Kurdistan Region Government-Iraq
Ministry of Higher Education and Scientific Research
University of Salahaddin - Erbil
College of Engineering
Department of Software & infomratics engineerig

# 80 Questions
# in
# Data Security

**B.Sc. Degree in Software & informatics engineering**
**4th Year Material**
**Academic year 2022-23**

## Mr. Zana Farhad Dogramachi

zana.softeng@gmail.com

# Answer the following Questions:

Q1 Mark the correct answer for the following questions. *Note that the **true** select have (**1** point) while the **wrong** select have (**-0.25** point).*

1. *The Digital Signature Standard specifies all of the following as valid algorithms for creating digital signatures except:*
   a) *DSA*
   b) *ECDSA*
   c) *RSA*
   d) *AES*
2. What key length does AES not support?
   a) 128-bit
   b) 256-bit
   c) 512-bit
   d) 192-bit
3. Which algorithms are no longer recommended for use?
   a) RSA
   b) DES
   c) IPSEC
   d) AES
4. *The ..... cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.*
   a) *Transposition*
   b) *Additive*
   c) *Shift*
   d) *None of the above*
5. *In ..... , a claimant proves her identity to the verifier by using one of the three kinds of witnesses.*
   a) *Message authentication*
   b) *Entity authentication*
   c) *Message confidentiality*
   d) *Message integrity*
6. *A(n) ..... can be used to preserve the integrity of a document or a message.*
   a) *Message digest*
   b) *Decryption*
   c) *Encrypted message*
   d) *None of the above*
7. *Which of the following is a disadvantage of asymmetric cryptology?*
   a) *No potential for centralized key management*
   b) *Complex key distribution*
   c) *Does not provide non-repudiation*
   d) *Slower than symmetric cryptology*
8. *What is the padding for SHA-512 the length of the message is:*
   a) *5120 bits*
   b) *5121 bits*
   c) *5122 bits*
   d) *6143 bits*
9. *Message ..... means that the sender and the receiver expect privacy.*
   a) *Confidentiality*
   b) *Integrity*
   c) *Authentication*
   d) *None of the above*
10. *Secure hash algorithms provide both confidentiality and integrity?*
    a) *True*
    b) *False*

*Q2* Compare the compression function of SHA-512 without the last operation (final adding) with Feistel cipher of 80 rounds. show the similarities and differences.

Q3 Define Kerberos and name its servers. Briefly explain the duties of each server.

*Q4 Using* the Rabin cryptosystem with p =47, q = 11 and Message = "*ok we have done*"

a) Find the ciphertext for the first character (o) in the message.(2 points)
b) Explain can you use the same keys to encrypt the message word by word?(2 points)
c) Use the Chinese remainder theorem to find four possible plaintexts.

Q5 Draw two different ways in which a hash value be secured so as to provide message authentication?

*Q6* Assume that you are Eve, and have captured Alice and Bob and imprisoned Diffie-Hellman protocol. You overhear the following dialog.
Bob: Oh, let's not bother with the prime in the Diffie-Hellman protocol, it will make things easier.
Alice: Okay, but we still need a base to raise things to. How about g = 3 & p=17?
Bob: All right, then my result is 10.
Alice: And mine is 5.
Find $K_A$, $K_B$ and their secret combined key by using Man in the middle Attacker?

*Q7* Write key generation algorithm in RC4?

Q8 In what order should the signature function and the confidentiality function be applied to a message, and why?

*Q9 Define the RSA digital signature scheme and compare it to the RSA cryptosystem*

Q10 Find the multiplicative inverse and greatest common divisor of 1234 mod 4321 by using the extended Euclidean algorithm.

Q11 Use the below secret key to encrypt the plaintext "Inshalla"

Secret Key =

| | | | | |
|---|---|---|---|---|
| L | G | D | B | A |
| Q | M | H | E | C |
| U | R | N | I/J | F |
| X | V | S | O | K |
| Z | Y | W | T | P |

*Q12* What is the salt in a password-based authentication system? How does it help in defending against accessing a password file attacks?

*Q13* Find the result of $5^{\wedge 17}$ mod 60.

Q14 List categories of security services?

Q15 Draw the General Design of AES encryption cipher and show the relationship between number of rounds and cipher key size?

Q16 Compare the substitution in DES and AES. How many are they in each?

*Q 17* What are requirements for a Hash Function?

Q18 What are weakness in DSS approach and draw it's diagram?

*Q19* If you are using RSA algorithm, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35.

1. What is the plaintext M?
2. Explain can you use the same keys to encrypt the plaintext "*always be honest about your skills*" word by word?

Q20 What types of attacks are addressed by message authentication? define them?

*Q21* What are drawbacks in Public Available Directory?

Q22 Compare and contrast attacks on digital signatures with attacks on cryptosystems.

*Q23* What is the one way function in this system?

Q24 What is the trapdoor in the system?

Q25 Define the public and private keys in this system.

Q26 Describe the security in this system.

Q27 Find all values of x for the following congruence:

$$4x + 7 \equiv 5 \pmod 6$$

Q28 If Alice uses a multiplication cipher, she often needs to encipher plaintext made of bother letters (a to z), digits (0 to 9) and three symbols (@,!,$). What is the size of the key domain? What is the modulus?

Q29 What is the salt in a password-based authentication system? How does it help in defending against offline dictionary attacks?

Q30 Find the value of $\varphi(96)$.

Q31 List categories of Passive Attack?

Q32 If you're using AES encryption, put the plaintext is "*we have DS exam*" in to state?

Q33 Draw the structure of the Single Round of DES Algorithm?

