CT-486 (NIS)

Cryptography (Encryption)

plaintext $\xrightarrow{E}$ Cyphertext

1) Given - Cyphertext Only
2) Given - Cyphertext + Samples $(P_1, C_1)(P_2, C_2)$
   (Known plaintext attack)
3) Given - Cyphertext + Samples as per choice
   $(P_1, C_1)(P_2, C_2)$

8bits $\longrightarrow$ 256
9bits $\longrightarrow$ 512

Key Size	No. of keys	1 decryption / μsec
32bits	2^{32}	36.8 minutes
DES Scheme (56 bits)	2^{56}	1142 years
AES Scheme (128 bits)	2^{128}	5.4×10^{24} years
3DES (168 bits)	2^{168}	5.9×10^{36} years

Scanned with CamScanner

cipher : F I F L R B N I T J M M Q

cipher text :

FIFLRBNITJMMQ

10^{-6} decryption / μsec

2.15 milisec

10.02 hrs

5.4×10^{18} years

5.9×10^{30} years

DES and 3DES means to apply DES 3 times.
(difference)

Computational Security — none is able to compute scheme or break it. will take particular duration

Unconditional Security — no difference will be affected on its scheme

Basic Encryption Techniques :

1) Substitution :

Caesar Cipher

T F D S F U
S E C R E T

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

21	22	23	24	25
V	W	X	Y	Z

plaintext

no. of shifts

$$E(P, K) = C$$

$P + K$

$P = CAR$ $\qquad$ $\therefore (P+K) \bmod 26$

$Key = 9$

	C	A	R
	2	0	17
Key	9	9	9
P+K	11	9	26
	L	J	A

$P = XYZ$

$Key = 19$

	X	Y	Z
	23	24	25
	19	19	19
	42	43	44
	↓	↓	↓
	16	17	18
	Q	R	S

mod 26

For Decryption $\quad D(C-K) \bmod 26$

Scanned with CamScanner

18/10/23

Playfair Cipher (Charles Wheatstone 1854)

friend Baron Playfair

Secret Keyword: MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

e.g.
FLOOR
OO is duplicate
FLOXOR

Plaintext: NEDUNIVERSITYX
Ciphertext: MGCZAGUFATKSBW

Rule 1: Make pairs (No duplication in pair)

Rule: we have to the first letter we focus on horizontal

Scanned with CamScanner

2) PHONEX
VFNATU

If 2 letters are in same row, col we will take next character after that letter.

(Assignment)

Q#1) Frequency analysis of individual letters technique would be helpful to break this type of substitution? Justify your answer with a simple example?

Q#2) Write the decryptive example for this playfair cipher.

Scanned with CamScanner

23/10/23

Hill Cipher: by Lester S. Hill

Secret key is a nxn matrix

Taking NED

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 13 \\ 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 177 \\ 263 \\ 373 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 \\ 3 \\ 9 \end{pmatrix}$$

Substitution Cipher VDJ

Plaintext: NEDUET
13 4 3 20 4 19

Taking UET

$$= \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 20 \\ 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 235 \\ 514 \\ 753 \end{pmatrix}$$

$$= \begin{pmatrix} 235 \\ 514 \\ 753 \end{pmatrix} \bmod = \begin{pmatrix} 1 \\ 20 \\ 25 \end{pmatrix}$$

1	20	25
B	U	Z

Scanned with CamScanner

Now the Ciphertext will be

Plaintext : N E D U E T
Cipher : V D J B U Z

↓

Modular Inverse Matrix

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 21 \\ 3 \\ 9 \end{pmatrix} = \begin{pmatrix} 273 \\ 654 \\ 549 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 4 \\ 3 \end{pmatrix}$$

N E D simultaneously & so on for UET.
13 4 3

Modular Theorem:

$$\overset{\text{int}}{a} \bmod \overset{\text{int}}{m}$$

R is remainder of $\frac{|a|}{m}$

Residue (r) which will three cases:

1) Remainder's value is the ans. {if $a \geq 0$}
2) Value of a is -ve and remainder is not 0.
   {m-R if $a<0$ and $R \neq 0$}
3) 0 if $a<0$ and $R=0$

Scanned with CamScanner

{ **Co-prime** : are those two numbers that dont have any common factors other than 1. In other words, they are not divisible by same numbers other than 1 }

$-80 \bmod 26$

$$R = \frac{|-80|}{26} = \frac{80}{26} = 2$$

$= m - R \Rightarrow \quad 26 - 2 = 24$

$-52 \bmod 26$

0

How to Calculate Modular Inverse of a Number?

