Date ____/____/____
Page ____

① Cryptography –

It is an art of writing text or data in secret code. It encrypts the plain text data into unreadable format, which is called as cipher text.

It is based on mathematical algorithms. These algorithms use a secret key for the secure transformation.

In cryptography, each person receives a pair of keys, called the public-key and the private key. Each person's public key is published while the private key is kept secret.

Anyone can send a confidential message using public information, but it can only be decrypted with a private-key that is in the sole possession of the intended recipient.

~~② Classical cipher comp~~

② Classical Cryptographic Techniques –

(1) Substitution Techniques – A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Some of the substitution techniques are –

(i) Caesar Cipher – It involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. Eg – A B C ⇒ D E F (Plain Text → Cipher Text)

Encryption algorithm → $C = E(3, p) = (p+3) \bmod 26$

General caesar algorithm → $C = E(k, p) = (p+k) \bmod 26$

Decryption algorithm → $p = D(k, C) = (C-K) \bmod 26$

(ii) Monoalphabetic substitution cipher – It relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Eg – if 'a' is encrypted to 'R', then every time we see the letter 'a' in the plaintext, we replace it with the letter 'r' in the ciphertext.

(iii) Playfair Cipher – It is based on the use of a 5×5 matrix of letters constructed using a keyword.

The matrix is constructed by filling in the letters of the keyword (– duplicates),

from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. One place have two letters ~~same~~ in the same ~~row~~ place.

Plaintext is encrypted two letters at a time, according to the following rules-

(1) Repeating plaintext letters that are in the same pair are separated with a filler letter.

(2) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.

(3) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

(4) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

(iv) Hill Cipher - This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a=0, b=1...)

For m = 3, the system can be described as -

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

$$\Rightarrow (c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$C = PK \bmod 26 = E(K, P) \quad \text{(Encryption)}$$
$$P = CK^{-1} \bmod 26 = D(K, C) \quad \text{(Decryption)}$$

(v) Polyalphabetic substitution Cipher - It use different monoalphabetic substitution as one proceeds through the plaintext message. Features -

(i) - A set of related monoalphabetic substitution rules is used.

- A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher - In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext A

$C = C_0 C_1 \ldots C_{m-1} = E(K, P) = E[(K_0, K_1, \ldots, K_{m-1}), (P_0 P_1 \ldots P_{m-1})]$

$= (P_0 + K_0) \bmod 26, (P_1 + K_1) \bmod 26, \ldots, (P_{m-1} + K_{m-1}) \bmod 26,$

$(P_m + K_0) \bmod 26, (P_{m+1} + K_1) \bmod 26, \ldots (P_{2m-1} + K_{m-1}) \bmod 26 \ldots$

General Equation, $\boxed{C_i = (P_i + K_{i \bmod m}) \bmod 26}$

Decryption is given as, $P_i = (C_i - K_{i \bmod m}) \bmod 26$

Vernam Cipher - Keyword is choosen as long as the plain text and has no statistical relationship to it.

$\boxed{C_i = P_i \oplus K_i}$ $i \rightarrow$ ith binary digit, $\oplus \rightarrow$ XOR operation

(vi) One time Pad - Use random key as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message.

(2) Transposition techniques -

By performing some sort of permutation on the plaintext letters.

Rail fence technique - Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. Eg - PRIVANSHU GUPTA

Rail fence of depth 2 is given as, P I A S U U T ⇒ PIASUUTRYNHGPA

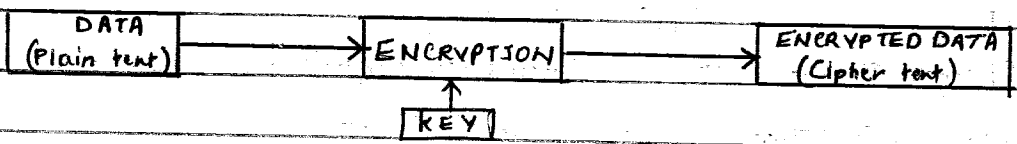
R Y N H G P A

**** A more complex scheme to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

(3) Encryption -

It is the process of converting data into a secret code. It is the most effective way to achieve data security.

To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.



(4) Decryption -

It is the process of decoding data that has been encrypted into a secret format. It requires a secret key or password.

Public key cryptography encryption and decryption is performed with public and private keys.

