The client sends its digital certificate (to the server if requested) ∞ Client sends an encrypted message to the server using the server's public key ∞ The server can use its private key to decrypt the message … ∞ … and get data needed for generating symmetric key ∞ Both server and client compute symmetric key (to be used for encrypting messages) // session key established ∞ The client sends back a digitally signed acknowledgement to start an encrypted session ∞ The server sends back a digitally signed acknowledgement to start an encrypted session **1 mark** for each point, **max 3** points	**3**
4(c)	Applications, for example: ∞ online banking ∞ private email ∞ online shopping ∞ online messaging etc. **1 mark** for each point, **Max 2**	**2**

Answer 14

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	**A mark for each correct data item –** **Max 3**

(b) (i)	Public The individual keeps their private key private // the public key can be known by others (the public)	**1** **1**
(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	**1** **1**
(iii)	Private 'Only' the CA's public key will allow decryption of the Certificate // proving the certificate was issued by the CA	**1** **1**
(c) (i)	Digital signature	**1**
(ii)	Alexa's digital certificate (Includes) Alexa's public key Used to hash message received // produce message digest Generated hash compared to digital signature	**1** **1** **1** **1** **Max 2**
(iii)	Examples: Financial transaction Legal document Software distribution	 **1** **1** **1** **Max 2**

Answer 15

(b) (i) Plain text is the original text [1]

Cipher text is the encrypted version of the plain text [1]

(ii) Asymmetric keys means that the key used to encrypt (public key) is different from the key used to decrypt (private key) [1]
Ben acquires Mariah's public key [1]
Ben encrypts email … [1]
using Mariah's public key [1]
Ben sends encrypted email to Mariah [1]
Mariah decrypts email … [1]
Using her private key [1]

[Max 4]

Answer 16

4 **(a)** **(i)** A set of rules … [1]
governing communications/transmission of data /sending and receiving data [1]

(ii) For example, (Web) browser / email client [1]

(iii) For example, Web server / email server [1]

(iv) Security //example: for example, alteration of transmitted messages [1]
Privacy // for example, only intended receiver can view data [1]
Authentication // for example, trust in other party [1]

[Max 2]

(b) For example:

which protocol will be used… [1]
there are a number of different versions of the two protocols [1]
session ID … [1]
uniquely identifies a related series of messages between server and client [1]
session type … [1]
reusable or not [1]
encryption method … [1]
public / private keys to be used // asymmetric/ symmetric [1]
authentication method … [1]
use of digital certificates / use of digital signature [1]
compression … [1]
method to be used [1]

[Max 2 parameters]

[Max 4]

(c) For example:

banking [1]
private / secure email [1]
shopping [1]
financial transactions [1]
secure file transfer [1]

[Max 2]

Answer 17

(c)	**encryption**: process of turning plain text into cipher text **public key**: key widely available that can be used to encrypt message that only owner of private key can decrypt // can be used to decrypt a message thereby confirming originator of message	1 1
(d) (i)	digital signature	1
(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	Any **four** points 1 mark each

Answer 18

Question	Answer	Marks
8(a)	**One** mark for each correct marking point **(Max 2)** • The SSL and TLS protocols provide communications security over the internet / network • … they provide **encryption** • They enable two parties to identify and authenticate each other • … and communicate with confidentiality and integrity.	**2**
8(b)	**One** mark for each correct marking point **(Max 4)** • An SSL/TLS connection is initiated by an application • … which becomes the client • The application which receives the connection becomes the server • Every new session begins with a handshake (as defined by the (SSL/TLS) protocols) • The client requests the digital certificate from the server // the server sends the digital certificate to the client • The client verifies the server's digital certificate • …and obtains the server's public key • The encryption algorithms are agreed • The symmetric • … session keys are generated / defined	**4**

Answer 19

Question	Answer	Marks
8(a)(i)	Any **two** from • To ensure the message is authentic // came from a trusted source • To ensure that only the intended receiver is able to **understand** the message • To ensure the message has not been altered **during transmission** • Non-repudiation, neither the sender or receiver can deny the transmission occurred	**2**
8(a)(ii)	Symmetric Asymmetric	**2**
8(b)(i)	Any **two** from • Any eavesdropping can be identified (as the state will be changed) • Integrity of the key once transferred can be guaranteed (cannot be copied and decrypted at a later date) • Longer/more secure keys can be exchanged	**2**
8(b)(ii)	Any **two** from • Limited range • requires dedicated fibre (optic) line and specialist hardware • cost of dedicated fibre (optic) line and specialist hardware is expensive • polarisation of light may be altered whilst travelling down fibre optic cables	**2**

Answer 20

Question	Answer	Marks
7(a)	Any **three** from MP1 enquiry made to Certificate Authority (CA) MP2 enquirer's details checked by CA MP3 if enquirer details verified by CA then public key is agreed MP4 CA creates/issues certificate that includes the enquirers public key MP5 encrypting data sent to/by CA with the CA's public/private key	**3**
7(b)(i)	MP1 The **message** is hashed with (the agreed hashing algorithm)… MP2 … to produce a message **digest** MP3 The message **digest** is then encrypted with the sender's private key to form the digital signature	**3**
7(b)(ii)	Any **four** from MP1 The message together with the digital signature is decrypted using the receiver's private key MP2 The digital signature received is decrypted with the sender's public key to recover the message digest sent MP3 The decrypted message received is hashed with the agreed hashing algorithm to reproduce the message digest of the message received MP4 The two message digests are compared MP5 … if they are the same the message has **not** been altered // if they are different the message has been altered	**4**