Modular Inverse :

$a \cdot x \bmod m = 1$ Where 'x' is any number we can take in order to get 1

Coprime

$3(2) \bmod 5$

$6 \bmod 5 = 1$

$-80 \bmod 26$

these are not Coprime

it is possible

Scanned with CamScanner

Calculating the Modular Inverse matrix for Hill Cipher:

$$A \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(1) det (A)

(2) Mod. inverse of det (A) = x

(3) Adjugate of $A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

4) $(x \cdot Adj(A)) \bmod 26$

$$A = \begin{pmatrix} 3 & 2 \\ 5 & 1 \end{pmatrix}$$

1) det (A)

$A = 3 - 10$

$A = -7$

2) $-7 \cdot x \bmod 26$ $\qquad R = \frac{|a|}{m} = 7$

$-7(11) \bmod 26 = 25$

$26 - 25 = 1$

$= m - R$

Scanned with CamScanner

3) $\text{Adj } A = \begin{pmatrix} 1 & -2 \\ -5 & 3 \end{pmatrix}$

$\text{Adj } A = 3 - (-10)$

$\text{Adj } A = 13$

4) $\left\{ 11 \begin{pmatrix} 1 & -2 \\ -5 & 3 \end{pmatrix} \bmod 26 \right\}$

$\begin{pmatrix} 11 & -22 \\ -55 & 33 \end{pmatrix} \bmod 26$

This is decrypte matrix

Scanned with CamScanner

25/10/23

VIGENERE CIPHER

Key = SECRET

Plaintext = NED UNIVERSITY
SEC RETSECRETS

Add mod 26

Ciphertext

	N	E	D	U	N	I	V	E	R	S	I	T	Y
	S	E	C	R	E	T	S	E	C	R	E	T	S
	13	4	3	20	13	8	21	4	17	18	4	24
	+	+	+	+	+	+	+	+	+	+	+	+
	18	4	2	17	4	19	18	4	2	17	4	18
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	31	8	5	43	17	27	39	8	19	35	12	42
mod	5	8	5	11	17	1	13	8	19	9	12	

Scanned with CamScanner

AUTOKEY Cipher

Plaintext : [NED UNIVERSITY
SEC RETNEDUNIV

Add mod 26

Railfence Cipher

Ciphertext :

MEATRHCASETFETELS

M E A T R H C A S
E T F E T E L S

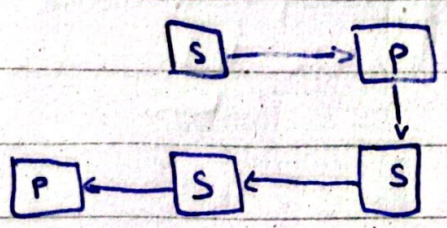
Scanned with CamScanner

30/10/23

Row Transposition :

CRYAAETTMTTPKESAAX

2	4	3	6	1	5
A	T	T	A	C	K
A	T	T	A	R	E
E	P	M	X	Y	Z



permutation P
substitution S

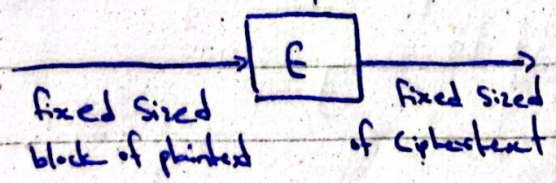
DES, AES

Binary Strings :

In the modern world there are types of binary schemes

1) Block Ciphers
2) Stream Ciphers

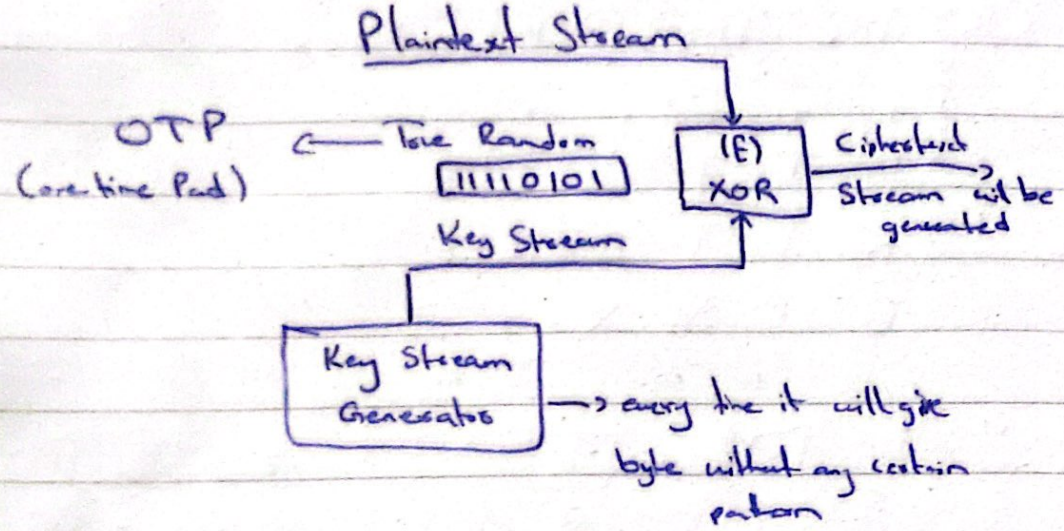
DES (64 bits)
AES (128 bits)



(depends on the nature of scheme)

Scanned with CamScanner

Stream Ciphers :




```
P  01010101
K  11110101
C  10100000   ---> receiver
```

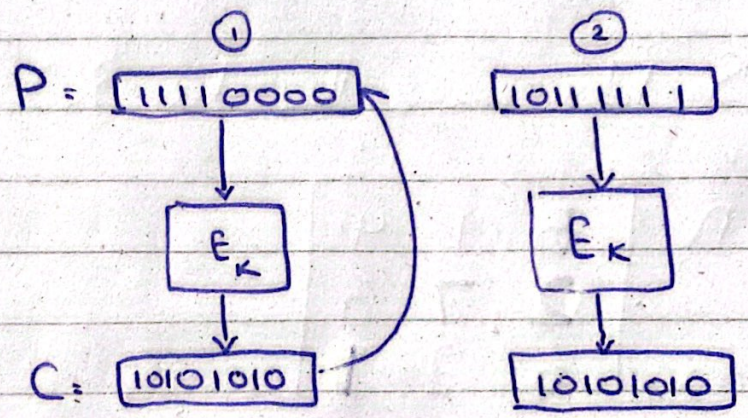
Shannon's Theorem :

