Diffe-Hellman key Exchange Algorithm:—

Key should be prime no. (large prime no.)

Why Prime No.

Because it has only 2 factors 1 & itself

Alice
Bob

I Both sender & receiver will decide two prime no.
n ; g → Prime No.

II Sender will decide any no. either pn or npn

Alice , x ; $A = g^x \bmod n$

III Alice send A to Bob.

IV Bob , y ; $B = g^y \bmod n$

V Bob send B to Alice

VI Alice will calculate the key

Alice → $K1 = B^x \bmod n$

VII Bob will calculate the key

Bob → $K2 \bmod n$

$K_1 = K_2$

Ex— 1. $n = 11$, $g = 7$

2. Alice → $A = 7^3 \bmod 11$ $x = 3$
$= 9$

3. Alice → 2 → Bob

4. Bob → $B = 7^6 \bmod 11 = 4$ $y = 6$

5. Bob → 4 → Alice

6. $k_1 = 4^3 \bmod 11 = 9$

7. $k_2 = 2^6 \bmod 11 = 9$

Advanced Encryption Standard (AES)

Upgraded form of DES

It was first proposed by Rijndael in 2000

128-bit Plain Text

↓

128 bit Cipher Text

Rounds	Length of key	version
10 →	128 bits	AES-128
12 →	192-bits	AES-192
14 →	256-bits	AES-256

