Cairo University
Institute of Statistical Studies & Research
Department of Computer & Information Sciences
CS-634 Networks Security January 2017 Time: 3 hours Imane Fahmy

Answer all the following questions in your answers sheet:

Question 1: Choose the correct answer to complete the following sentences and write its corresponding letter (a), (b), (c) or (d) in your answers sheet: **[10 marks]**

1- Most symmetric block ciphers are based on a ………………… Cipher structure.
(a) Caesar (b) human (c) Feistel (d) substitution

2- The message must be decrypted at each switch to read address in ……………. encryption.
(a) End-to-end (b) link (c) asymmetric (d) none

3- Traffic padding protects against ……………. attacks.
(a) passive (b) active (c) DoS (d) (b)&(c)

4- Ciphers need to completely obscure statistical properties of original message by ………….
(a) Confusion (b) diffusion (c) (a)&(b) (d) digital signature

5- ………………… Cipher is the main concept upon which Feistel cipher.
(a) Transposition (b) Invertible product (c) Asymmetric (d) Shift

6- The effective key size of triple DES is ……….. bits length.
(a) 112 (b) 64 (c) 32 (d) 256

7- Among the advantages of authentication without encryption of message: ………………………..
(a) cheaper (b) faster (c) easier (d) (a),(b)&(c)

8- The Internet Protocol security IPSec services are implemented at the ……………. layer.
(a) TCP (b) above TCP (c) network (d) application

9- Handshake failure results in ……………. alert by SSL alert protocol.
(a) Negotiation (b) fatal (c) warning (d) no

10- The Secure Shell SSH protocol provides secure ………………… service.
(a) Remote logon (b) key exchange (c) encryption (d) digital signature

Question 2: Indicate whether the following sentences are True (T) or False (F) and write (T) or (F) and correct the false sentences in your answers sheet: **[10 marks]**

1- DES round function uses a round key with 128 bits length. ( )
2- AES inputs a 128-bit data block and assumes 64 bits key length. ( )
3- DoS attacks require attacking the servers and the network infrastructure. ( )
4- Worms are malware that require some sort of user interaction to infect user's device. ( )
5- An IP spoofing attack is a passive receiver that records a copy of all your packets. ( )
6- In vulnerability DoS attack, attackers send huge number of packets to the target host. ( )
7- Secure Hash Algorithm SHA-512 uses 1024 bits data blocks to produce 512 bits digest. ( )
8- Encryption could protect against IP spoofing attacks. ( )
9- Pretty Good Privacy PGP compresses message after signing but before encrypting. ( )
10- Hash function collision-free property implies that it is computationally infeasible to find data mapping to specific hash. ( )

Question 3: Design and Sketch the following questions: **[28 marks]**

1) Design the encryption/decryption diagrams between two communicating entities: Source A and destination B for the following schemes: [6 marks]
   a. Public key encryption
   b. Digital Signature
2) Sketch the Secure Socket Layer SSL record protocol operation steps applied on application data. [5 marks]
3) Given the cryptographic expression:
   $C = E(K, [M \| E(PR_a, H(M))])$ provides: authentication, digital signature and confidentiality for a plaintext message M, where K is the secret key used for encryption. [6 marks]
   a) Draw a diagram to generate the ciphertext C at the source and to verify the ciphertext C at the destination
   b) Which part of the given expression provides digital signature?
4) If Alice and Bob chose to secure their exchanged mails using the Pretty Good Privacy PGP algorithm. Draw a diagram to help them secure their message M according to their security requirement as follows: [6 marks]
   a) Confidentiality only.
   b) Authentication only.
5) Assume A and B, share a common secret key K_{AB}. When A has a message M to send to B, it calculates the Message Authentication Code MAC as a function of the message and the key: $MAC_M = F(K_{AB}, M)$. The message plus code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code. Draw the MAC scheme between A and B. [5 marks]

Question 4: Solve the following problems: **[30 marks]**

1) Given the binary plaintext **P**: 0100111100010100111000101 0 bit stream and the encryption repetitive key pattern **k**: 01011 used by ***Vernham*** cipher, deduce the ciphertext **C** generated by the source then verify the recovery of the plaintext **P** at the destination using the same repetitive key pattern for decryption. [4 marks]
2) A product cipher encryption technique based on a ***Caesar*** shift substitution cipher followed by a ***Rail Fence*** transposition cipher was used to generate the following ciphertext:
   C= WHQPDWHDHKHHBWKJW. Decrypt the original message plaintext **P**. [4 marks]
3) Using Diffee-Helman key exchange, Alice and bob agreed on global parameters: a large prime integer or polynomial $q=353$ and $e=17$ primitive root < q. Alice and Bob then generate their secret values: $\mathbf{x_a=11}$, $\mathbf{x_b=191}$. Then, they should generate their public keys: $\mathbf{y_a}$, $\mathbf{y_b}$ to share on a public domain based on the global parameters and their private values. Finally, when Alice and Bob initiated their communication session, they computed their session key $\mathbf{K_{a,b}}$. [12 marks]
   A. Show all D-H algorithm steps used to make all keys computations.
   B. What is the secret keys selection condition that Alice and Bob must respect?
   C. Compute Alice's and Bob's public keys.
   D. Compute their session key $\mathbf{K_{a,b}}$ at both points: Alice and Bob. Is it the same value?
   E. What could be the equation used by a cryptanalyst in order to deduce the secret value?
   F. What is the attack that D-H key exchange scheme may suffer from?
4) Perform encryption and decryption using RSA algorithm, for the following parameters: prime numbers $p = 31$; $q = 13$, $e = 5$ and message input $M = 15$. [10 marks]
   a) Show all RSA algorithm computations steps.
   b) Sketch the encryption/decryption process showing the resulting public and private keys used to encrypt M into ciphertext C at source then decrypt C into M at destination.

Best wishes