Q34 How many transformations are there in AES-128? How many round keys are needed for AES-256?

Q35 How many XOR operations are used in the DES cipher?

Q36 Alice often needs to encipher plaintext made of bother letters (a to z), and digits (0 to 9). What is the key domain? What is the modulus? If she uses a multiplication cipher.

Q37 What is the block size, cipher key size and round key size in DES?

Q38 Find $\varphi(72)$?

Q39 Write key expansion algorithm for AES-128.

Q40 A small private club has only 100 members. Answer the following questions:

i. How many secret key are needed if all members of the club need to send secret key message to each other?
ii. How many secret key are needed if everyone trusts the president of the club? If a member needs to send message to another member, she first sends it to the president; the president then sends message to the other members.

Q41 Eve has intercepted the ciphertext C = 2, whose public key is e =7, n = 187. What is the plaintext M? if RSA algorithm has been used for ciphering.

Q42 Eve has intercepted the ciphertext “djx”. Show how she can use a brute force attack to break the cipher if she knows Additive algorithm has been used.

Q43 Explain RC4 Algorithm briefly.

Q44 Briefly explain the idea behind the Rabin cryptosystem

i. What is the one way function in this system?
ii. Define the public and private keys in this system?
iii. Describe the security in this system.

Q45 Find the multiplicative inverse and greatest common divisor of 550 mod 1759 by using the extended Euclidean algorithm.

Q46 What are drawbacks in first approach one-time password?

Q47 What is known weaknesses in Kerberos?

Q48 Explain Dictionary attack in second approach fixed password?

Q49 What is benefit and drawback of using DNA as biometric authentication?

Q50 Define nonce? Describe it? What is it used for?

Q51 Describe the role of Ticket granting server (TGS) in Kerberos authentication protocol.

Q52 What is the difference between verification and identification give an example for each?

Q53 Draw Public Key distribution Scenario's diagram?

Q54 Describe in detail a man-in-the-middle attack on the Diffie-Hellman key exchange protocol whereby the adversary ends up sharing a keys $k_1$ & $k_2$ with Alice and Bob, they cannot detect that anything has gone wrong.

What happens if Alice and Bob try to detect the presence of a man-in the middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

Q55 Briefly Explain the operation in Kerberos or just draw it's diagram?

Q56 How can a system prevent a guessing attack on a password? How can a bank prevent PIN guessing if someone has found or stolen a bank card and tries to use it?

Q57 What is $N^2$ Problem in symmetric key distribution? Is that the only problem? Explain how you can use KDC to create a symmetric (session) key $K_{AB}$ between Alice and Bob

Q58 What is the key domain for any multiplicative cipher?

Q59 Define a trapdoor one way function and explain its use in asymmetric key cryptography?

Q60 What is Diffusion and Confusion?

Q61 What is benefit and drawback of using Face as biometric authentication?

Q62 What are the essential ingredients of a public key directory?

Q63 What are the two general approaches to attacking a cipher?

Q64 What is the difference between SubBytes and SubWord in AES?

Q65 What are potential attacks on RSA?

Q66 Write Fast Exponentiation Algorithm.

Q67 What is Important considerations to design good stream cipher?

Q68 What problem was Kerberos designed to address?

Q69 How many keys are required for two people to communicate via a cipher?

Q70 Using the Rabin cryptosystem with p = 11, q = 7 and Message = hi

a) Find the ciphertext for the second character (i).
b) Use the Chinese remainder theorem to find four possible plaintexts.

Q71 Bob often needs to encipher plaintext made of both letters (a to z), operations (+,-,*,/) digits (0 to 9). If she uses an affine cipher, what is the key domain? What is the modulus?

Q72 What are the parameters and design features that Feistel network depends on?

Q73 What are all possible plaintext for the ciphertext C=" WQWW" in Z30 by using generalized Rabin cryptosystem If the public key is 33. Then choose the correct plaintext.

Q74 Use a brute force attack to decipher the following message enciphered in Z26 by Alice.
YZIPNCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

Q75 What are the weakness in Public Announcement scenario?

Q76 Trace the following mathematical procedures Fast_Exponention (3, 11, 26)

Q77 Draw the hash code in which the two communicating parties share a common secret value with confidentiality.

Q78 What are certificates? How are certificates used? Who issues certificates and how?

Q79 Assume Person A sent an encrypted message to person B by using ElGamal cryptosystem, A uses B's prime key (31) to send a message for him,

1. Choose appropriate e1 and d then calculate e2.
2. Encrypt the plaintext "WOW"
3. Decrypt the ciphertext to obtain plaintext.

Q80 Use Vigenere cipher with the key "show you" to encrypt the message "I used to wonder why".

Q81 Write key expansion algorithm for AES-128.?

Q82 Define the RSA digital signature scheme and compare it to the RSA cryptosystem.

Q83 If Alice uses Bob's RSA public key (e=29, n=35) to send the plaintext encrypted in z26 as "KUN". Show how Eve can use the factorization attack if she has access to Bob's computer to find the plaintext .

Q84 Use a brute force attack to decipher the following message enciphered in Z26 by Alice. Assume that you know it is an affine cipher and that the plaintext "ab" is enciphered to "GL".

Q85 What are the drawbacks in Public Key Authority scenario?

Q86 Trace the following mathematical procedures Fermat factorization (323)

Q87 What are the Requirements for Hash Function?

Q88 What are all possible plaintext for the ciphertext C=" WQWW" in Z30 by using generalized Rabin cryptosystem If the public key is 33. Then choose the correct plaintext.