According to Shannon's Theorem if the key is perfectly random and plaintext = key = ciphertext then it will have perfect Secrecy

Scanned with CamScanner

	B	C	D	
	1	2	3	
+	Z	B	Y	modulo 26
	25	1	24	
	0	3	1	

Block Cipher Scheme :



Irreversible Mapping then Scheme is useless

Design Block Cipher Scheme of two bits

Block Ciphe Scheme of two bits:

00	01	10	11
Not	Not	Not	Not
11	10	01	00

if all the inputs are defined then all the outputs will be also defined, this type of scheme is called Ideal Block Ciphers Scheme.

input	output
00	00
01	01
10	10
11	11

Scanned with CamScanner

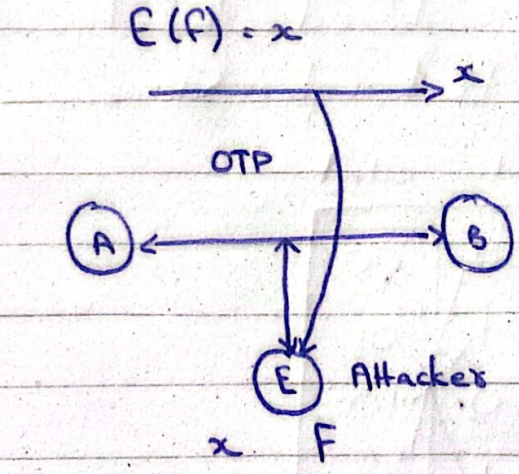
1/11/23

Q# Define Attack Model (imp paper)

Attack Model.

It is based upon some realistic assumptions, we demonstrate any vulnerability / attack.

Example :



F = file
E = Extension
x = Encrypted file

$K = F \oplus x$

plaintext Cipher

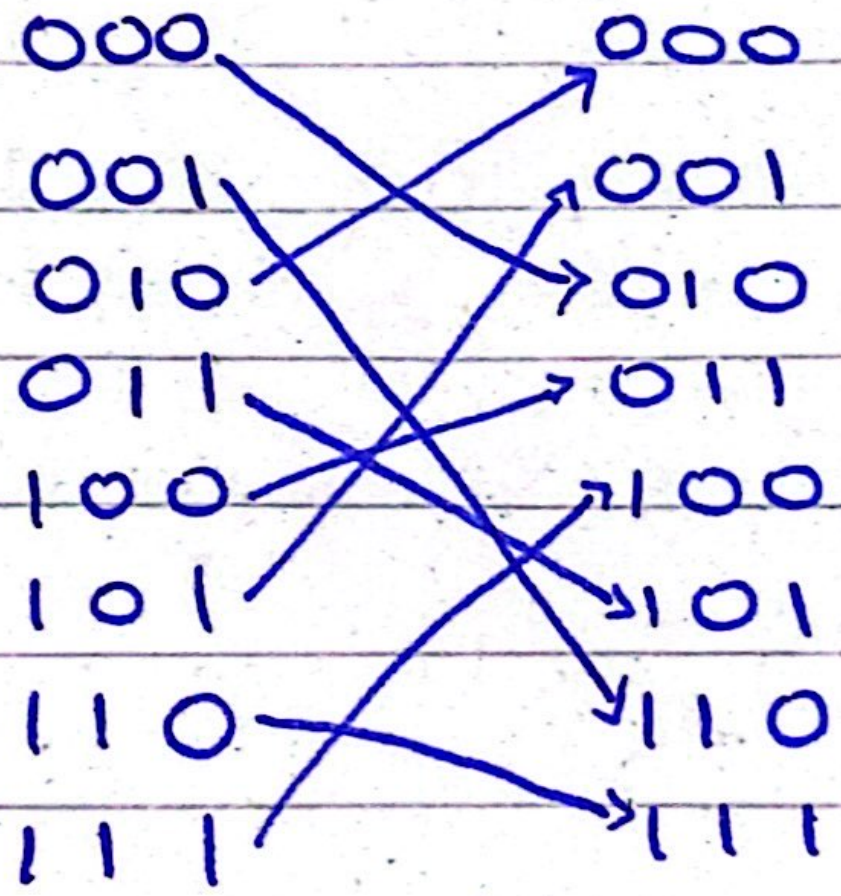
→ Now the attackers can decrypt key.

Assumptions :

1) Attack already have the copy of key
2) Key is reusing
3) OTP

Scanned with CamScanner

3-bits (Random) Ideal Block Ciphers



Scanned with CamScanner

P = 011 011 000 101 010

101 101 010 001 000

(A) ⟶ (B)

$2^3 = 8$

8×3 bits

	Key	Key
000	010	
001	110	
010	000	
011	101	
100	011	
101	001	
110	111	
111	100	

We have to transfer 24 bits key for (Block Size) 3 bits Ideal Ciphers.

