**BCT 2314 – CAT**

**Name: STANLEY NGUGI Registration Number: SCT212-0065/2017**

1. **What requirements must a public key cryptosystem fulfill to be a secure algorithm? (4 marks)**

* An adversary with the public key and or the cipher text in hand, should be unable to recover the original message
* It should be computationally easy for a party B to generate a pair of keys (Pub,Prb)
* An adversary with hand, the public key should not be able to determine the private key
* It should be computationally easy for a sender A, knowing the public key and message to be encrypted to generate corresponding cipher text (C=E(Pub,M)

1. **Outline the components of the RSA algorithm (4 marks)**

* **Plaintext**: Refers to the readable message that is fed into the algorithm as raw input.
* **Encryption algorithm**: This refers to a sequence of steps that performs various transformations on the plaintext, using the encryption keys to generate a ciphertext.
* **Public and Private keys**: Refers to unique sequence of characters that facilitate the transformations performed by the algorithm on the plain text to produce unreadable ciphertext
* **Ciphertext**: Scrambled message produced as output from encryption. Depending on the plaintext and the key for a given message, different keys will produce different cipher texts

1. **Let (𝑃𝑈𝑎, 𝑃𝑅𝑎) be the public and private key of Alice, and (𝑃𝑈𝑏, 𝑃𝑅𝑏) are the public and private key of Bob. Let 𝐻( ) be a hash function, 𝐸(𝐾𝑒𝑦,𝐷𝑎𝑡𝑎) denote an encryption, and 𝐷(𝐾𝑒𝑦,𝐷𝑎𝑡𝑎) decryption operation, || denotes a concatenation and 𝐷𝑜𝑐 be a document. Describe the digital signature algorithm performed by Alice, on the document 𝐷𝑜𝑐. (5 marks)**
2. Alice generates two keys, (𝑃𝑈𝑎,𝑃𝑅𝑎)
3. Alice keeps the private key, then sends the public key to Bob.
4. After creating the message (Doc), she generates a digest by hashing the memo using the hash function ( ).
5. She then encrypts the digest with her private key, 𝑅𝑎. The encrypted digest is the signature for the message.
6. Alice now sends the memo and digital signature to Bob.
7. **Let 𝐶(𝐾𝑒𝑦, 𝑀) denote a message authentication code function, produced for the message M and a shared key Key. Let 𝐸(𝐾𝑒𝑦, 𝑀) denote encryption of a message M with a key Key, and let || denote the concatenation. If Alice send to Bob the following information:**

**𝐸(𝐾2, 𝑀)||𝐶(𝐾1, 𝐸(𝐾2, 𝑀)) where 𝐾1,𝐾2 are shared secret keys.**

**Describe the goals of the message. (4 marks)**

* The shared secret keys are used to generate the key which enables decryption and encryption of a message by either party.
* **Authentication**. This gives the receiver (Bob), reason to believe that the message created and sent by Alice.
* **Non-repudiation**. Ensures that the sender (Alice can’t deny having sent the message later on.
* **Integrity**. Gives the assurance that the message wasn’t changed in transit.

1. **In the Diffie Hellman Key exchange protocol between user A and B both users have a**

**private key: 𝑋𝐴 = 6 and 𝑋𝐵 = 35 , respectively. The public keys are 𝑌𝐴 = 𝑎**

**𝑋𝐴 𝑚𝑜𝑑 𝑝 and**

**𝑌𝐵 = 𝑎**

**𝑋𝐵 𝑚𝑜𝑑 𝑝. What is the common key K for p = 71 and a = 7? (4 marks)**

**STEP 1**

* Alice uses her private key to calculate: 7^6 mod 71=2
* Alice shares this result with Bob.
* Bob uses his private key to calculate: 7^35 mod 71=23.
* Bob shares his result with Alice.

**STEP 2**

* Alice takes Bobs result and raises it to the power of her private number: 23^6 mod 17=8
* Bob takes Alice’s result and raises it to the power of his private number: 2^35 mod 17 =8

The Common key is 8.

1. **The RSA system was used to encrypt the message M into the cipher-text C = 6. The public**

**key is given by 𝑛 = 𝑝. 𝑞 = 187 and 𝑒 = 107 . By answering the following, try to crack**

**the system and to determine the original message M.**

* 1. **What parameters comprises the public key and the private key? (2 marks)**

Pub(n,e)

Pr(d)

* 1. **What steps are necessary to determine the private key from the public key? (2 marks)**

The Private Key d is calculated from p, q, e. For a given n and e,there is a unique number d.

d is the inverse of e modulo (p-1) (q-1). This means that d is the number less than (p-1) (q-1) Such that when multiplied by e, it is equal to 1 modulo (p-1) (q-1).

The relationship: de =1 mod(p-1)(q-1)

* 1. **Determine the private key for the given system. (5 marks)**

pq=187; e=107;

187 is a product of two primes.

