ISA-562 ASSIGNMENT

**NAME:Sushmitha Konduru**

**G-NUMBER:G01456225**

Answers:

1 a) Which of the following is asymmetric cryptography?

Ans) C-RSA

   b) From the following list of cryptographic algorithm combinations, choose the combinations that can be used to generate digital signature.

Ans**)** B-SHA256 and RSA

C-SHA256 and MD5

2)Given two primes p=3, q=7 and e=5, use RSA’s public key to encrypt a message 4. (First generate the public and private key, and then encrypt the message?

Ans) Given**: p=3, q=7, e=5, M=4**

 -> **Calculate n=p x q**

n=3 x 7

**n=21**

->**Calculate φ(n)=(p-1) (q-1)**

    = (3-1) (7-1)

    = (2)(6)

**φ(n)=12**

->**Select integer e**

**e=5**

->**Calculate d such that (d\*e) mod φ = 1**

5d mod 12=1

**d=5**

->**Therefore, Public key (KU)= {e, n}**

**KU= {5,21}**

->**Private key (KR)= {d, n}**

**KR= {5,21}**

**ENCRYPTION:**

For message M, **the cipher text(C)=Me mod n**

->Given M=4,

C=45mod21

  =1024 mod 21

             =16

**Encryption:16**

3)Alice and Bob want to use the Diffie-Hellman key agreement to establish a secret key. They agree on a prime modulus p = 5, and a generator g = 2. Alice selects a private number a = 3, and Bob selects a private number b = 4. Please compute their secret key.

Ans) **Diffie-Helman key agreement:**

->Having agreed on values prime modulus **p=5**, generator **g =2** and Alex’s private number **Xa=3**, Bob’s private number **Xu=4**.

->**Deriving the public keys:**

Ya (Alice’s public key) = gXa mod p

          =23 mod 5

                      =8 mod 5

            =3

Yb(Bob’s public key) =gXb mod p

        =24 mod 5

                    =16 mod 5

        =1

->**Deriving the shared Secret key:**

K = Yb **Xa** mod p (Alice’s Secret key)

    =13 mod 5

    =1

K=Ya **Xb** mod p (Bob’s Secret key)

  =34 mod 5

  =81 mod 5

  =1

->**Computed secret key**:1

4)Two properties of a secure cipher are confusion and diffusion. Please explain

a) What is confusion?

Ans) It is one of the basic building blocks of cryptography algorithms. It ensures that the relationship between the cipher text and the key is made difficult. This technique provides that the cipher text provides no clue about the plain text. The main goal of confusion is to make it very complex to find the use even if most of the cipher-plaintext pairs are formed using a similar key, each bit of the cipher key should be based on the entire key if not and in several ways on multiple bits of the key such that changing one bit of the key should change should change the cipher text completely. This is achieved using substitution techniques

b) What is diffusion?

Ans) Diffusion is the process such that changing one bit of plain text, should change the cipher text in an unpredictable and pseudo random manner and vice vera. It hides the statistical relationship between plaintext and cipher text. It focuses on spreading the influence of each plain text element through the cipher text to distribute the information uniformly. This achieved using permutation or transposition techniques.

c) how are they achieved in des?

Confusion and diffusion are achieved in DES using substitution and permutation respectively:

**Substitution:**

->The substitution step takes place in the S-box substitution. After the 32-bit right half of the plain text is XOR’ed with the key, the 48-bit result moves to a substitution operation. The substitution is performed by eight different substitution boxes or S-boxes. The 48 bits are divided into eight 6-bit sub-blocks. Each separate box is operated on by a different S-box. Each S-box is a table of 4 rows and 16 columns. The 6-bit input of the S-box specifies under which row and column number to look for output.

Assume a 6-bit input 110011.The first and last bits combine to form 11 which corresponds to the row number-row 3 and the middle 4 bits combine to form 1001 which corresponds to the column number-column 9. The value found under 3rd row and 9th column is substituted for 110011.

The result of this substitution is eight 4-bit blocks which are recombined into a single 32-bit block. This block then moves to the next step-P-box permutation.

S-box’s features of:

-> Nonlinearity: The output of S box is not a simple function of input

->Diffusion-A small change in one part of the input to the S-box can lead to changes in output of multiple S boxes.

->Resistance against cryptanalysis.

**P-box Permutation:**

->A permutation at this point is of security value to DES.It ensures that the output of the S-box of one effect the input of multiple S-boxes in the next rounds. The 32-bit output of the S-box is permuted according to a P-box. This permutation maps each input bit to an output position, no bits are used twice and no bits are ignored-box permutation obscures any underlying patterns that might be existing in plain text and cipher text through this it defeats frequency analysis.

5)Explain the following?

a) The process of generating a digital signature, and the security objectives that can be achieved by digital signature.

Ans) Digital signature: Is a technique used to validate the authenticity and integrity of a message.

Process:

**1)**Before generating a digital signature a message digest(h) is computed by applying a hashing function(H(m)) on the message. A hash function takes an arbitrary value of input and gives a fixed value of output. The value returned by the hash function is called the message digest

H(m)=h

**2**)Signing algorithms are used to encrypt the message digest with the private key of the user generating the digital signature

s = Sign (PR, H(m))

                                                  = E (PR, H(m))

**3**)The digital signature is appended to the message(m) and sent to the receiver

**4**)The receiver when receives the message(m1) calculates the message digest H (m1) using the same hashing function as used by the sender.