For 4-bits

$2^4 = 16$

$16 \times 4 = 64$

General formula

$: 2^n \times n$

exams (imp)

Q*) We dont use ideal block ciphers because it is not

feasible to handle the large key size in practical system.

When bits are less, security is Compromised but when bits are more in size Security will be increased and it will be more secure because it does not any algorithm or method to crack as it works on Combinations.

SP-Network

S - P

Substitution → Confusion

Permutation → Diffusion

Confusion: Ciphertext ⟷ key Complex

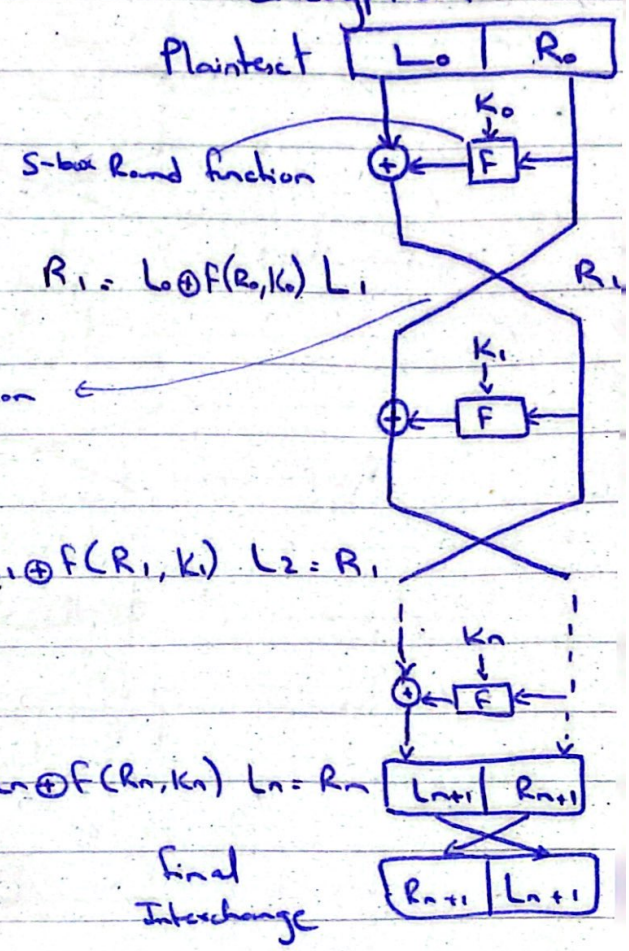
Diffusion: plaintext ⟷ ciphertext

Scanned with CamScanner

Feistel Ciphers (by Horst Feistel)

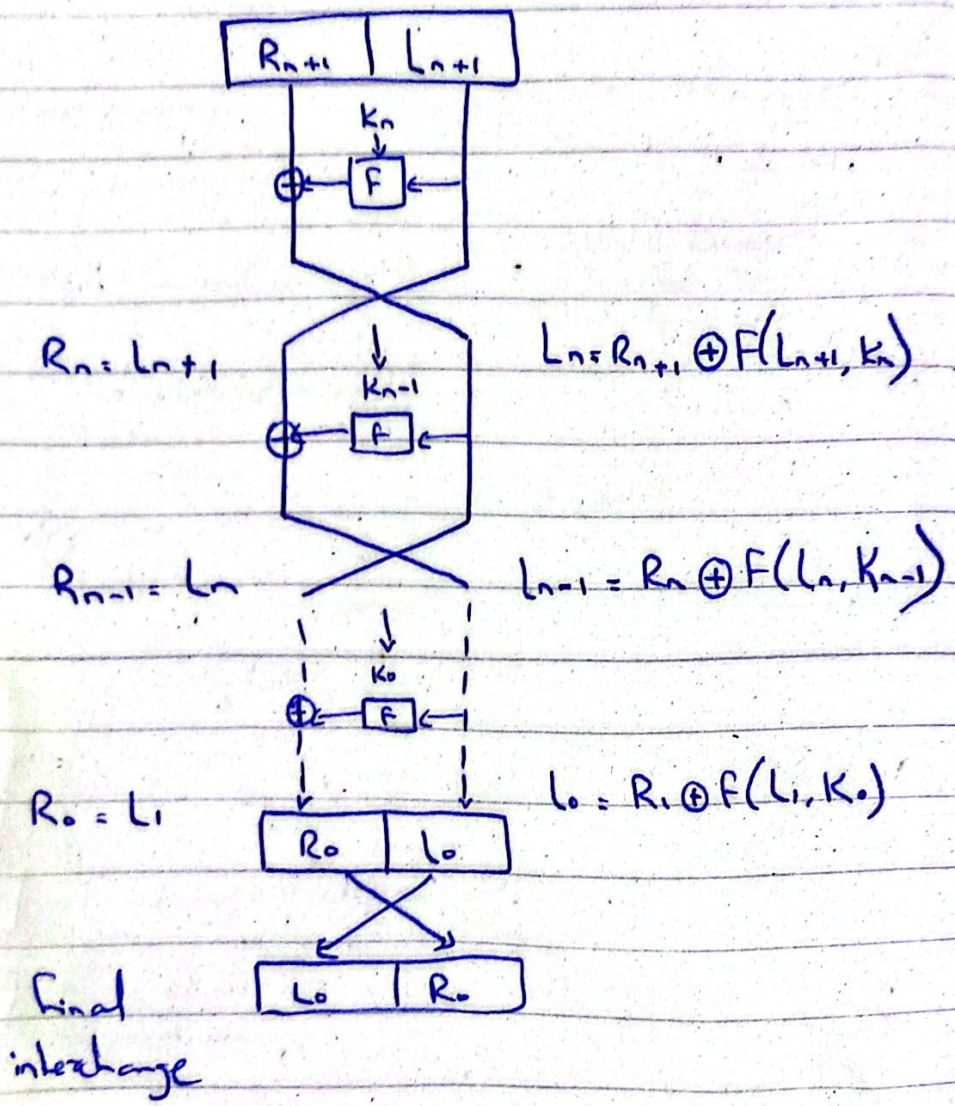
Symmetric Key
Block Ciphers
Product Ciphers