DES

64 bit Plain Text

← 56 bit key

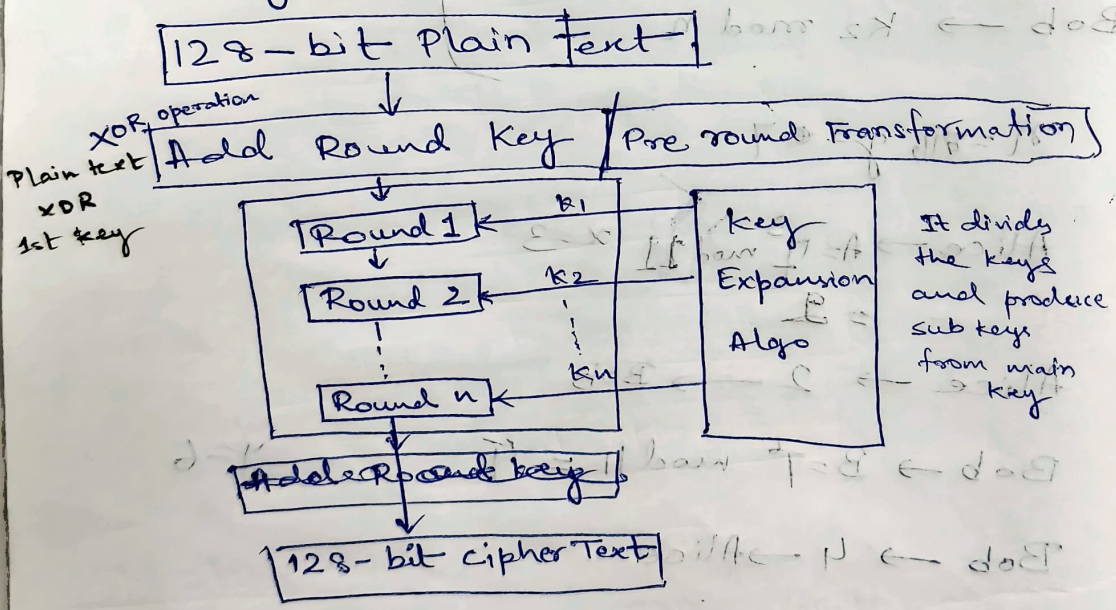
64 bit cipher text

16 rounds

each round have 5 steps

AES is more secure than DES because of the no. of rounds

Working Process of AES



Steps

1. Substitution Bytes
2. Shift Rows
3. Mix Columns
4. Add Round key

128 → No. of rounds + 1 = 10 + 1 = 11

Means k0 to k11

AES

S box ⟶ 16 × 16 matrix

S box contains hexadecimal values

1 1 1 1 — Rows

1 1 1 1 — Column

Newly formed matrix is known as state Matrix

After 1st step

Step II Matrix

3A	1B	7	4D
9	7D	4F	3E
5E	8	3F	2B
5C	3D	7C	5B

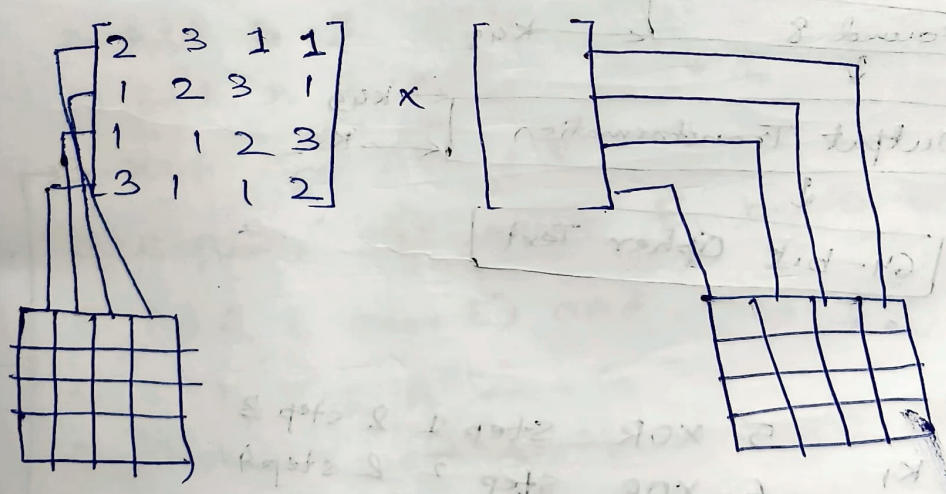
State Matrix

left shift ⟶

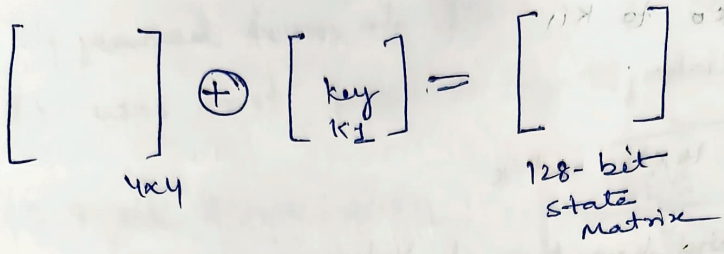
3A	1B	7	4D	0 shift
7D	4F	3E	9	1 shift
3f	2B	5E	8	2 shift
5B	5C	3D	7C	3 shift

Step 3 Mix columns

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times$$



Step 4



Last round only 3 steps are there and step 3 is ignored or discarded.

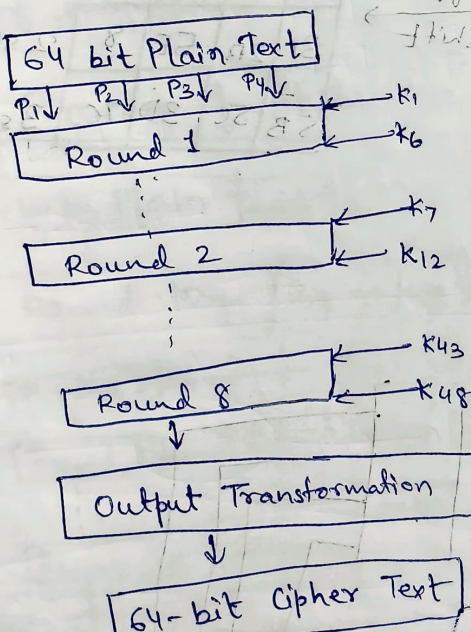
International Data Encryption Algorithm (IDEA)

Plain Text: 64 bits

Key : 128 bit

Round : 8 round

No. of steps in each round : 14



14 steps are:

1) Multiply P_1 & K_1
2) Add P_2 & K_2
3) Add P_3 & K_3
4) Multiply P_4 & K_4
5. XOR Step 1 & step 3
6. XOR step 2 & step 4
7. Multiply step 5 & K_5
8 Add step 6 & step 7
9 Multiply step 8 & K_6
10 Add step 7 & step 9

11. XOR step 1 & step 9 (P_1 for next steps)
12. XOR step 3 & step 9 (P_2 ")
13. XOR step 2 & step 10 (P_3 ")
14. XOR step 4 & step 10 (P_4 ")

For output Transformation,
4 subkeys ($K_{49} - K_{52}$) + ~~$P_1 - P_4$~~ $P_1 + P_2 + P_3 + P_4$

Rivest Cipher - 5 (RC5) :-

No of key & No. of round is variable.