CODE BREAKING -

(1) Methodologies -

Various methodologies used for code breaking are -

(1) Using Brute-force
(2) Frequency Analysis
(3) Trickery and deceit
(4) One-time pad

(2) Cryptanalysis (Code Breaking or Cracking the code) -

It is the study of methods for obtaining the meaning of the encrypted information without accessing the secret information. Typically, this involves finding the secret key.

It is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general.

However, cryptanalysis usually excludes attacks that do not primarily target weaknesses in the actual cryptographic methods such as bribery, physical coercion, burglary, keystroke logging, and so on.

(3) Cryptography attacks -

They are based on the assumption that the cryptanalyst has knowledge of the encrypted information. There are mainly five types of cryptography attacks -

(1) Ciphertext only attack - Encryption algorithm and ciphertext is are known to Cryptoanalyst.

(2) Known Plaintext attack - Encryption algorithm, Ciphertext and one or more plaintext are known to Cryptoanalyst.
(- ciphertext pairs)

(3) Chosen Plaintext attack - Encryption algorithm, ciphertext and plaintext (chosen by cryptoanalyst) are known to cryptoanalyst.

(4) Choosen Ciphertext attack - Encryption algorithm, Ciphertext and a ciphertext (chosen by cryptanalyst) are known to Cryptanalyst

(5) Choosen Text attack - Encryption algorithm, Ciphertext, a plaintext (chosen by cryptanalyst) and a ciphertext (chosen by cryptanalyst) are known to Cryptanalyst.

Cryptanalyst chooses plaintext (or ciphertext), corresponding ciphertext (or decrypted plaintext) is generated with the secret key.

Adaptive choosen-plaintext attack and Rubberhose attack are two more types of Cryptography attack.

(4) Brute-Force attack -

The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success. It depends on several factors -

(1) How long can the key be?

(2) How many possible values can each component of the key have?

(3) How long will it take to attempt each key?

(4) Is there a mechanism which will lock the attacker out after a number of failed attempts?

(5) Use of Cryptography -

(1) It is used to protect data from theft and alteration.

(2) It is used to provide secure communication on any untrusted medium such as Internet.

(3) It is used to authenticate the sender and the recipient.

(4) It is used to provide privacy and integrity.

(5) It is used to protect web transactions and e-commerce applications.

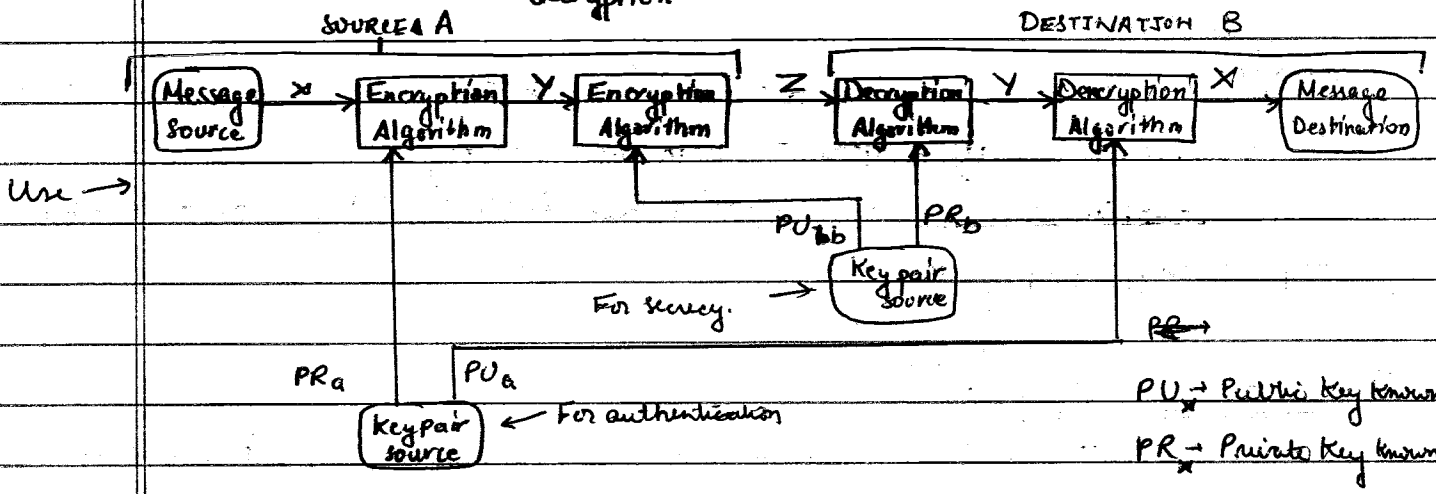
(6) Public Key Cryptography -

It uses one key for encryption and another for decryption. One key is designated as a public key which is open to public and the other key is designated as a private key which is kept secret secret.

