1.

**a) Give four examples of modern malware.**

Ransomware, Trojans, Worms, Viruses

**b) What is a product cypher? Why were product cyphers important in the development of modern cryptography?**

A product cipher combines two or more transformations.

It is so important because it makes the resulting cipher more secure than the individual components, and it has become the standard for some algorithms such as DES and AES.

**c) Write down three important design considerations for a Feistel cipher.**

block size, key size, number of rounds

**d) Briefly explain the term triple DES. Why are multiple DES encryptions genuinely stronger than a single DES encryption?**

Triple DES is a symmetric-key block ciper, which applies the DES cipher algorithm three times to each data block.

Multiple DES encryptions define a bigger class of substitutions on 64-bit data blocks, which makes it more stronger.

**e) Which algorithm is used to find the inverse of an element in a finite field?**

Euclidean algorithm.

**f) Describe briefly the Blum-Blum-Shub pseudo-random number generator.**

Blum-Blum-Shub generator is based on public key algorithms. It is unpredictable given any run of bits. Besides, it is so slow, since very large large numbers must be used. It is too slow for cipher use, but good for key generation.

**g) What property is possessed by counter mode, that is not possessed by any other standard block cipher mode?**

Parallel-computation.

**h) What is the most important property of digital signatures?**

Non-repudiation.

**i) Why does quantum factoring not constitute a threat to RSA?**

PK shemes are generic and super-polynomial, we can always choose a bigger instance.

**j) What is keywrapping good for?**

Keywrapping gives more confusion and diffusion in encryption of a session key...plus authentication block.

2.

**a) Describe the structure of a round of a Feistel cypher.**

In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input − the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.

**b) Describe the *Extended Euclid Algorithm* for finding not only the GCD of two numbers *x* and *y*, but also the coefficients *a* and *b* such that GCD(*x*, *y*) = *ax* + *by*.**

define a function exgcd(a,b)

if b!=0

then gcd(a,b) = gcd(b, a mod b)

assume that we get the solution of (b, a mod b), which is (x',y')

then ax+by = bx'+(a mod b)y'

then ax+by = bx'+(a-b\*[a/b])y'

then ax+by = ay' + b(x' - [a/b]y')

so x=y' y=x'-[a/b]y'

The question becomes how to calculate exgcd(b, a mod b)

recur until b=0 we get the solution.

**c) 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.

**d) What defence does Optimal Asymmetric Encryption Padding provide against malevolent manipulation of the final cyphertext produced?**

1.Add an element of randomness which can be used to convert a deterministic encryption scheme into a probabilistic scheme.

2.Prevent partial decryption of ciphertexts by ensuring that an adversary cannot recover any portion of the plaintext without being able to invert the trapdoor one-way permutation f.

**e) Describe the Diffie-Hellman key agreement protocol.**

(1)Alice and Bob choose a prime number q and a primitive root of q 'a', a<q.

(2)Alice select private XA, XA<q, then calculate public YA = a^XA mod q.

(3)Bob select private XB, XB<q, then calculate public YB = a^XB mod q.

(4) Then they exchange the public.

(5)Alice calculates the secret key by K = (YB)^XA mod q.

(6)Bob calculates the secret key by K = (YA)^XB mod q.

3.

**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) Explain the RSA-PSS digital signature scheme.**

RSA-PSS is a probabilistic signature scheme with appendix. A signature scheme with appendix requires the message itself to verify the signature.

**c) What useful property does the RSA-PSS digital signature scheme have?**

It is provably reducible to the hardness of the RSA problem.

**d) Describe the ElGamal encryption scheme using elliptic curves.**

1.encode any message must first encode any message M as a point on as a point on the elliptic curve the elliptic curve Pm

2. select suitable curve and point select suitable curve and point G as in D-H.

3. receiver chooses private key receiver chooses private key nA < n

4.receiver computes public key receiver computes public key PA = nA \* G

5.sender chooses private random key sender chooses private random key k

6.sender encrypts sender encrypts Pm : Cm = {kG,, Pm + kPb}

7.decrypt decrypt Cm compute: compute:

Pm + kPb –– nB(kG) = Pm + k(nBG) –– nB(kG) = Pm