Key - 0-255 (should be 8 bit)

Round → 0-255

Plain Text size → 16, 32, 64

Steps
XOR
C.L.S (circular left shift)
Add subkey

1. Plain text is divided into two equal parts, A, B
2. Add A & S[0] (1st subkey) → C
   Add B & S[1] → D
   set counter i = 1
3. XOR C & D → E
4. Circular left shift E by D bits
5. Add E (new E) and S[2i] → F
6. XOR E & F → G
7. Circular left shift G by F bits
8. Add G and S[2i+1] → H

   increment i by 1;

   C = F
   D = H

   i < 8 ? Yes / No

   Stop

Blowfish by Bruce Schenein

It is symmetric algo.

Key
~~Plain Text~~: 32 – 448

Plain Text : 64 bit

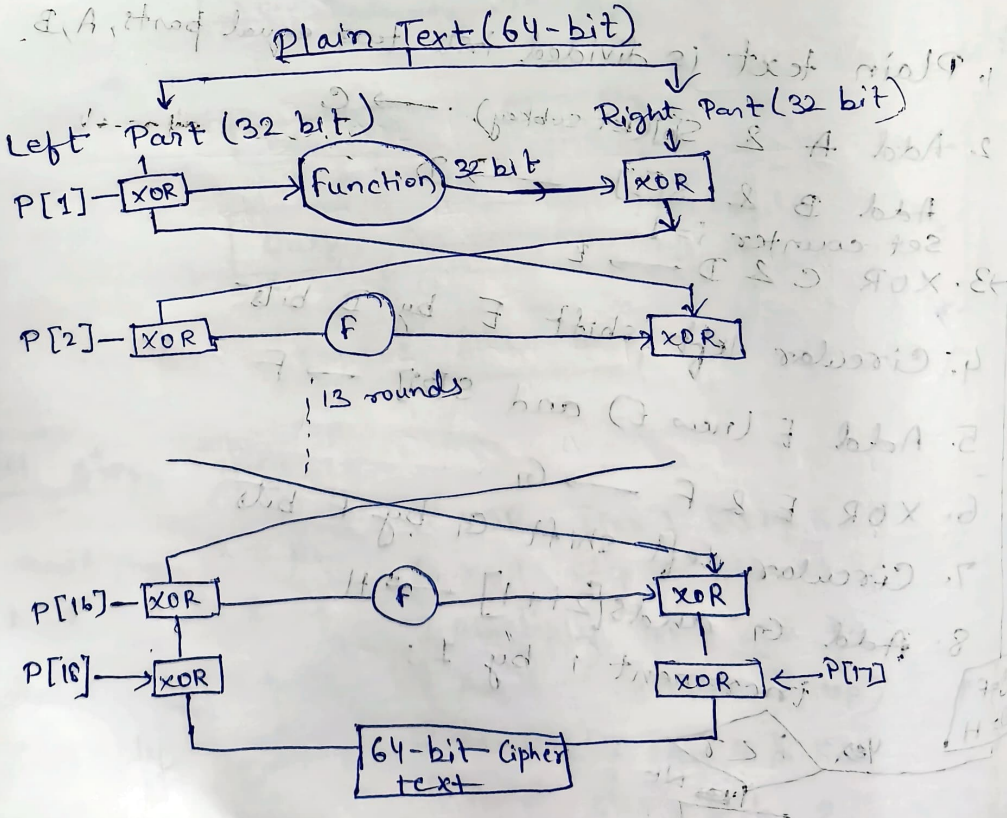
14 subkeys are generated from the main key

P- Arrays – 18

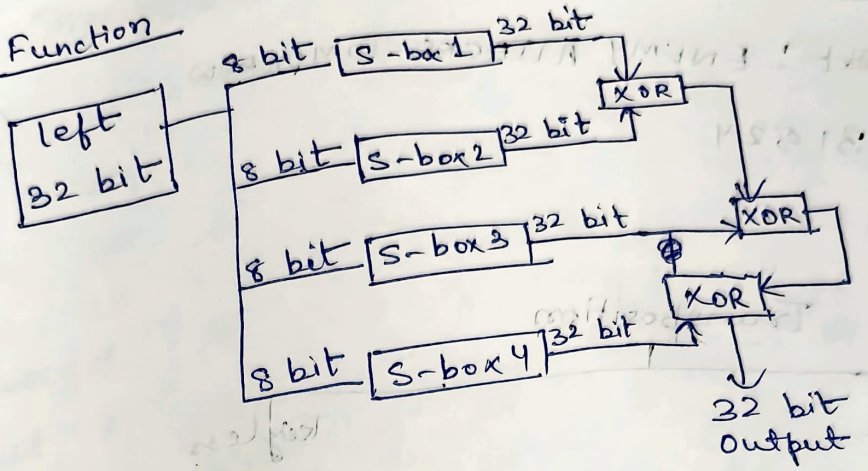
P-Arrays are hexadecimal values with 1D array