Encryption



Scanned with CamScanner

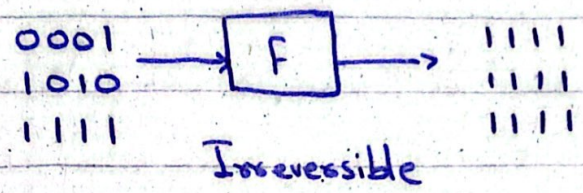
Decryption:



Scanned with CamScanner

Fiestel Cipher

" Round function f " is always invertible



Fix:

Block Size : 8-bits
No. of Rounds : 6
f is constant

DES (Data Encryption Standard)

→ 1976 → 1999
Standard by NBS
FIPS (Federal Info. Processing Standard)
Broken in 1999 (by distributed.net and EFF)
↳ decrypted in 22hrs 15min

DES Design based on Fiestel Ciphers:

Scanned with CamScanner

fix: for DES:

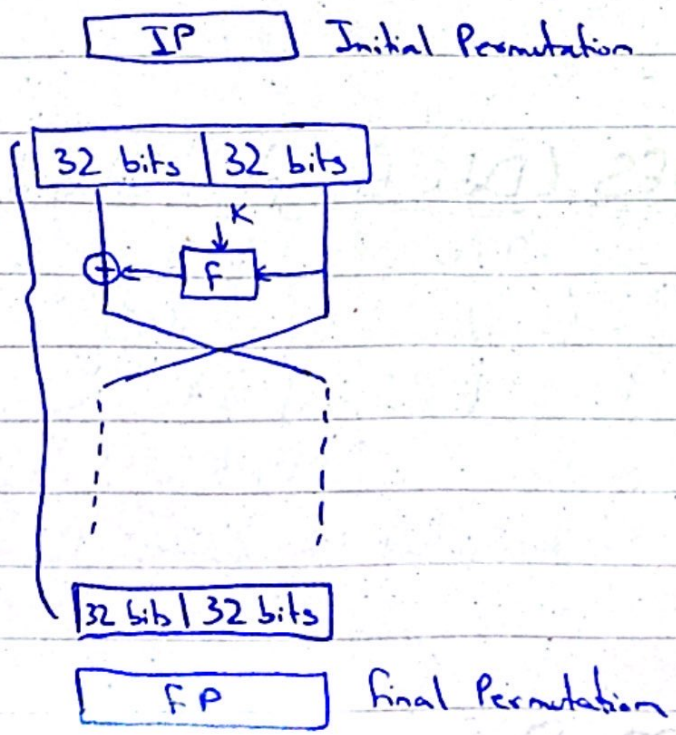
Block Size = 64 bits

No. of Rounds = 16

Key : 64 bits

Internal Structure of Round function F is specifically designed for DES.

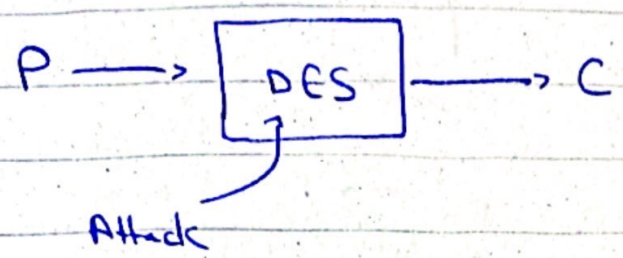
Key Generation Algorithm



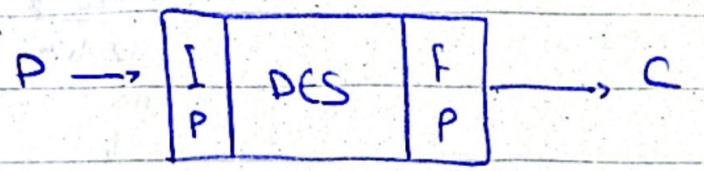
This IP and FP has no cryptographical significance, it is only added for the purpose of secure implementation

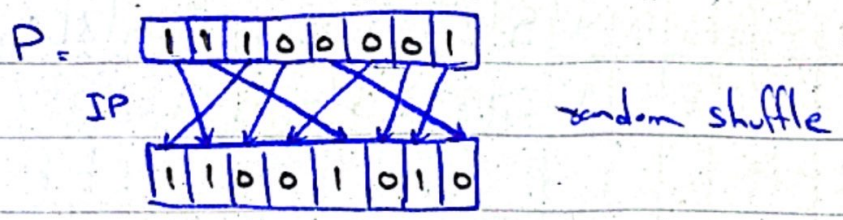
Scanned with CamScanner

We Implement DES Scheme in specialized hardware.

