Past-paper walk-through

Encryption, Encryption Protocols and Digital Certificates ▪ 17.1

eXercise

Questions in this set

- 9618/32 N25 Q7 ▪ 5 marks
- 9618/33 N25 Q9 ▪ 4 marks
- 9618/11 J25 Q7 ▪ 11 marks
- 9618/31 J25 Q9 ▪ 4 marks
- 9618/32 J25 Q10 ▪ 4 marks
- 9618/33 J25 Q7 ▪ 4 marks

Reading the mark scheme

- **B1** a mark that stands on its own – the point is either made or not.
- **M1** a *method* mark: the right approach, even if the number is wrong.
- **A1** an *answer* mark, and it usually needs its M mark first.
- **C1** a working mark on the way to the answer.
- // separates answers the examiner accepts equally.
- **ecf** = error carried forward: a later part is marked on your own earlier answer.
- **owtte** = "or words to that effect" – the wording need not match.

Question 7

9618/32 N25 ▪ Q7 ▪ 5 marks

(a) Asymmetric encryption is a type of cryptography.
Identify **one** other type of cryptography. **[1]**

(b) An organisation holds two asymmetric encryption keys, which they intend to use to receive secure transmissions.
Explain how the organisation makes use of the two keys to receive a secure transmission. **[4]**

Solution 7

(a)

Mark scheme

- One from
- Symmetric (cryptography / encryption)
- Quantum (cryptography)

Solution 7

(b) Mark scheme

- One mark per mark point (Max 4)
- MP1
- The two keys held by the organisation are a private key and a public key
- MP2
- The organisation makes the public key available to anyone who wishes to send them secure transmissions // The sender obtains the organisation's public key
- MP3

Solution 7

- The sender uses the organisation's public key to encrypt the message / plain text // The sender uses the organisation's public key to turn the message into cipher text
- MP4
- The organisation uses its private key to decrypt the message.

Question 9

9618/33 N25 ▪ Q9 ▪ 4 marks

A company requires a digital certificate to ensure the authenticity of its online communications.

Outline the process followed to acquire a digital certificate. **[4]**

Solution 9

- One mark per mark point (Max 4)
- MP1 the company generates a public and private key pair locally using a web browser and an RSA key generator tool, which may be part of the CA's web page
- MP2 the company requests a digital certificate from a Certificate
- Authority (CA)
- MP3 the CA responds with its public key and digital certificate,
- MP4
- ... signed with its private key

Solution 9

- MP5 the company gathers authentication information e.g. its public key
- MP6
- ... and sends it to the CA signed with the company's private key and encrypted with the CA's public key
- MP7 the CA verifies the received information and generates/issues the digital certificate.

Question 7

9618/11 J25 ▪ Q7 ▪ 11 marks

A banker stores personal data on their work computer.

(a) The banker needs to transfer confidential data across the internet.

Identify and describe **one** method of restricting the risks posed by an unauthorised person intercepting the data whilst it is being transferred across the internet.

Description **[3]**

(b) The banker receives confidential data across the internet. The data includes a digital signature.

Explain how a digital signature can make sure the data has **not** been changed during transmission. **[5]**

(c) The data that is transferred can also be verified using a checksum.

Explain how data can be verified using a checksum. **[3]**

Solution 7

(a) Mark scheme

- 1 mark for a correct method:
- 1 mark each to max 2 for a corresponding description
- Method: Encryption
- Description:
- ▪ Data is encoded/scrambled using a key to create cipher text
- ▪ if intercepted it cannot be understood
- ▪ without being decrypted using a key

Solution 7

(b) Mark scheme

- 1 mark each to max 5
- ▪ The sender hashes the document / message
- ▪ to produce a digest
- ▪ The sender encrypts the digest to create the digital signature
- ▪ The message and the signature are sent to the banker / receiver
- ▪ The receiver decrypts the signature to reproduce the digest
- ▪ The receiver uses the same hashing algorithm on the document received to produce a second digest

Solution 7

- The receiver compares this digest with the one from the digital signature
- If both of the receiver's digests are the same the document has not changed

Solution 7

(c)

Mark scheme

- 1 mark each to max 3
- ▪ The data is put through an algorithm to create a checksum value
- ▪ The data and checksum are sent to the receiver
- ▪ The receiver performs the same algorithm on the data
- ▪ if both checksums match the data is verified

Question 9

9618/31 J25 ▪ Q9 ▪ 4 marks

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two protocols.

(a) State **two** functions of SSL/TLS.

1. 2. **[2]**

(b) Give **two** examples of situations where the use of SSL/TLS would be appropriate.

1. 2. **[2]**

Solution 9

(a)

Mark scheme

One mark for each mark point (Max 2)

- MP1 Ensure security/privacy when using the internet
- MP2 Data encryption
- MP3 Identification / authentication of client and server

Solution 9

(b)

Mark scheme

One mark for each mark point (Max 2)

- MP1 When transmitting authentication data e.g. passwords, session cookies
- MP2 When transmitting data that must be protected from modification on its way to or from a server e.g. user input, or results from the server
- MP3 When transmitting data classified as non-public.

Question 10

9618/32 J25 ▪ Q10 ▪ 4 marks

Identify the **two** main protocols that form Transport Layer Security (TLS) **and** state the purpose of each.

Protocol 1

Protocol 2 **[4]**

Solution 10

- One mark for identifying a protocol and one mark for stating its purpose
- MP1
- Handshake protocol
- MP2
- To establish a secure and reliable connection between two devices, systems or networks // Permits the web server and client to authenticate each other to make use of encryption algorithms
- MP3

Solution 10

- Record protocol
- MP4
- Provides a secure and reliable way to send and receive data over a network // To exchange records between the client and server // Responsible for securing application data end ensuring its integrity and authenticity during transmission // Encrypts and authenticates data exchanged between a client and a server // Deals with the format for data transmission.

Question 7

9618/33 J25 ▪ Q7 ▪ 4 marks

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two protocols. Explain how SSL/TLS is used when client-server communication is initiated. **[4]**

Solution 7

- One mark for each correct marking point (Max 4)
- MP1
- An SSL/TLS connection is initiated by an application/client.
- MP2
- Every new session begins with a handshake as defined by the SSL/TLS protocols.
- MP3
- The client requests the digital certificate from the server // The server sends the digital certificate to the client.

Solution 7

- MP4
- The client verifies the server's digital certificate
- MP5
- ... and obtains the server's public key.
- MP6
- The encryption algorithms are agreed. // The symmetric session keys are generated/defined.
- MP7
- A secure session is established between client and server.