SOLUTIONS

Module:	Security and Authentication		
Module Code	EBU714U	Paper	A
Time allowed	2hrs	Filename	Solutions_1617_EBU714U_A
Rubric	ANSWER ALL FOUR QUESTIONS		
Examiners	Dr Yasir Alfadhl	Dr Michael Chai	

[NOTE FOR MARKERS: 1 mark for every underlined statement unless otherwise stated]

Question 1

a) Answer the following questions: **[7 marks]**

i) Within the context of security requirements, define **confidentiality** and explain which security mechanisms can achieve it. (2 marks)

ii) Consider the scenario of an e-commerce website like *Taobao* where customers can register an account and purchase items online with secure transactions. Give examples of the security services the system should provide in terms of confidentiality, integrity, access control, availability and non-repudiation. (5 marks)

Answers:

i) Confidentiality: preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorised disclosure of information. [1 mark]

Encryption can achieve confidentiality. [1 mark]

ii) The website must keep the account information confidential, both in the server and during the transaction [1 mark]. It must protect the integrity of account information/purchase information. [1 mark] The website should ensure that only authorised users can login and purchase items. If a user is registered as seller then the user can sell items. [1 mark] The website should be available to users at all times [1 mark] Non-repudiation means a user cannot deny a purchase after the transaction is done. [1 mark]

b) Answer the questions below about *one-time pad:* **[12 marks]**

i) One-time pad is a stream cipher. What is a stream cipher? (2 marks)

ii) A one-time pad uses the XOR function (⊕) as an encryption and decryption method. Given a plaintext of 11010 and key stream of 01110, what's the ciphertext? (2 marks)

iii) What is a brute-force attack? Is one-time pad vulnerable to brute-force attack? Explain your answer. (8 marks)

Answers:
i) Stream Cipher: Process one input element [1 mark] at a time. [1 mark]
ii) 10100 [2 marks]
iii) Brute-force attack is a technique of attack - The attacker tries every possible key [1 mark] on a piece of ciphertext until an intelligible translation into plaintext is obtained. [1 mark]
One-time pad is not vulnerable to brute-force attack.[1 mark]

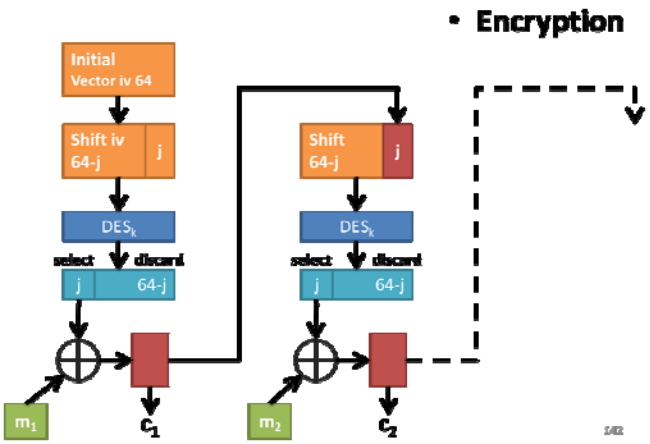
One-time pad use a new random key for each message [1 mark] that is as long as the message [1 mark].

Given one ciphertext, the attacker can try different random keys [1 mark] and get different intelligible plaintexts[1 mark], and there is no way the attacker will know which one is the plaintext [1 mark].

c) DES is a block-cipher and its basic mode of operation is Electronic Code Book (ECB). In this mode of operation, if the same 64-bit block of plaintext appears more than once in a message, it always produces the same ciphertext. In order to avoid such a security weakness, DES can be deployed in different modes of operation such as the Cipher feedback (CFB) mode. Briefly explain how CFB mode works, with the help of diagrams. **[6 marks]**

Answers:
i) CFB convert DES into a stream cipher.