P[1] = P[1] XOR S[1]
P[2] = P[2] XOR S[2]
⋮ ⋮
P[14] = P[14] XOR S[14]
P[15] = P[15] XOR S[1]
P[16] = P[16] XOR S[2]
P[17] = P[17] XOR S[3]
P[18] = P[18] XOR S[4]

4 Sbox – 256 bit



Function



Row Transposition Technique / Simple columnar Technique

Plain Text: All the best for your exams

Key: Integer value Ex: 51324, 12345, CRYPTO 146352

Key: 146352

1st iteration

1	4	6	3	5	2
A	L	l	t	h	e
b	e	s	t	f	o
r	y	o	u	r	e
x	a	m	s	y	z

→ Last alphabets.

↳ Dummy characters / Bogus characters

Double Columnar

~~Cipher text: Abrx eoez ttus~~

Temporary Cipher text: Abrx eoezttusleyahtryldsom

2nd iteration

1	4	6	3	5	2
A	b	r	x	e	o
e	z	t	t	u	s
l	e	y	a	h	f
r	y	l	s	o	m

Cipher text: Aelrbzeyrtyl xtaseuhoosfm

original cipher ~~text~~

Keyed Transposition Technique

Plain Text: ENEMY ATTACKS TOMORROW

Key : 31524

Transposition

- keyed
  - (Simple columnar / Double " / Keyed Transposition)
- keyless (Rail Fense)

As key size is 5 so we have to divide Plain text into 5 blocks

Plain Text:-

1	2	3	4	5
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	M
O	R	R	O	W
↓	↓	↓	↓	↓
E	E	Y	N	M
T	A	C	T	A
T	K	M	S	O
R	O	W	R	O

Cipher Text: EEYNMTACTATKMSOROWRO

Vernam Cipher (Substitution Technique)

Plain Text: HOW ARE YOU

Key: NCBTZQARX

Size of the key & Plain text are same (given)

	7	14	22	0	17	4	24	14	20
Plain Text:	H	O	W	A	R	E	Y	O	U
Key:	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
Add →	20	16	23	19	42	20	24	31	43
	20	16	23	19	16	20	24	5	17
	U	Q	X	T	Q	U	Y	F	R ← Cipher Text

No. greater than 25 we have to substract that no. from 26

Decryption

		X	T	Q	U	Y	F	R
U	Q	23	19	16	20	24	5	17
20	16	B	T	Z	Q	A	R	X
N	C	1	19	25	16	0	17	23
13	2	22	0	-9	4	24	-12	-6
Sub 7	14	22	0	17	4	24	14	20
Add 7	14	W	A	R	E	Y	O	U
H	O							

Cryptography

↳ art / study / graphical representation

Security

Types of Security

i) No security
ii) Security through Obsecurity (Hide something)
iii) ID & Password
iv) Encryption

Principle of security

- Access Control
- C Confidentiality
- I Integrity
- A Availability
- Non repudiation

Attacks

- Passive attack: A → B, C → (C can see but can't edit)
- Active attack: A → B, C can see & can modify messages

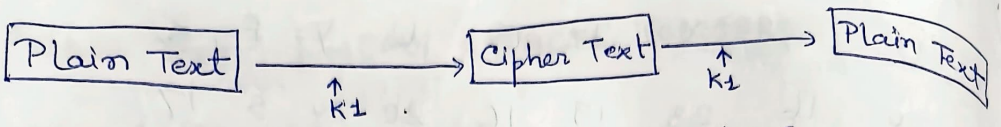
Cryptography

An art / science for achieving security through encryption.

i) Symmetric key cryptography (private)
ii) Asymmetric key cryptography (public)