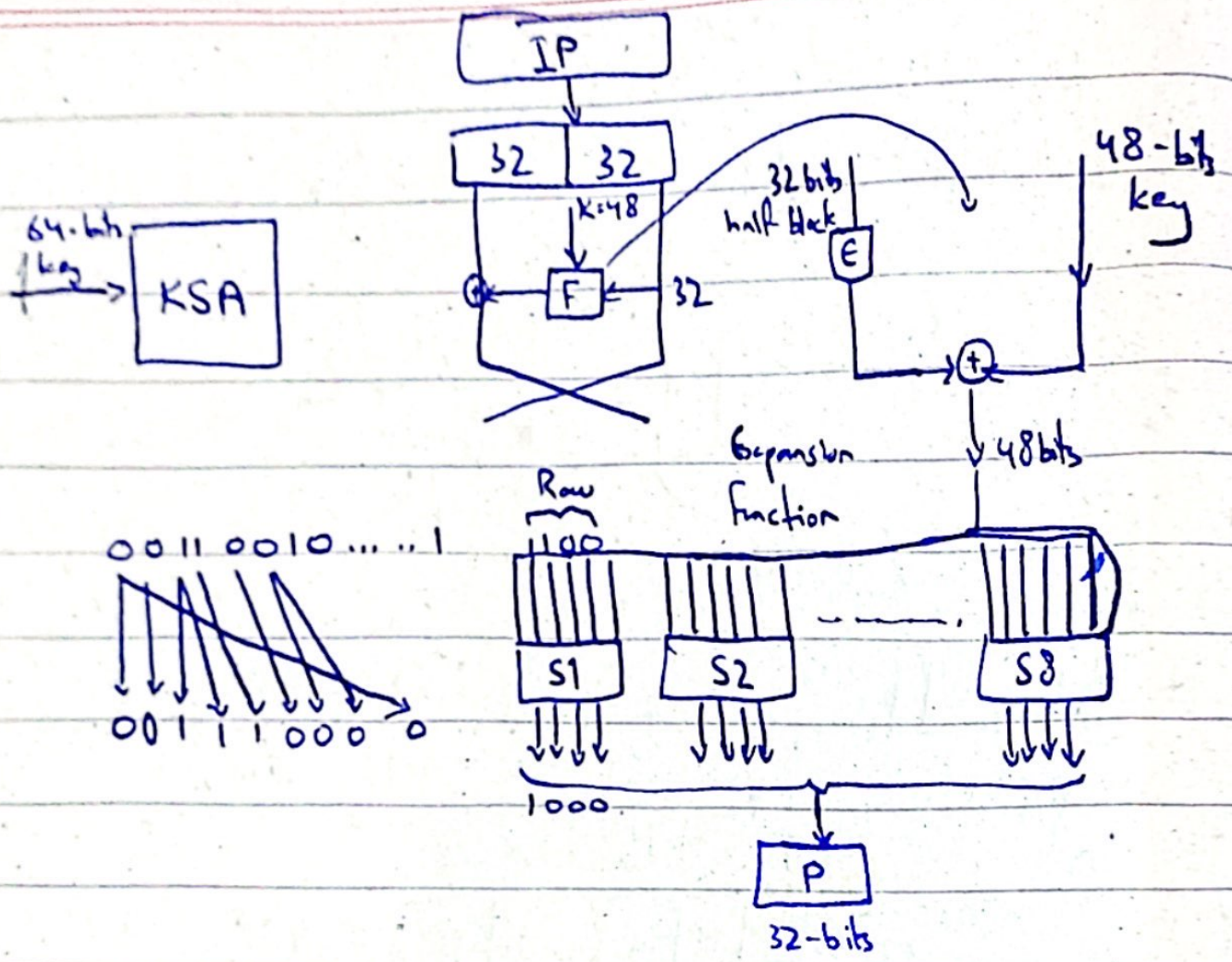


Before data is given to hardware we add Initial permutation in the hardware





Scanned with CamScanner

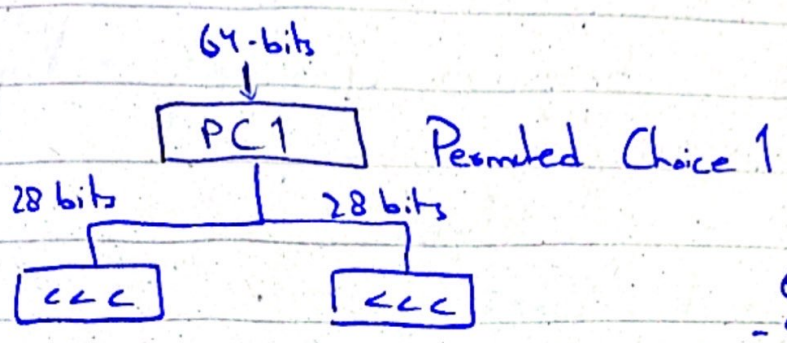


1100

Rows		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	0	F	E	3	D	4	5	D	C	1	B	2	9	A	8	7	E
01	1	F	0	E	D	1	C	2	B	3	A	4	9	8	5	7	E
10	2																
11	3																

Scanned with CamScanner

Key Schedulling :



$$\begin{array}{r} 64 \\ -56 \\ \hline 8 \end{array}$$

These 8 bits are left forever and donot contribute in the generation of keys.

