# Homework 1&2

## Chose the correct answer

| | | | | |
|---|---|---|---|---|
| 1 | **…… is a potential for violation of security which exists when there is a circumstance ,capability , action or event that could breach security** | | | |
| | ***(a)Threat*** | ***(b)Attack*** | ***(c)Spam*** | ***(d) none of the mentioned*** |
| 2 | **…….. an assault on system security derived from intelligent threat that's attempt to evade security services and violate security system** | | | |
| | ***(a)Threat*** | ***(b)Attack*** | ***(c)Spam*** | ***(d) none of the mentioned*** |
| 3 | **OSI stands for ……………………………** | | | |
| | ***(a)Open Security Interconnection*** | ***(b)Open Systems Interconnection*** | ***(c )Open Services Interconnection*** | ***(d) none of the mentioned*** |
| 4 | **Which of the following is a type of passive attack** | | | |
| | **(a)Release of message content** | **(b)Traffic analysis** | **(c )both of them** | **(d) none of the mentioned** |
| 5 | **Which of the following g isn't a type of passive attack** | | | |
| | **(a)Release of message content** | **(b)Traffic analysis** | **(c )Modification of message** | **(d) none of the mentioned** |
| 6 | **Which of the following is not a type of symmetric-key cryptography technique?** | | | |
| | ***(a)Caesar cipher*** | ***(b)Data Encryption Standard (DES)*** | ***(c )Hill cipher*** | ***(d)Play fair cipher*** |

| 7 | **Which of the following options correctly defines the Brute force attack?** | | | |
|---|---|---|---|---|
| | ***(a)Brutally forcing the user to share the useful information like pins and passwords*** | ***(b)Trying every possible key to decrypt the message.*** | ***(c )One entity pretends to be some other entity*** | ***(d) The message or information is modified before sending it to the receive*** |

1. Define and draw the security system?
2. State the security requirements?
3. Define the meaning of: Masquerading, unauthorized access, and denial of service
4. Compare between classical and modern cryptography
5. Define the meaning of: signature, data integrity, non-repudiation , and confidentiality,
6. Let the key string be gold. Using the encoding rule A=0, B=1, …,Z=25, the numerical representation of this key string is (6,14,11,3) . What is the Vigenre encryption of the plaintext string PROCEED MEETING AS AGREED
7. Define the hash function?
8. Write a program that can encrypt and decrypt using the general Caesar cipher, also known as an additive cipher.
9. What is the difference between a block cipher and a stream cipher
10. Classify the cryptographic hash function and its application?

11. Explain rail fence technique? Use the complex scheme of rail fence technique with the Key: 4 3 1 2 5 6 7 to encrypt the message: :meet me after the toga party" Write the cipher text?

12. One-time pads can easily be generalized to work in alphabets other than the binary. For manual encryption, an especially useful one is a OTP that operates on letters.

(a) Develop a OTP system which operates with the letters A,B,…,Z, represented by the numbers 0,1,…,25. How does the key (stream) look? What are the encryption and decryption functions?

(b) Decrypt the following cipher text:

BSASPP KKUOSR

Which was encrypted using the one-time pad:

RSIDPY DKAWOA