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