(7) Principles of Public key cryptosystems (Asymmetric cryptography)

Principle → plaintext —encryption, public key e→ ciphertext

ciphertext —private key d, decryption→ plaintext



Applications -

(1) Encryption/Decryption (2) Digital signature (3) Key exchange

CRYPTOGRAPHIC ALGORITHMS -

(1) RSA (Rivest Shamir Adleman) -

It is a public-key cryptosystem. It uses modular arithmetic, and elementary number theories to perform computations using two large prime numbers.

RSA encryption is widely used and is the de-facto encryption standard.

→ Algorithm -

→ Key Generation Receiver -

Select p, q	p and q are both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	$\phi(n)$ is a Euler totient function
Select Integer e	$\gcd(\phi(n), e) \leq 1 \; ; \; 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

→ Encryption by sender with receivers public key -

Plaintext ⇒ $M < n$ ~~Ciphertext~~ Ciphertext ⇒ $C = M^e \bmod n$

→ Decryption by receiver with receiver's public key -

Ciphertext ⇒ C Raw Plaintext ⇒ $M = C^d \bmod n$

→ RSA attacks are -

(1) Brute force attack

(2) Mathematical attack → factoring the product of two primes

(3) Timing attack → depend on the running time of the decryption algorithm

(4) Chosen ciphertext attack

Modifying the plaintext using a procedure known OAEP (Optimal asymmetric encryption padding) to avoid Chosen ciphertext attack.

(2) Data Encryption Standard (DES) -

It is algorithm for encrypting and decrypting unclassified data. It is a block cipher that takes a plaintext string as input and creates a ciphertext string of the same length.

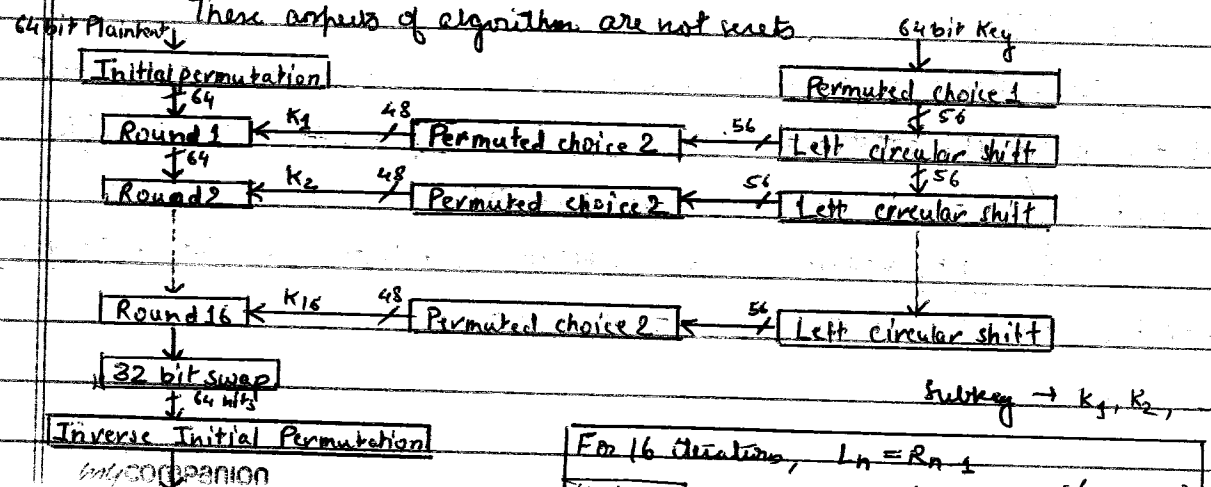
It uses a symmetric key, which means that the same key is used to convert ciphertext back into plaintext. The DES's block size is 64 bits.

The key size is also 64 bits, although 8 bits of the key are used for parity, which makes the effective DES's key size 56 bits.

~~DES acts~~

Algorithm - DES acts on 64-bits blocks of the plaintext. It invokes 16 rounds of permutations, swaps and substitutions. The standard includes tables describing all of the selection, permutation, and expansion operations.