Rotate left

11000

10001 ROL 1

00011 ROL 2

Scanned with CamScanner

15/11/2022

Avalanche Effect:

Minor change in (plaintext or key) results in a big change in Ciphertext.

In DES Scheme

Change 1 bit in plaintext ⟶ 34 bits Ciphertext

Change 1-bit in key ⟶ 35 bits Ciphertext.

DES is not secure now!

1) DES Challenge 1 by Rocke Verse (Uni of Colorado took 96 days to break.

2) DES Challenge 2 by RSA Labs (Deep Crack) took 56 days to break

$250,000 (investment in 1999)

Speed : 90 billion keys/sec

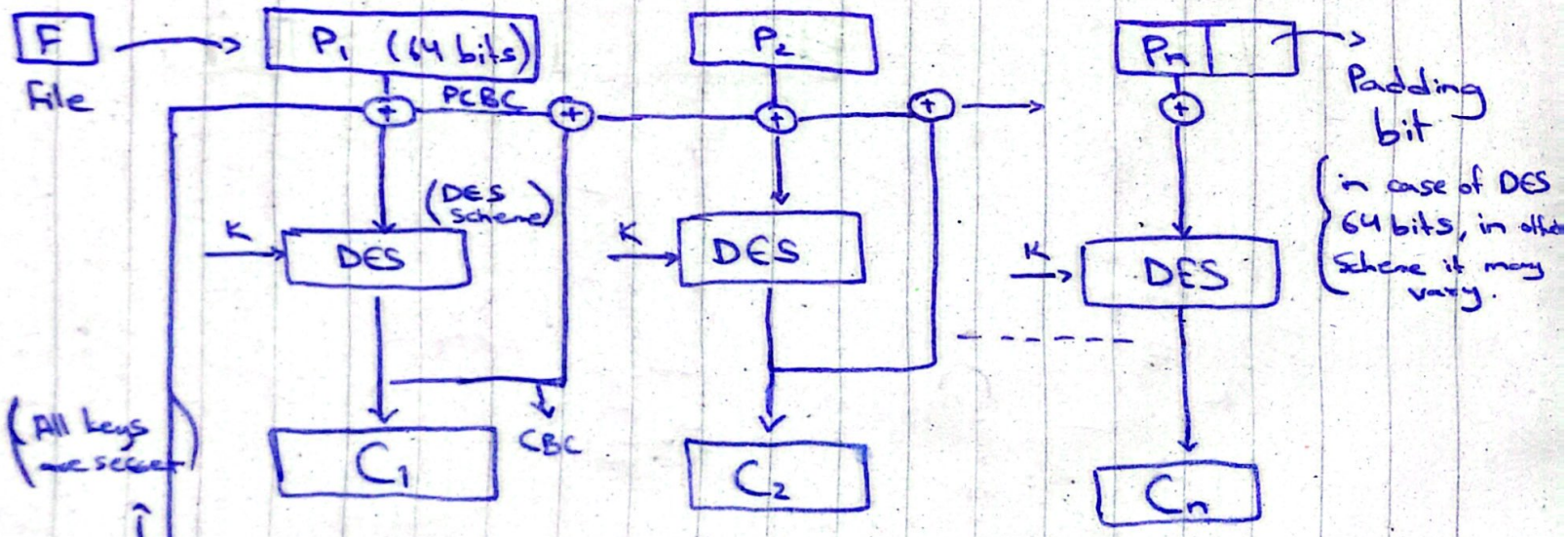
} Brute force attacks are applied on every DES Scheme

Assignment) Write a program which will apply Brute force on 2x2 Hill Ciphers.

Scanned with CamScanner

Modes of Operation for Block Ciphers :-

Sender:



1) This straightforward scheme is called ECB (Electronic Code Book).

Scanned with CamScanner

If $P_1 = P_3$

Then $C_1 = C_3$

If we give big amount of data, then it is not recommended to use ECB.

2) CBC (Ciphers Blockchain Chaining):

If $P_1 = P_3$

Then $C_1 \neq C_3$

The outcome will make XOR with plaintext, we need C_{n-1} in case of P_n.

2a) $C_0 = IV$

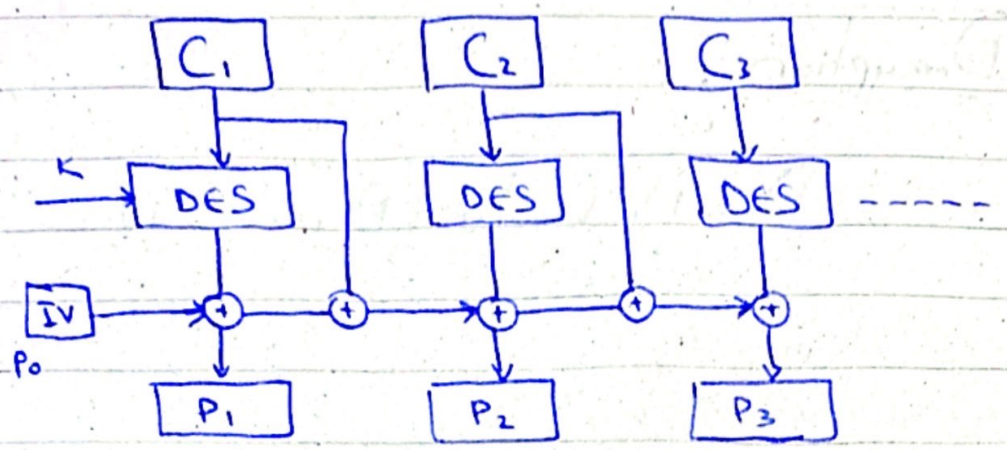
General Equation:

$$C_i = E_K(P_i \oplus C_{i-1})$$

"This scheme cannot be implemented parallely, we can do it sequentially instead."

