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

Ransomware, Trojans, Worms, Viruses

**b) What is a product cipher? Why were product ciphers 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) Consider a block cipher working on 64 bit blocks. How many possible block ciphers are there in the ideal case? How many are there if a key of 64 bits is used?**

2^64

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

The "Crib". In 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 kind of the chosen plaintext attack.

**e) 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.

**f) 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.

**g)Briefly explain the terms one-way function and trapdoor one-way function.**

One-way function: A one-way function is easy to compute on every input, but hard to compute the opposite direction.

Trapdoor one-way function: A trapdoor one-way function is easy to compute in one direction, yet difficult to compute the opposite direction without special information, called the "trapdoor".

**h) What is the hard problem used in elliptic curve cryptography?**

The elliptic curve discrete logarithm is the hard problem.

**i) Why is it that in certain public key cryptographic tasks, discrete log problems in prime fields can be substituted by elliptic curve techniques?**

Because it is hard to calculate 2^n but easy to calculate elliptic curve for n times.

**j) Why is Weisner Quantum Money secure?**

The bank can authenticate an untampered banknote by checking all the TSS states using information that only it knows. It can also disvocer a forgery by checking all the TSS states, since 25% of the states will come out wrong.

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) Describe the difference between a pseudo random number generator and a true random number generator. How do you guard against bias in a true random number generator?**

The difference is that TRNGs use an unpredictable physical means to generate numbers(like atmospheric noise), and PRNGs use mathematical algorithms(completely computer-generated).

problem of bias:

- have to compensate for this when sample, often by passing bits through a hash function

-best to only use a few noisiest bits from each sample

- RFC4086 recommends using multiple sources + hash

**d) Name two pseudo random number generators.**

Linear Congruential Generator

Tausworth Generator

3.

**a) 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.

**b) Describe the ElGamal public key encryption and decryption algorithms.**

(1) Alice generate her key.

- chooses a secret key: 1<xA<q-1

- computes her public key: yA = a^xA mod q

(2) Bob encrypt a message to send to Alice

- Bob represents message M in range 0<=M<=q-1

-Bob chooses random integer k with 1<=k<=q-1

-Bob computes one-time key K = yA^k mod q

-Bob encrypts M as a pair of integers (C1,C2) where C1= a^k mod q and C2 = KM mod q

(3)Alice then recovers message by

- recovering key K as K = C1^xA mod q

- computing M as M = C2\*K^(-1) mod q

**c) Briefly describe the principles behind digital signatures.**

(1) Sender uses hash function to get the digest of the message, Digest1.

(2)Sender uses his private key to encrypt Digest1.

(3)Receiver uses sender's public key to decrypt the ciphertext and get Digest1.

Then the receiver uses hash function to get the Digest2 of the message.

Compare Digest1 and Digest2, and if they match, the message is valid.

**d) Describe the *Keywrap* algorithm.**

The Key wrap algorithms are intended for application such as protecting keys while in untrusted storage or transmitting keys over untrusted communication networks.