These aspects of algorithm are not secret.



RC → Rivest Cipher

DES Decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.

③ RC4 –

It is a variable key size stream cipher with byte-oriented operations, and is based on the use of a random permutation.

Algorithm –

```
/* Initialization */                    State vector S → 256 bytes contains
for i=0 to 255 do                       permutation of all 8 bit numbers from
  S[i] = i;                             0 to 255.
  T[i] = K[i mod keylen];               T → Temporary vector.
/* Initial Permutation of S */          Use T to produce initial permutation of S
  j=0;
  for i=0 and to 255 do
      j = (j + S[i] + T[i]) mod 256;
      Swap (S[i], S[j]);
/* Stream Generation */                 Cycling of all the elements of S[i]
  i,j = 0;                              After S[255] is reached, the process
  while (true)                          continues, starting over again at S[0].
    i = (i+1) mod 256;
    j = (j + S[i]) mod 256;
    Swap (S[i], S[j]);
    t = (S[i] + S[j]) mod 256;
    k = S[t];
```

For encryption and decryption, a byte k is generated from S by selecting one of the 255 entries in a systematic fashion. As each value of k is generated, the entries in S are once again permuted.

To encrypt, XOR the value k with the next byte of plaintext. To decrypt, XOR the value k with the next byte of ciphertext.

Date ___/___/___
Page ___

④ RC5 -

It is a parameterized algorithm with a variable block size, variable key size and a variable number of rounds.

RC5 is word-oriented → Two-word input and Two-word output

Representation - RC5-w/r/b

w → word size, r → number of rounds, b → number of bytes in key.

→ Three components of RC5 are -

(1) Key expansion algorithm -

Magic constants → $P_w = Odd((e-2)2^w)$, $Q_w = Odd((\phi-1)2^w)$

Step-1 - Convert secret key bytes to words

```
for i = b-1 downto 0 do
    L[i] = (L[i] <<< 8) + K[i];
```

Step-2 - Create an expanded key table, S[0..t-1], t = 2(r+1) w-bit words

Initialize array S,

```
S[0] = Pw;
for i = 1 to t-1 do
    S[i] = S[i-1] + Qw;
```

Step-3 - Mix the secret key into table, S

```
i = j = 0;   A = B = 0;
do 3* max(t,c) times:
    A = S[i] = (S[i] + A + B) <<< 3;
    B = L[j] = (L[j] + A + B) <<< (A+B);
    i = (i+1) mod(t);
    j = (j+1) mod(c);
```

(2) Encryption algorithm -

```
A = A + S[0];   B = B + S[1];
for i = 1 to r do
    A = ((A XOR B) <<< B) + S[2*i];
    B = ((B XOR A) <<< A) + S[2*i + 1];
```

(3)

(3) Decryption algorithm -

for i=r downto 1 to

B = ((B - S[2*i+1]) >>> A) XOR A;

A = ((A - S[2*i]) >>> B) XOR B;

B = B - S[1]; A = A - S[0];

→ RC5 attacks -

(1) Exhaustive search (3) Timing attacks

(2) Differential Cryptanalysis (4) Linear cryptanalysis

(5) RC6 -

It is a symmetric key block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard (AES) competition.

It has a block size of 128 bits and support key sizes of 128, 192 and 256 bits.

RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operation. Although RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word.

Key expansion algorithm is identical to RC5

Encryption algorithm -

B = B + S[0]; D = D + S[1];

for i = 1 to r do {

t = (B*(2B+1)) <<< lg w;

u = (D*(2D+1)) <<< lg w;

A = ((A XOR t) <<< u) + S[2i];

C = ((C XOR u) <<< t) + S[2i+1];

(A, B, C, D) = (B, C, D, A)

}

A = A + S[2r+2];

C = C + S[2r+3];

Decryption algorithm -

C = C - S[2r+3];

A = A - S[2r+2];

for i = r downto 1 do {

(A, B, C, D) = (D, A, B, C)

u = (D*(2D+1)) <<< lg w;

t = (B*(2B+1)) <<< lg w;

C = ((C - S[2i+1]) >>> t) ⊕ u;

A = ((A - S[2i]) >>> u) ⊕ t;

}

D = D - S[1]; B = B - S[0];

