University	:	*Menoufia*		*Date*	: *13/1/2019*
Faculty	:	*Electronic Engineering*		*Time*	: *3 Hours*
Department	:	*Computer Sci & Eng*		*No. of pages*	: *4*
Academic level	:	*4th Year, 1st Term*		*Full Mark*	: *90 Marks*
Course Name	:	*Network Security*		*Exam*	: *Final Exam*
Course Code	:	*CSE 413*		*Examiner*	: *Dr. Mohamed Moawed*

Answer all the following questions (90 degrees):

Question No. 1: Complete the following (15 degrees):

1. Packet Sniffing is .....
   But Packet Spoofing is .....
2. Privacy means .....
3. Digital Signature means .....
4. There are two requirements for secure use of conventional encryption ..... and .....
5. An encryption scheme is unconditionally secure if .....
6. There are Three disadvantage of Caesar cipher ....., ..., and .....
7. The mechanism of Confusion seeks to make .....
8. In DES function, whitener step means .....
9. In DES key generation, the first step to convert the key from 64-bits to 56-bit is called .....
10. RC4 is widely used in ..... and ..... protocols.
11. The possible approaches to attack the RSA algorithm which are ....., ..., ..., and .....
12. There are different types of PGP messages such as ....., ..., and .....
13. S/MIME adds some new content types to include security services to the MIME, this new content is called .....
14. SSL defines six key-exchange methods to establish this pre-master secret such as ....., ..., ..., and .....
15. SSL defines four protocols, Alert protocol is one of them that is used to .....

Go to next page

Question No. 2: Choose the correct answer (10 degrees):

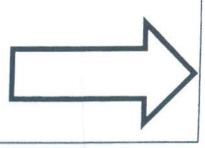
1. **(Security mechanism – Security service – Cryptography - Steganography)** is a processing that enhances the security of the data processing systems and the information transfers of an organization.
2. The best-known multiple-letter encryption cipher is **(Caesar - Vigenère – Playfair - Rail Fence)**
3. Converting the plaintext to the ciphertext is known as **(deciphering – enciphering – cryptanalysis – steganography)**
4. The solution to protect from a brute-force attack is using **(small keys – faster algorithm – Caesar cipher - large keys)**
5. One example of Block Ciphers Influenced by DES is **(CATS – CTAS – CSTA – CAST)**
6. **(ChangeCipherSpec - Handshake – Record – Alert)** protocol is one of SSL protocols that carries the message from three other protocols and the data coming from the application layer.
7. **(RC4 – DES – RC2 – 3DES)** protocol is used in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards.
8. In **(DES – RC4 – RSA - Caesar)** protocol, the plaintext and ciphertext are **numbers**.
9. **(Encrypted – Signed – Certificate - Signature)** message is one of the PGP message that is a combination of user ID packet and a public-key packet
10. TLS position in the internet model between **(transport & network – network & data-link – data-link & physical - application & transport)** layers

---

Question No. 3: Answer the following question (20 degrees):

1. **Encrypt** the message **"Network Security"** using: (9 degrees)
   a. **Caesar cipher** with key = 6. (3 degrees)
   b. **Playfair cipher** with a keyword "**Secret**". (3 degrees)
   c. **Vigenère cipher** using a keyword "**Final**". (3 degrees)
2. **Decrypt** the Message "**RRNMXTEYEJESTL3NKIA1WCFXAOUIAN**" using "**Use of Permutation**" algorithm with the key "**4 3 2 5 6 1**". (3 degrees)

Go to next page



3. **What is meant by:** "SSL_RSA_WITH_RC4_128_MD5"? (2 degrees)

4. **Decrypt** the message ciphertext (**11001100**) and the key (**01101100**) using the **stream cipher**. (2 degrees)

(4 degrees)

5. **Encrypt the plaintext (M=5) using RSA algorithm when p = 3 and q = 11.**

Question No.4: Answer the following question (15 degrees):

Assume that the **Cipher-text** be **0010 1001**, Block size be 8 bits, Key size = 8 bits (C_0 = **0011**, D_0 = **1010**), Number rounds be 2, Half the block size = 4.

Decrypt the ciphertext to get the plaintext using **DES**.

T_1 = Initial Permutation table (IP) = $\begin{bmatrix} 1 & 4 & 6 & 8 \\ 3 & 5 & 2 & 7 \end{bmatrix}$

T_2 = Final Permutation table = $\begin{bmatrix} 1 & 7 & 5 & 2 \\ 6 & 3 & 8 & 4 \end{bmatrix}$

T_3 = Expansion table = $\begin{bmatrix} 4 & 1 & 2 & 3 \\ 2 & 3 & 4 & 1 \end{bmatrix}$

The two S-boxes:

- $S_1 = \begin{pmatrix} 0 & 2 & 1 & 3 \\ 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 0 \\ 3 & 0 & 2 & 1 \end{pmatrix}$ & $S_2 = \begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 0 & 2 \\ 2 & 1 & 0 & 3 \end{pmatrix}$

T_4 = Permutation of 4 bits [2 1 4 3]

T_5= Key shift table

Rounds	1	2
Shifts	2	1

Question No.5: Answer the following questions (15 degrees):

1. What are the characteristics of cryptographic systems?
2. Describe briefly with drawing the block diagram the DES function.
3. Briefly discuss the services that could be provided by SSL protocol.

Go to next page

4. In triple DES, how encryption and decryption is done using 3 keys and 2 keys. Present your answer with only figures and equations.
5. Briefly discuss how Public-key encryption can offer confidentiality or sender authentication or both, depending on keys used for encryption/decryption.

Question N.6: Put True (T) or False (F) for the following sentences (15 degrees):

1. System integrity assures that information and programs are changed only in a specified and authorized manner.
2. Security requires regular monitoring which is easy today.
3. Passive attacks are very difficult to detect.
4. Bacterium is a program that replicates itself by installing copies of itself on other machines across the network.
5. No single mechanism that will support all services required.
6. There is no encryption algorithm that is unconditionally secure.
7. Stream ciphers are applicable to a wider range of applications than block ciphers.
8. There is no way to find an "m" that hashed to "h(m)".
9. If the text message has been compressed before encryption, then recognition is more difficult.
10. PGP provides authentication, where the sender creates a digest of message and signs it with his private key.
11. A special type of attack called "meet in the middle attack" that attacks triple DES.
12. RC2 is faster than DES.
13. Compression is optional in SSLv3.
14. The key distribution is simple when using public-key encryption, compared to the key distribution for symmetric encryption.
15. Fortezza Key Exchange Algorithm is used with SSL but not used with TLS.

With my best wishes
Dr. Mohamed Moawed ☺