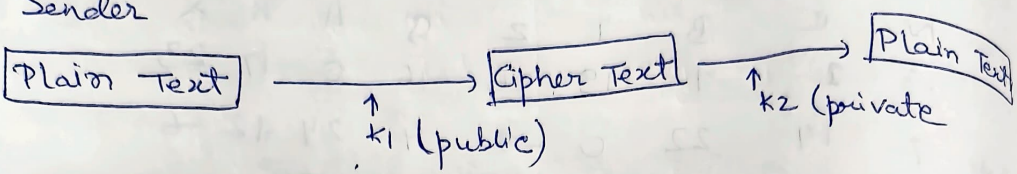
Sender

Reciever



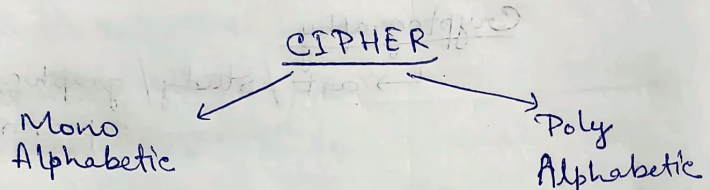
Sender

Receiver



Algorithm

Ceaser Cipher



CIPHER TECHNIQUES

- Substitution
- Transposition

Substitution methods has 2 classification

1) Monoalphetic Cipher

2) Polyalphetic Cipher

For encryption : $C(P) = (P+k) \bmod 26$

C — Cipher Text, P — Plain text, k — position

For decryption: $P(C) = (C-k) \bmod 26$

-ve → +26

P ⟶ UNIVERSITY

$C(U) = (U+4) \bmod 26$
$= (20+4) \bmod 26$
$= 24 \rightarrow Y$

$C(N) = (N+4) \bmod 26$
$= 13+4 \bmod 26$
$= 17 \rightarrow R$

$C(I) = (I+4) \bmod 26$
$= 8+4 \bmod 26$
$= 12 \rightarrow M$

$C(V) = (V+4) \bmod 26$
$= 25 \rightarrow Z$

$C(E) = (E+4) \bmod 26$
$= 8 \rightarrow I$

$C(I) = (I+4) \bmod 26$
$= 12 \rightarrow M$

$C(R) = (R+4) \bmod 26$
$= 21 \rightarrow V$

$C(S) = (S+4) \bmod 26$
$22 \rightarrow W$

$C(T) = (T+4) \bmod 26$
$= 23 \rightarrow X$

$C(Y) = (Y+4) \bmod 26$
$= 28 \bmod 26$
$2 \rightarrow C$

YRM = I V W MXC

↓ Decryption

$(C-k) \bmod 26$

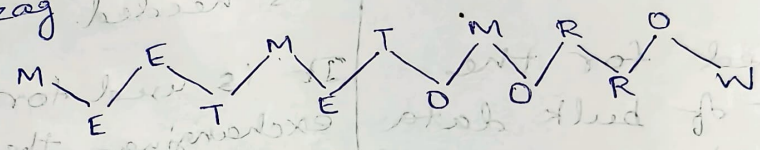
Transposition Method

Rail Fense Technique:-

Plain Text → MEET ME TOMORROW

*If the key is not present remember Key = 2

Zig-zag



Cipher Text: MEMTMROETEOORW

NOTE: Cipher Text doesn't have any space.

Symmetric key Cryptography

i) Private key (Similar key for both encryption & decryption)

ii) Hash code is known message Digest

iii) Algorithm DES, IDEA, AES

Assymmetric key Cryptography

ii) Public key (Encryption) & private key of reciever decryption

iv) RSA algo

Hash code → (Hash fn) → Hash code → Message digest MD5

Symmetric and Asymmetric

Symmetric	Asymmetric
i) This is also known as private key or secret key cryptography	This is also known as public key cryptography
ii) Only one key is used for both encryption & decryption	Two different keys (public key and private key) are used for encryption & decryption respectively.
iii) This is faster in execution	This is slower in executing
iv) It is less complex and less compational power is required.	It is more complex and more computational power is needed.
v) It is used for the transfer of bulk data (because it executes faster)	It is used for secretly exchanging the secret key
vi) Sharing the key between sender and receiver is not safe.	No problem of key sharing because of private key concept
vii) Commonly used algorithm are DES, AES, RC5, DDES DBDES etc	Commonly used algorithm are RSA, DSA etc.

DES Analysis

Avalanche effect - A small change in plain text or the key should create a significant change in the cipher text. This is called avalanche effect

completeness effect - Each bits of the cipher text needs to depend many bits of the plain text This is ~~des~~ DES Analysis

Disadvantage of DES / Weakness

i) Key size: In DES 56 bit keys is required for encryption. Hence, a total of 2^{56} combinations can be made out of these 56 bit keys. In todays parallel processing, it is very easy to crack the actual key.

ii) Weak keys: There are 4 weak keys

i) These are 1st all 0's

ii) All 1's

iii) Half 0's

iv) Half 1's

Semi-weak keys:

i 6 pairs of keys are called semi weak keys.

Possible weak keys

There are 48 possible weak keys out of 2^{56} combinat

Key clustering:

It means that two or more keys can create a same cipher text from the plain text.

Weakness in cipher design:

Two specifically choosen input 2-s box array can create same output