Experiment - 11

No 1 1

Install Jcrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory network security and Management.

Installation of Jcrypt Tool :-

1) Turn on PC.
2) Go to my computer -> Local Disk D -> setup crypt tool -1-4.30.
3) Double click on it -> next -> I agree -> Install -> next -> finish.
4) Installation gets completed.

Using symmetric Algorithm :-

1) open Jcrypt tool
2) Go to file -> new -> write the content and save it.
3) Go to encrypt/decrypt -> symmetric (modern) = RC2 = Replace 00 with A1 click encrypt.
4) Go to encrypt/decrypt -> symmetric (modern) = RC2 = disk decrypt the content will appear in the new windows.
5) Go to encrypt/decrypt -> symmetric (modern)- RC4 = Replace 00 with A2.
6) Repeat step 5 and click decrypt content will

appear.

7) click encrypt.

8) Repeat step 5 for both encryption and decryption to (ECB... DESC(BC)... Triple BES (ECB)... Triple DES (BSC))

Using Asymmetric Algorithm :-

1) Go to digital signature / PKI -> PKI -> Generate import keys.

2) Give full name, last name & a PIN click generate new key pair.

3) Go to encrypt / decrypt -> Asymmetric -> RSA encryption.

4) In ~~the~~ Panel select on your name and click encrypt.

5) Go to encrypt / decrypt -> Asymmetric -> RSA decryption.

6) In the Panel select your name, enter PIN and click decrypt, content will appear.

7) Go to encrypt / decrypt -> Hybrid - RSA - AES encryption.

8) Panel appears / open document -> Generate key -> select asymmetric key -> encrypt the document symmetric -> encrypt session key asymmetric.

9) Encryption / decryption -> RSA - AES Decryption -> continue -> select your name, enter pin code click OK -> continue -> continue -> decrypted ~~your~~ content will appear

b. RSA Algorithm. →

Revest Shamir Adleman (RSA) crypto system B a public key system based on the underlying hard problems and named after it 3 inventors. The algorithm was introduced in 1978.

RSA is a public key encryption or decryption algorithm and is much slower than DES(Data Encryption Std). The key length is variable and block size is also variable. A typical key length is 512bits. RSA uses a public key and private key and uses a fact that large number extremely difficult to factorise.

The two keys used in RSA 'd' and 'e' are used for decryption and encryption. They are actually interchangeable either can be choosen one. You must keep the either private for simplicity. We will call the encryption 'e' and the decryption 'd' also because of the nature of the RSA algorithm. The key can be applied is either order.

$P = (E(DCP) = D(ECP))$

Any plain text blocks 'p' is encrypted as $p^e$ mod n because exponentiation is performed mod n factoring $p^e$ to uncover the encrypted plain text is difficult.

The RSA algorithm was 2 keys 'd' and 'e' which work in pair for decryption and encryption respectively. A plain message p is encrypted to cipher text c by

$$C = p^e \bmod n$$

The plain text is recovered by

$$P = E^d \bmod n$$

Because symmetric is modular arithmetic encryption and decryption are manually inverse and acommutative.

$$P = c^d \bmod n = (p^e)^d \bmod n$$

$$(p^d)^e \bmod n$$

This relationship means that one can apply the encryption transformation and the decrypting one or the decrypting one followed by encrypting one.

# RSA Algorithm →

## Key Generator :

- → Select P, Q prime number $P \neq Q$
- → Calculate $N = PQ$
- → Compute $Q(N) = (P-1)(Q-1)$
- → Select e such that relatively prime number where $1 < e < Q(N)$
- → Calculate D

## Public Key Generation →

| | |
|---|---|
| Public Key | $K_u = \{e, n\}$ |
| Private Key | $K_p = \{d, n\}$ |

## Encryption →

| |
|---|
| Plain text $M < N$ |
| Cipher text $C = M^e \bmod n$ |

## Decrypt →

Cipher text c
Plain text $M = C^d \bmod n = M^{cd} \bmod n$

## DES Algorithm →

The DES was issued in 1977 as Federal Information Processing Standard 46 (FIPS - 46) by National Bureau of Standards and is known as Data Encryption Algorithm (DEA).

(1) The DEA makes use of 64 bits plain text, block in length as input and 56 bits key in length.

(2) Therefore, longer plain text will be processed in multiples of 64 bits block.

(3) The original 56 bits key is used to generate 16 sub keys and are used one each for every round.

(4) The DEA uses 16 rounds of processing separately for Encryption and Decryption.

For Decryption, Cipher text is input to the DES Algorithm and sub-keys are used in reverse order. a5 - K15 to first round K14 to second round and so on upto K0 for 16 (last) round.

The strength of the DES Algorithm is 56bit key length since it is difficult to perform cryptanalysis and brute force attack is almost impractical.

## AES Algorithm →

Advanced Encryption Standard (AES) Algorithm is finalized as Rijndael AES Algorithm as FIPS PUB 197 standard in November 2001. This algorithm was developed by 2 cryptographers of Belgium country Dr. Vincent Rijmen and Dr. Joan Daeman (Rijndael).

The AES makes use of 128 bits plain text block in length as input and keys length can be 128, 192 or 256 bits.

- Common implementation of key length is usually 128 bits.

The AES does not use Fiestel Cipher Structure but processes the entire data block in parallel during each round using substitution and permutation. Accordingly, 4 stages are used 1 permutation (i.e., shift rows) and 3 substitutions (substitute bytes, mix column, add round key).