**5**)The receiver then uses the public key to decrypt the encrypted hash value that was attached to the received message. This provides authenticity as only the sender has his private key and only the sender can encrypt using his private key which is able to be decrypted with the public key.

H(m) = D (PU, s)

**6**)The receiver then compares the calculated message digest and the decrypted message digest. If they both match then digital signature is valid and the message has not been tampered with. If they both do not match then the message has been tampered with or the sender’s private key does not match the sender’s public key.

if H (m1) = H(m), message authenticated

**Example**: Bob wants to send a message to alike so

Bob uses a secure hash function, such as SHA-512, to generate a hash value for the message and then encrypts the hash code with his private key, creating a digital signature. Bob sends the message with the signature attached.

When Alice receives the message plus signature, she

 (1) calculates a hash value for the message;

 (2) decrypts the signature using Bob’s public key;

 (3) compares the calculated hash value to the decrypted hash value. If the two hash values match, Alice is assured that the message must have been signed by Bob.

The security objectives that are achieved through digital signature are Data integrity, authentication and non-repudiation:

1)**Data Integrity**: An adversary may change the message but does not have the private to sign the message digest. Therefore, the integrity of the message is maintained.

2)**Authentication**: Only the sender will have the private key so a message can only be signed and sent from the sender, if the message is decrypted using the public key, then the sender is authenticated.

3)**non-repudiation**: only the sender can generate the digital signature, since only the sender owns the private key. Thus, the sender cannot deny that the message was signed by her

5b) The process of generating a message authentication code (MAC), and the security objectives that can be achieved by MAC.

Ans) Message authentication code: Message authentication code (MAC) is a small piece of information that allows the verification of the sender and the content of the message. This technique assumes that the sender and receiver both share a common secret key KAB.

If A wants to send information to B,

**1**)A calculates the message authentication code as a complex function of the message and the shared key:

MACM=F (KAB, M)

**2**)The MAC code is appended to the message and transmitted along with the message to the receiver.

**3**)The receiver performs the calculation on the received message(M1) using the shared secret key, to generate a new message authentication code.

MACM1=F (KAB, M1)

**4)**The received code is compared with the calculated code, if we assume that only the sender and the receiver have access to the secret key and if the received code matches the calculated code, then the message is authenticated and confirms message integrity.

MACM=MACM1

A popular Message Authentication Code algorithm is **HMAC**-Hash based Message Authentication Code:

HMAC-Is a technique for generating a message authentication code using cryptographic hash function and a secret key. The commonly used hash function in HMAC is SHA-1, SHA-3, MD5, SHA-256, SHA-512 but SHA-1 and MD5 are not secure as they are prone to length extension attacks so only SHA-2 is recommended now

The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function. The size of its hash output and the size and quality of the key.

The security objectives that are achieved through MAC are Data integrity, authentication and non-repudiation:

1)**Data Integrity**: Provides a way to verify if the message has been tampered by comparing the computed MAC and received MAC.

2)**Authentication**: The use of a secret key to produce the MAC provides a way to verify the authenticity of the message as only the sender and the receiver will have access to the shared secret key.

3)**Non-repudiation**: Only the sender and receiver have access to the shared secret key so the authenticity of the message can be verified.

6)Answer the questions about the CBC mode encryption as shown in the following figure

1)If two different Initialization Vectors (IVs) are used for encryption, what is the consequence for the corresponding ciphertexts?

Ans) A block cipher processes a message in the form of a fixed size block but the message is almost always bigger than the block size so the message is divided and processed one at a tieback-Cipher Block Chaining is a method of operation on the block of message.

Working:

The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block, the same key is used for each block. Through this we are chaining together the processing of the sequence of plaintext blocks.

Cj = E (K, [Cj -1 ⊕ Pj])

For decryption, each cipher block is passed through the decryption algorithm. The result is XORed with the preceding ciphertext block to produce the plaintext block.

D(K, Cj) = D(K, E(K, [Cj -1 ⊕ Pj]))

To produce the first ciphertext block, an Initialization Vector (IV) is XORed with the first block of plaintext. On decryption, the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext.

**->**If we use two different initialization vector for encrypting a message, it will produce two different ciphertext blocks. The IV is chosen in such a way that even when two same messages are given as input, the cipher text will diverge from the point IV is introduced. The cryptography operations involved in the encryption algorithm ensure that even small changes in the input or IV will cause significant change in the ciphertext generated. It has a strong avalanche effect.

2) If one plaintext block is modified, what is the consequence for the ciphertext?

If one plaintext block is modified then the corresponding ciphertext block and all the consequent ciphertext block will be affected. If one plaintext is modifying then it produces a ciphertext with an error which is carried forward and XORed with the plaintext to produce the ciphertext so the error gets carried forward towards the processing of all the blocks and generates cipher texts with error. Therefore, modifying one plaintext block effects all the ciphertext blocks.