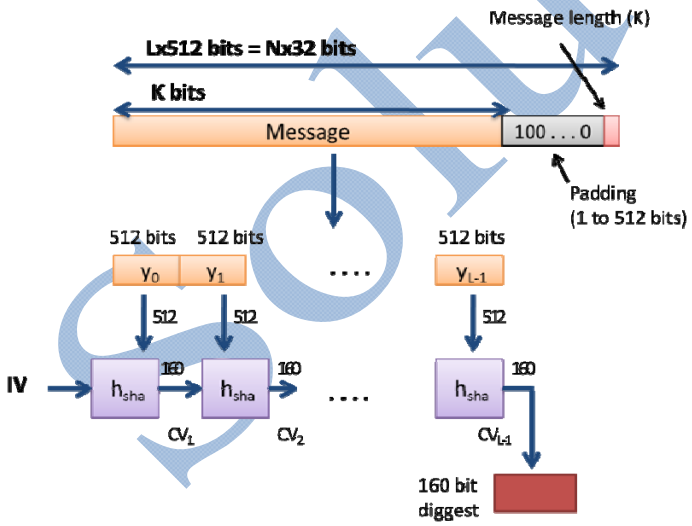
- Start with an initial vector (iv) (given) [1 mark]
- Shift *j* bits [1 mark]
- Encrypt using DES [1 mark]
- Select first *j* bits [1 mark]
- XOR with the *j* bits of the message [1 mark]
- Use the encrypted message as new iv [1 mark]



[3 marks for the diagram if correct, not exceeding total mark]

Question 2

a) Using block diagrams, explain how would SHA1 process any length of data block to produce a unique 160-bits output. **[5 marks]**



[1 mark for every underlined statement]

Main are appended with padding bits to reach a length dividable by 512 bits.
Then, each 512 block is processed using Hsha process, each block is processed with the previous stage, each block outputs 160-bits, same length as the initial stage takes a pre-defined IV.

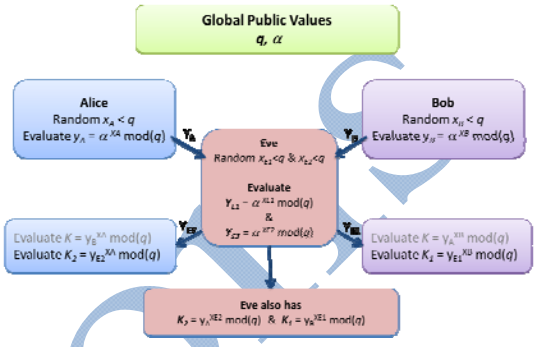
b) Explain the mechanisms of each of the following attacks: **[8 marks]**

i) 'Replay' attack:

It refers to replaying a valid sequence to gain access [or similar meaning]. (1 mark)

ii) 'Man-in-the-middle' attack:

Used on diffie-hellman key exchange method (1 mark)



Blocks worth 1 mark each block/description (6 marks).

.

c) Key distribution is one of the major problems when implementing a security mechanism. List two Public-key encryption algorithms which can be used to solve this problem. Explain how each of these methods can be used to exchange keys between two parties.
[12 marks]

Diffie-Hellman method (1 mark)
Based on Discrete Algorithms; both users know common values (prime number and its primitive root), each user generates a random secret value (<p); users then raise the primitive root to the random value to compute a public-value; they exchange the public values and raise them to the secret value to achieve identical key value at both ends. (5 marks)
RSA: (1 mark)
Each user holds a Public-Private key pair; one user could generate a random session (conventional) key; the user uses the receiver's public key to encrypt the session key (confidentiality); the user can then encrypt the new cipher using the user's private key (authentication); the receiver can then verify the authentication and validity of the received session key. (5 marks)

Question 3

a) What is a public key certificate? Explain what information a certificate contains to guarantee its integrity. **[5 marks]**

Is a certificate, typically provided by a trusted third party, which guarantees that the public information that the certificate contains has not been forged by an unauthorised user. (2 marks)

A public--key certificate consists of a public—key, the user ID of the key owner and the whole block signed by the trusted third party. (3 marks)

b) A certificate includes a period of validity. Sometimes the certificate is revoked before it expires. **[5 marks]**

i) Give three reasons why a certificate should be revoked before its expiry date?
ii) How can Certification Authorities (CAs) maintain an up-to-date validity of all users and avoid invalid keys?

(i)

- User's Private-Key has been compromised
- Certification Authority has been compromised
- User is no longer certified by this Authority

(ii) A list consisting of all revoked but not expired certificates issued by that CA, known as the certificate revocation list (CRL).

Each CRL posted to the directory is signed by the issuer and includes the issuer's name, the date the list was created, the date the next CRL is scheduled to be issued, and an entry for each revoked certificate.

Each entry consists of the serial number of a certificate and revocation date for that certificate. Because serial numbers are unique within a CA, the serial number is sufficient to identify the certificate.
Users should check certificates with CA's CRL.

c) Briefly explain how the Tunnel and Transport Modes operate in IPSec. **[4 marks]**

Transport mode, in this mode the load of the datagram is encrypted (ESP) or authenticated (AH) depending which protocol is used.

