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 **Description** / **Term** **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