**Solutions**

**QUESTION 1 [Total 50 marks]**

1. Define each of the fundamental challenges in information security known as the CIA triangle. **[10 marks]**

**Hints**

Confidentiality: prevent unauthorized *reading* of information;

Integrity: detect unauthorized *writing* of information;

Availability: data is available in a *timely manner* when needed.

1. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important?

**[5 marks]**

**Answer**

The bank’s primary concern is with integrity of transactions, while its’ costumers will have roughly equal concerns with both.

1. Define Kerckhoffs' Principle in the context of cryptography.

**[5 marks]**

**Answer:** According to Kerckhoffs’ Principle in the context of cryptography the following basic assumptions should be respected:

* + The system is completely known to the attacker;
  + Only the key is secret;
  + That is, crypto algorithms (ciphers) are not secret.

1. What is a digital signature? Explain how this can be implemented using public key encryption.

**[10 marks]**

**Hint:** A digital signature is the equivalent of a physical signature in that it guarantees that a message was sent by a signer unaltered. If Alice wants to send a signed message to Bob, a digital signature can be implemented as follows: Alice uses a secure hashing function (e.g. MD5) to create a digest of the message. The digest is encrypted to Alice's private key. The encrypted digest is appended to the unencrypted message and sent to Bob. Bob uses the same hashing function to calculate a digest of the message. Bob decrypts the encrypted digest using Alice’s public key. If the two digests match, Bob can be sure that the message was sent by Alice and has not been changed.

1. Give the definition of a Feistel Cipher and justify if DES and AES are (or not) a Feistel Cipher. Why is the Tiny Encryption Algorithm (TEA) "almost" a Feistel Cipher?

**[10 marks]**

**Answer:**

Feistel cipher (ss nota specific block cipher!) is a type of block cipher.

Algorithm:

Split plaintext block P into left and right halves:

P = (L0, R0)

For each round i = 1, 2, ..., n, compute

Li = Ri-1

Ri = Li-1  F(Ri-1, Ki)

where F is round function and Ki is subkey.

Ciphertext: C = (Ln, Rn)

DES is a Feistel Cipher, while AES is NOT.

TEA is “almost” a Feistel Cipher because uses “ + ” and “ - “ instead of .

1. Define non-repudiation in the context of cryptography.

**[5 marks]**

**Similar Answers**

So simply, non-repudiation , means that Alice cannot repudiate (deny) a given transaction. Non repudiation can be achieved using private keys. If Alice signs her message, she cannot deny later that she was not the person who sent that message.

Non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only Bob is convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob.

1. What are the properties that a cryptographic hash function must satisfy?

**[5 marks]**

**Answer:**

Compression, efficiency, one-way, weak collision residence, strong collision residence

**QUESTION 2**

Suppose that Alice's RSA public key is *(N,* e) = (33,3) and her private key is *d* = 7.

1. If Bob encrypts the message *M =* 17 using Alice's public key, what is the ciphertext *C?* Show that Alice can decrypt *C* to obtain *M.*

**[10 marks]**

1. Let *S* be the result when Alice digitally signs the message M = 21. What is S? If Bob receives *M* and *S,* explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

**[15 marks]**

**[Total 25 marks]**

**Answer:**

1. Follow similar solution but for M=17 (instead of M=19)
2. Follow similar solution but for N=21 (instead of N=25)



**QUESTION 3**

Consider the knapsack cryptosystem. Suppose the public key consists of (18,30,7,26) and *n =* 47.

1. Find the private key, assuming *m* = 6.

**[15 marks]**

b. Encrypt the message M = 1101 (given in binary). Give your result in decimal.

**[10 marks]**

**[Total 25 marks]**

**Answer:**