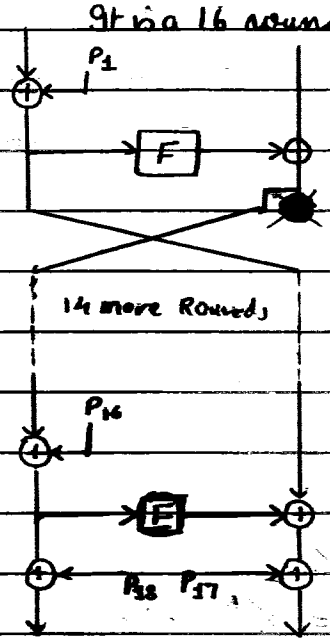
Date ____/____/____
Page _____

(6) Blowfish -

It is a 64-bit block cipher that uses a key length that can vary between 32 and 448 bits.

It includes key-dependent S-boxes and a highly complex key schedule

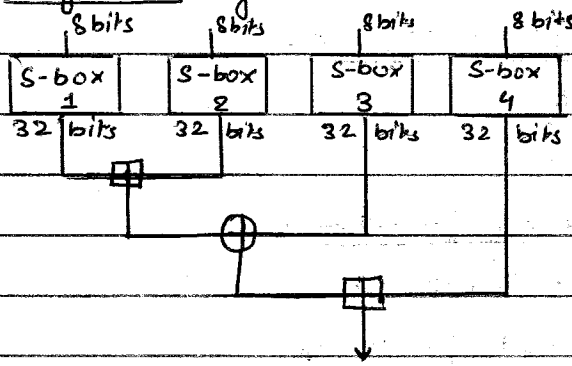
It is a 16 round Feistel Cipher and uses large key-dependent S-boxes



Encryption algorithm -

Each line represents 32 bits. The algorithm keeps two subkey arrays - 18-entry P-array and four 256-entry S boxes.

F-function is given as -



Decryption algorithm - It is exactly the same as encryption, except that P1, P2, P18 are used in reverse order.

(7) Key Management -

→ Key Exchange Problem - It involves -

(1) Ensuring that keys are exchanged so that the sender and receiver can perform encryption and decryption.

(2) Ensuring that an eavesdropper or outside party cannot break the code.

(3) Ensuring the receiver that a message was encrypted by the sender.

→ Key Distribution Centers (KDCs) - It is a single, trusted network entity with which all network communicating elements must establish a shared secret key.

→ Public Key Management - Several solutions are -

(1) Public announcements where any user can broadcast their public keys or send them to selected individuals.

(2) Public directory maintained by a trusted authority

(3) Certificate Authority (CA) to distribute certificates to each communicating element.

→ ~~Key Escrow~~ - 9t

→ Key Escrow - 9t is a scheme in which a copy of the secret key is entrusted to a third party.

⑧ Diffie-Hellman Key Exchange -

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values.

Algorithm -

→ Global Public Elements -

q	prime number
α	$\alpha < q$ and α a primitive root of q

→ User A Key Generation -

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

→ User B Key Generation -

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$
→ Calculation of secret key by User A -	$K = (Y_B)^{X_A} \bmod q$
→ Calculation Of secret key by User B -	$K = (Y_A)^{X_B} \bmod q$

To hack the algorithm, Hacker have to calculate $X_B = d\log_{\alpha,q}(Y_B)$ that is $Y_B \equiv \alpha^i \pmod q$ where $0 \le i \le (q-1)$

The exchange protocol is insecure against a man-in-the-middle attack.

⑨ Elliptic curve cryptography -

It is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. It requires smaller keys as compared to others to provide equivalent security.

Elliptic curve equation is given as, $y^2 = x^3 + ax + b \bmod p$

Date ___/___/___
Page ___

→ Algorithm -

→ Global Public Elements -

$E_q(a,b)$ elliptic curve with parameters a, b and q, where q is a prime or an integer of the form 2^m

G point on elliptic curve whose order is large value n

→ User A Key Generation -

Select private n_A $n_A < n$

Calculate public P_A $P_A = n_A \times G$

→ User B Key Generation -

Select private n_B $n_B < n$

Calculate public P_B $P_B = n_B \times G$

→ Calculation of secret key by User A - $K = n_A \times P_B$

→ Calculation of secret key by User B - $K = n_B \times P_A$

→ Encryption - $C_m = \{KG, P_m + KP_B\}$

$K \rightarrow$ random positive integer, $P_m \rightarrow$ message

→ Decryption - $P_m + KP_B - n_B(KG) = P_m + K(n_B G) - n_B(KG) = P_m$