1.

**a) What is the main difference between a passive attack and an active attack?**

In Active attack, an attacker tries to modify the content of the messages. Whereas in Passive attack, an attacker observes the messages, copy them and may use them for malicious purposes.

**b) Write down the main difference between a chosen plaintext attack and a chosen cyphertext attack.**

In choosing plaintext attack, after receiving the ciphertext of a message, you need some of the paintext of the same encrypted message that was received. Then using a technique to match the cipher text with its identical plaintext to get the part of key which help to break the algorithm.

In choosing ciphertext attack, the cryptanalysis depend only on the cipher text of the received message to recover the key or break the algorithm by using for example statistical tests.

**c) In breaking Enigma, what was the main idea that led to success?**

The "Crib". At the end of the German's telegram, they would probably use "Our great leader Hitler". So we can use it as a crib to break Enigma.

It is a chosen plaintext attack.

**d) How can XTS-AES be exploited in ransomware?**

XTS-AES cannot guarantee the integrity of the data. So the data can be rewrote by the attacker.

**e) Write down three possible ways that cryptography could make use of a pseudorandom number generator.**

1. Construct session keys

2. Construct stream cipher

3. generate the secret key of symmetry encryption.

**f) Write down three differences between older ciphers like DES and more modern ciphers like AES.**

(1) older ciphers like DES have smaller key size which makes it less secure.

(2) In DES, plaintext block is divided into two halves before the main algorithm starts whereas, in AES the entire block is processed to obtain the ciphertext.

(3) DES works on Feistel Cipher structure, and AES works on Substitution and Permutation Principle.

**g) Why is HMAC robust against breaking a hash algorithm it uses?**

HMAC provides one important property: collision resistance. It is impractical to find two messages that result in the same digest. Besides, HMAC requires a key, and if it is 128 bits, there are 2^128 possibilities.

**h) In elliptic curve cryptography, what is the most important property of the generator that is used?**

Asymmetric encryption algorithm produce apparently random output.

**j) What is the saving in the B92 QKD algorithm compared with the BB84 QKD algorithm?**

BB92 protocol uses two states rather than possible 4 polarization states in BB84 protocol.

2.

**a) Describe the structure of AES.**

* data block of 4 columns of 4 bytes is state
* key is expanded to array of words
* has 9/11/13 rounds in which state undergoes:

- byte substitution( 1 S-box used on every byte)

-shift rows( permute bytes between groups/columns)

-mix columns(subs using matrix multiply of groups)

-add round key( XOR state with key material)

-view as alternating XOR key & scramble data bytes

* initial XOR key material & incomplete last round
* fast XOR & table lookup implementation

**b) Describe the RSA public key cryptography scheme.**

* to encrypt a message M, the sender:

- obtains public key of recipient PU={e,n}

- computes: C = M^e mod n, where 0<=M<n

* to decrypt the ciphertext C, the owner:

- uses their private key PR={d,n}

-computes: M = C^d mod n

* note that the message M must be smaller than the modulus n.

**c) Construct an example of the RSA scheme as follows. The two primes to be used for the modulus *N* are 5 and 7. What is (*N*)? Choose 7 as the encryption key. What is the corresponding decryption key? Encrypt the message 17 using your smallest encryption key. Confirm that you can decrypt the ciphertext using your decryption key.**

N = 5\*7 = 35

phi(N) = (5-1)\*(7-1) = 24

e = 7

Because d\*e = 1 mod phi(N),

7d = 1 mod 24

d = 7, because 7\*7 49 = 1+24\*2

M = 17

C = M^e mod n = 17^7 mod 35 = 3

M = C^d mod n = 3^7 mod 35 = 17

3.

**a) Below is the AES S-box. Apply it to the hex string AB23018FC4.**

62267C731C

**b) Describe the RC4 algorithm.**

\* starts with an array S of numbers: 0..255 starts with an array S of numbers: 0..255

\* use key to well and truly shuffle S use key to well and truly shuffle S

\* S forms S forms internal state internal state of of the cipher the cipher

for i = 0 to 255 do

S[i] = i

T[i] = K[i mod keylen] j = 0

for i = 0 to 255 do

j = (j + S[i] + T[i]) (mod 256)

swap (S[i], S[j])

c) **The RC4 algorithm makes much use of a swap(x,y) primitive. One common way of implementing a swap(x,y) primitive is the following:**

x = x 뒘 y ; y = x 뒘 y ; x = x 뒘 y

**Why should this never be used in RC4**?

It is really heavy to compute.

**d) Give a description of the two main Galois/Counter Mode operations.**

GHASH： GHASH is based entirely on GF(2^128)

GCTR： CTR mode with incremented counter

**e) Describe the Overview of the Galois/Counter Mode.**

Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers.The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. GCM is defined for block ciphers with a block size of 128 bits.