Tunnel mode the whole IP packet is encrypted (ESP) or authenticated (AH). This mode can be used to create a virtual private network VPN.

[2 marks for each type]

d) In IPSec, what are the specific key exchange algorithms in ISAKMP? What are the roles of the Oakley key determination protocol and ISAKMP? **[5 marks]**

ISAKMP by itself does not dictate a specific key exchange algorithm [1 marks]; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms [2 marks]. (Total = 3 marks)
Oakley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP. (2 marks)

e) List two techniques used by firewalls to control access and enforce a security policy. Explain each of them. **[6 marks]**

Any two from:

- Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service. (Type 1 marks; 2 marks for the explanations; Total 3 marks)

- Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall. (Type 1 marks; 2 marks for the explainations; Total 3 marks)

- User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec. (Type 1 marks; 2 marks for the explanations; Total 3 marks)

- Behaviour control: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server. (Type 1 marks; 2 marks for the explanations; Total 3 marks)

(1 mark for each type; 2 marks for each description = 6 marks)

Question 4

a) Define the following two important SSL concepts:
   i) SSL connection
   ii) SSL session

[4 marks]

A **connection** in SSL a transport that provides a suitable type of service. The connections are peer-to-peer relationships and are transient. Every connection is associated with one session. (2 marks)

A **session** in SSL is an association in between a client and a server. They define the security which can be shared between multiple connections (to avoid expansive renegotiation of security parameters). (2 marks)

b) In PGP key management, there is a possibility of multiple public keys per user, therefore the recipient of the message needs to know which of his/her public keys was used for encryption. Explain how PGP identifies the public key.

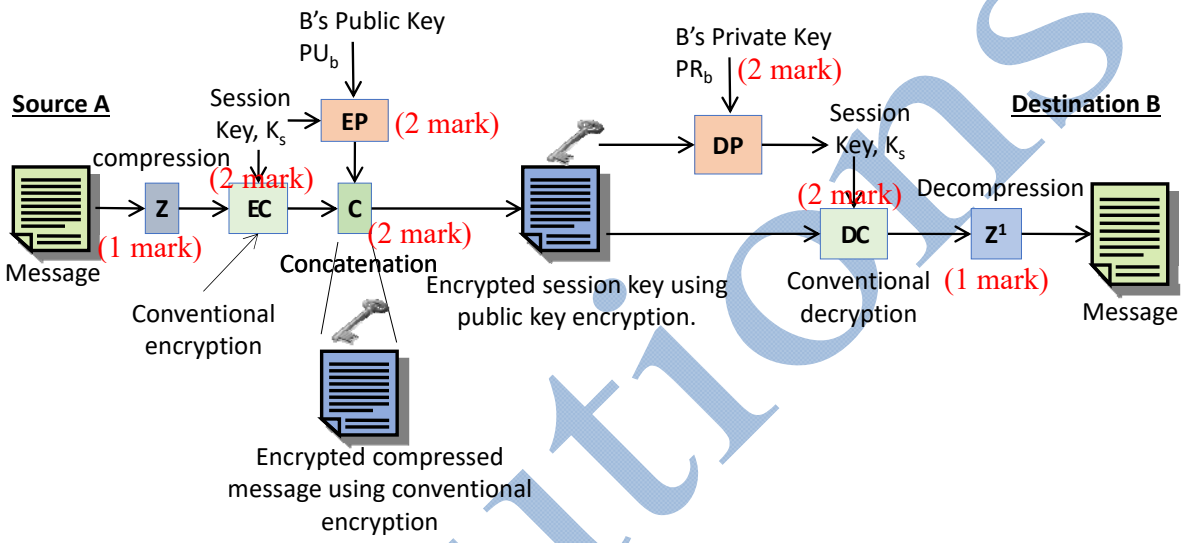
[4 marks]

PGP assigns an ID to each public key by using the last 64 significant bits of the key. The ID can be used to identify which public key was used.

[4 marks]

c) Draw a schematic diagram with adequate notations to show how a set of Private (PR_b) and Public (PU_b) keys of User B is used in the PGP's confidentiality operation.

[12 marks]



d) Explain the Certificates Processing of S/MIME.

[5 marks]

- Uses public-key certificates that conform to X.509 v3. (1 marks)
- Key management is hybrid between X.509 and PGP's web of trust. (1 marks)
- Each client has a list of trusted CA's certificates and own public/private key pairs & certificates. (2 marks)
- Certificates must be signed by trusted CA's (e.g. VeriSign) (1 marks)