The single 128 bits input block is shown as square matrix of bytes in FIPS PUB 197(16 bytes plain text: 4 rows X 4 columns). This block is copied into the state array which will be modified at each stage of encryption and decryption.

At the end of final stage (round 10), state array is copied to an output matrix that represent either cipher text (during encryption) or plain text (during decryption).

16 X 8 = 128 bits matrix : 4 X 4

It is to be noted that the 128 bit key is also represented as a square matrix of bytes (4 rows X 4 columns).

This key is then expanded into an array of keys scheduled words of size 4-bytes each and the total no. of keys scheduled words are 44 for 128 bit key pattern.

Also the ordering of bytes within the matrix is column by column.

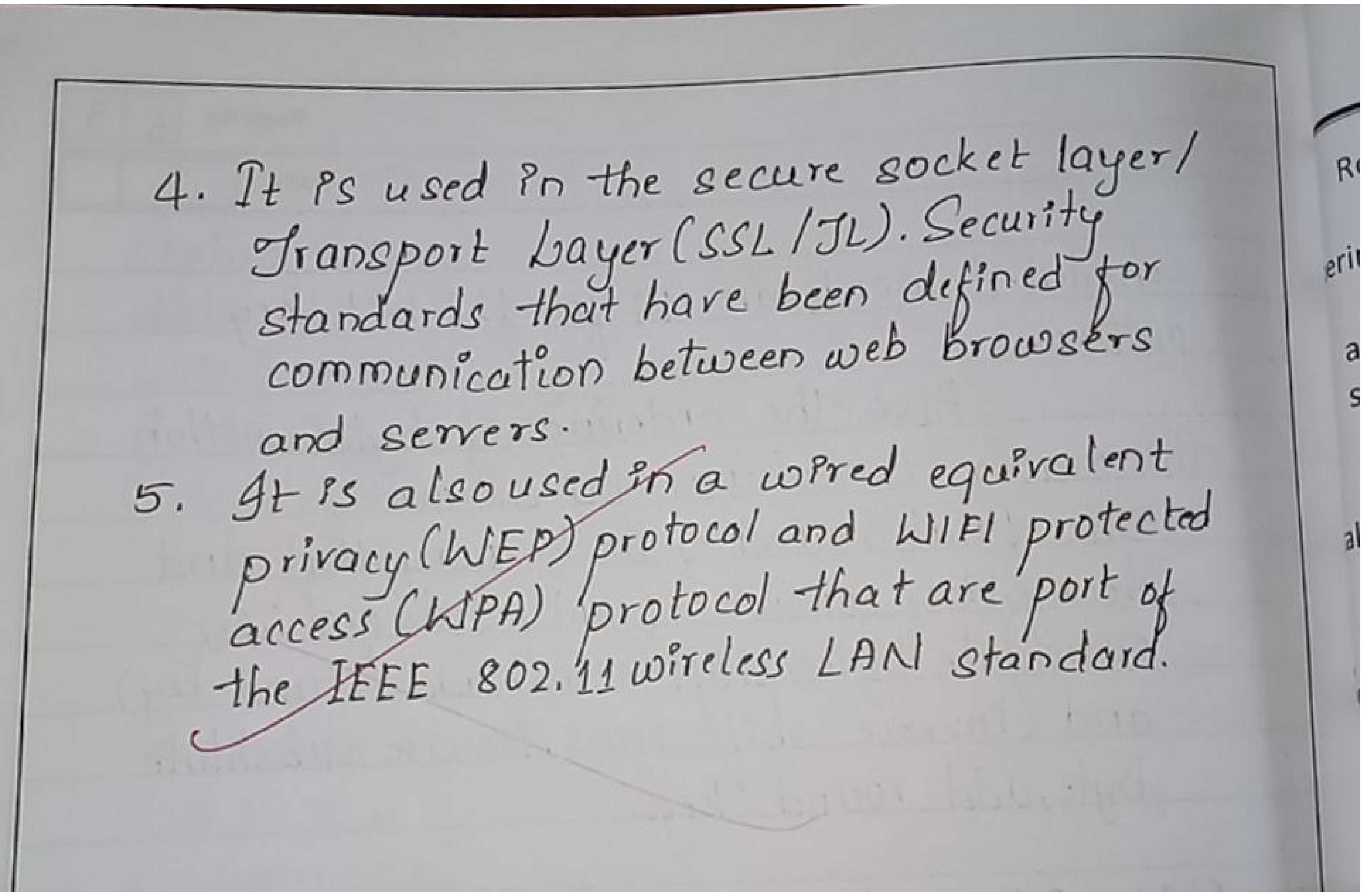
- The final round of both encryption and decryption consist of only 3 stages(i.e., substitute bytes, shift rows, add round key) and (inverse shift rows, inverse substitute byte, add round key).

## RC4 Algorithm →

RC4 is a stream cipher designed by Ron Rivest in 1987 for RSA security. The security is Rivest-Shamir-Adleman Public Key Encryption Algorithm introduced in 1978.

## Features Of RC4 Algorithm →

1. It is available key size stream cipher with byte oriented operation.
2. It is based on the use of random permutations
3. It is observed that 8 to 16 machine operations are required per output(cipher text) byte and the cipher is expected to run quickly in software.



4. It is used in the secure socket layer/ Transport Layer (SSL/TL). Security standards that have been defined for communication between web browsers and servers.

5. It is alsoused in a wired equivalent privacy (WEP) protocol and WIFI protected access (WPA) protocol that are port of the IEEE 802.11 wireless LAN standard.