The only possibilities are 17, 11.

(p-1)(q-1)=16.10 or 10.16=160.

d.e=1 mod 160.

d.170=1 mod 160.

Using Extended Euclidian Algorithm;

160(x) +107(y) =1

(160,107)160 = 107.1+53

(107, 53)107 = 53.2+1

(53, 1)53 = 53.1+0

Solve for remainders;

53=160-107.1

1=107-53.2.

Substitute 1=107-53.2

For 53;

107-(160-107)2

107-(160.2-107.2)

107-160.2+107.2

107.3-160.2

d=3

* 1. **What is the original message M? (2marks)**

C^d mod n=M

6^3 mod 187

Result: 108

1. **Recall the ElGamal cryptosystem. A community of users share a large prime p and a**

**primitive element a. Each user has a key pair (𝑥, 𝑌), where 0 < 𝑥 < 𝑝 − 1 is randomly**

**chosen and 𝑌 = 𝑎𝑥 𝑚𝑜𝑑 𝑝. Y is public and x is private. To send a message M to Alice,**

**who has key pair (𝑥𝐴, 𝑌𝐴), Bob performs the following steps:**

* + 1. **Choose a random 𝑥𝐵 with 0 < 𝑥𝐵 < 𝑝 − 1.**
    2. **Compute 𝐶1 = 𝑎, 𝑥𝐵 𝑚𝑜𝑑 𝑝 and 𝐶2 = 𝑀. 𝐴, 𝑥𝐵 𝑚𝑜𝑑 𝑝**

**iii. The ciphertext is (𝐶1, 𝐶2).**

1. **Explain how Alice decrypts the message, show the steps. (5 marks)**

The result of C1 is sent to Alice so that she can compute the secret shared key.

She will take Bobs result (C1) and raise it to the power of her private number 𝑥𝐴 so as to obtain the shared key;C1^ 𝑥𝐴 mod p.

Now that she has the shared key, she can obtain message M;

C2 =M. C1^ 𝑥𝐴 mod p.

M = C2 / C1^ 𝑥𝐴 mod p

1. **Assume that prime p = 17 and the primitive element a = 6. Bob, who has a private key 𝑥𝐵 = 12 wants to send a message M = 5 to Alice, who has a public key 𝑌𝐴 = 15. Compute the ciphertext is (𝐶1, 𝐶2). and show your steps. (5 marks)**

The result of C1 is sent to Alice so that she can compute the secret shared key.

Alice will take Bob's result (C1) and raise it to the power of her private number 𝑥𝐴 to obtain the shared key;

C1^ 𝑥𝐴 mod p.

Now that she has the shared key, she can obtain message M;

C2=M. C1^ 𝑥𝐴 mod p

M=C2/ C1^ 𝑥𝐴 mod p

1. **A Feistel cipher is used in the DES algorithm.**
   1. **Describe the operation of a Feistel cipher. (5 marks)**

The Feistel cipher is a block cipher that uses both permutation and substitution alternately. Input fed into the algorithm is a key, K i, and a block of plain text. The block is divided into two halves, LE 0 and RE 0. The blocks go through rounds of processing and then combine to produce the ciphertext block.

**Substitution** is where the plain text is uniquely replaced by a corresponding ciphertext element. In the cipher, it is performed on the left half of the data. An F function is applied on the right half of the data using input RE 0 and K i. An XOR operation is then performed between the output of the function and LE 0. The F function remains the same but the key changes with each round.

**Permutation** refers to the process in which elements are not added, deleted or replaced in the sequence. Instead, only the order in which they appear is changed. The right half side then directly moves to the left side and becomes LE 1. And the left half becomes RE 1 after the computations. The interchange of these two halves is a clear display of permutation. After several rounds, the halves finally directly interchange, hence producing the ciphertext block. Decryption occurs from the bottom up, meaning it is done in reverse order.

* 1. **Briefly describe three modes of operation of DES. (5 marks)**
     1. **Electronic Code Book (ECB) Mode -** In this mode, blocks of plain text are directly encrypted into blocks of ciphertext. For a large message, it is broken down into separate blocks of code which are then encrypted. It is advantageous because it is faster since encryption of blocks of bits is faster. And it is simple. However, it is insecure since there is a direct link between the ciphertext and plain text.
     2. **Cipher Block Chaining (CBC) Mode** - It is an advancement on ECB whereby a ciphertext is produced by encrypting the XOR output of the previous cipher block and the present plain text block. It works great for large inputs. It is also a good authentication method. However, it has one disadvantage in that parallel encryption is not possible.
     3. **Counter/ CTR Mode** - It is a simple counter-based block cipher implementation. In each round, a counter-initiated value is encrypted. It is then fed as input to XOR with the plain text, hence resulting in a ciphertext block. This mode is independent of feedback; hence it can be implemented in parallel.