Answer 21

Question	Answer	Marks
6(a)	**One** mark for each correct point (**Max 2**) • A private key is the unpublished/secret key/never transmitted anywhere. • It has a matching public key • It is used to decrypt data that was encrypted with **its** matching public key.	**2**
6(b)	**One** mark for each correct point (**Max 2**) • The message to be sent is encrypted using the **recipient's public** key. // The message to be sent is encrypted using the **sender's private** key. • The message is decrypted using the **recipient's private** key. // The message is decrypted using the **sender's public** key.	**2**
6(c)	**One** mark for each correct point (**Max 4**) • The message together with the digital signature is decrypted using the receiver's private key • The digital signature received is decrypted with the sender's public key to recover the message digest sent • The decrypted message received is hashed with the agreed hashing algorithm to reproduce the message digest of the message received • The two message digests are compared • … if **both digests** are the same the message has **not** been altered // if they are different the message has been altered.	**4**

Answer 22

Question	Answer	Marks
6(a)	**One** mark for each point • Symmetric encryption uses a single key and asymmetric encryption uses a pair of keys. • The symmetric single key is used by all, whereas only one of the keys for asymmetric encryption is available to everyone / one of the asymmetric encryption keys needs to be kept secret.	**2**

Question	Answer	Marks
6(b)	**One** mark for each point (**Max 4**) • The organisation requests a certificate from a Certificate Authority (CA) • The organisation may send their public key to CA • The organisation gathers all the information required by the CA in order to obtain their certificate, which includes information to prove their identity • The CA verifies the organisation's identity • The CA generates / issues the certificate including the organisation's public key (and other information).	**4**

Answer 23

Question	Answer	Marks
9(a)	**One** mark per mark point (**Max 2**) MP1 To provide better security MP2 … by using two different keys / a public key and a private key MP3 One of the keys is used to encrypt the message MP4 … the **matching key** is used to decrypt the message.	**2**
9(b)	**One** mark per benefit (**Max 2**) MP1 Provides security based on laws of physics rather than mathematical algorithms, so more secure. MP2 To protect the security of data transmitted over fibre optic cables. MP3 Virtually unhackable. MP4 The performance of quantum cryptography is continuously improved, making it suitable for most valuable government/industrial secrets. MP5 Longer keys can be used MP6 Eavesdropping can be detected **One** mark per drawback (**Max 2**) MP1 Lacks many vital features such as digital signature, certified mail, etc. MP2 High cost of purchasing / maintaining equipment required. MP3 Currently only works over relatively short distances. MP4 Error rates are relatively high as technology is still being developed. MP5 Polarisation of light can change during transmission. MP6 Allows criminals and terrorists to hide their communications.	**4**

Answer 24

Question	Answer	Marks
5(a)	**One** mark per mark point (**Max 2**) MP1 to produce a **virtually unbreakable** encryption system / send **virtually un-hackable** secure messages … MP2 …using the laws / principles of quantum mechanics / properties of photons MP3 detects **eavesdropping** … MP4 …because the properties of photons change MP5 to protect security of data transmitted over **fibre optic cables** MP6 to **enable** the use of longer keys.	**2**
5(b)	**One** mark per mark point (**Max 3**) MP1 Symmetric cryptography uses a single key to encrypt and decrypt messages, Asymmetric cryptography uses two. MP2 The symmetric key is shared, whereas with asymmetric, only the public key is shared (and the private key isn't). MP3 … the risk of compromise is higher with symmetric encryption and asymmetric encryption is more secure. MP4 Symmetric cryptography is a simple process that can be carried out quickly, but asymmetric is much more complex, so slower. MP5 The length of the keys in symmetric encryption are (usually) shorter than those for asymmetric (128/256 bits v 2048 bits).	**3**

Answer 25

Question	Answer	Marks
7(a)	**One** mark per point (**max 3**) MP1 A digital certificate is an electronic/online document. MP2 used to authenticate/prove the identity of a website/the online identity of an individual/organisation MP3 typically issued by a CA MP4 For example: it contains information identifying a website owner/individual and a public key	3
7(b)	**One** mark per point (**max 2**) MP1 The digital certificate **provides the public key** MP2 … that can be used to validate the private key associated with the organisation/website/digital signature	2

Answer 26

Question	Answer	Marks
4	**One** mark per mark point (**Max 4**) MP1 Sheila's computer uses an algorithm to generate a matching pair of keys private and public MP2 Sheila's computer sends Fred's computer Sheila's public key // Fred's computer acquires Sheila's public key MP3 Fred's computer encrypts the document/plain text using Sheila's public key to create cipher text MP4 Fred's computer sends the **cipher text** to Sheila's computer The cipher text can only be decrypted using Sheila's private key // Sheila's computer uses Sheila's private key to decrypt the cipher text.	4