Scanned with CamScanner

Receiver:



$$P_i = D_K((C_i) \oplus C_{i-1}$$

If there's any error found in IV, then it'll impact only on P_1 not on the whole process.

3) PCBC (Propagating Cipher Block Chaining)

Ciphertext $\oplus$ Plaintext

Block $\underbrace{\qquad\qquad\qquad}_{\oplus \text{ DES}}$ Block

then,

General Equation:

$$IV = P_0 \oplus C_0$$

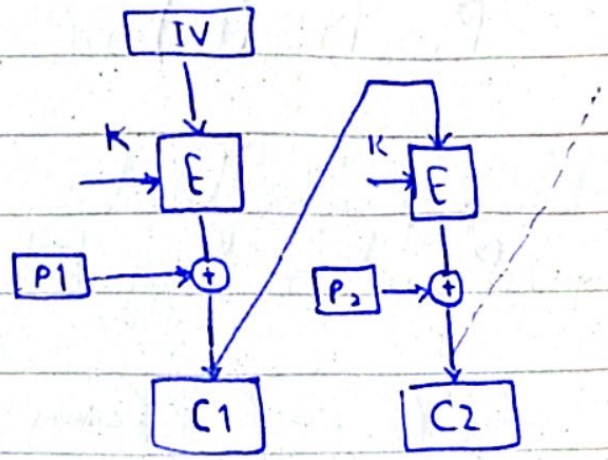
Scanned with CamScanner

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1})$$

<u>Decryption</u>:

$$P_i = D_K(C_i) \oplus (P_{i-1} \oplus C_{i-1})$$

4) CFB (Cipher feedback)

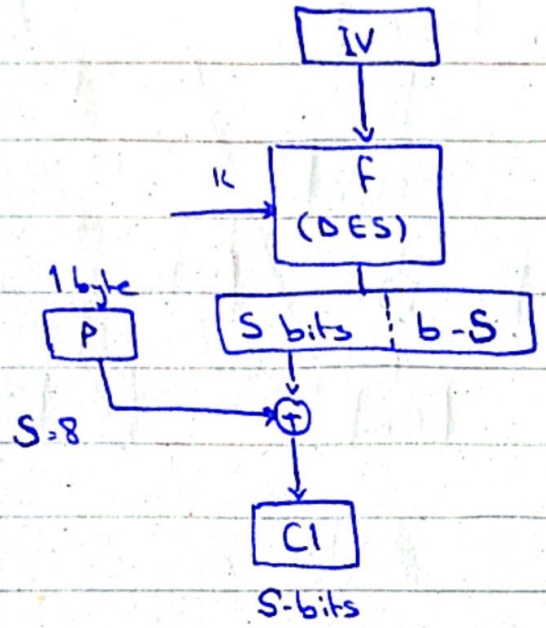


This mode of operation is suitable for stream based applications.

"If IV is 64 bits, we then put it in registers."

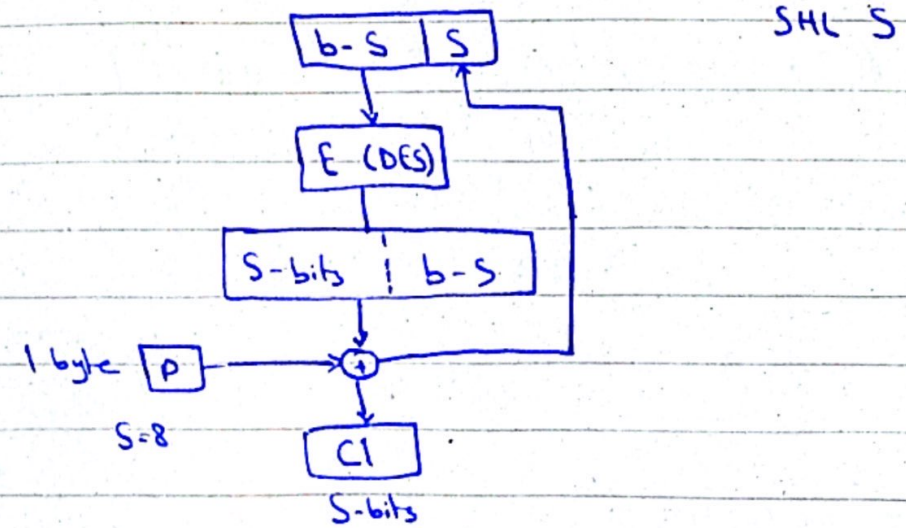
Scanned with CamScanner

Registers (64 bits)



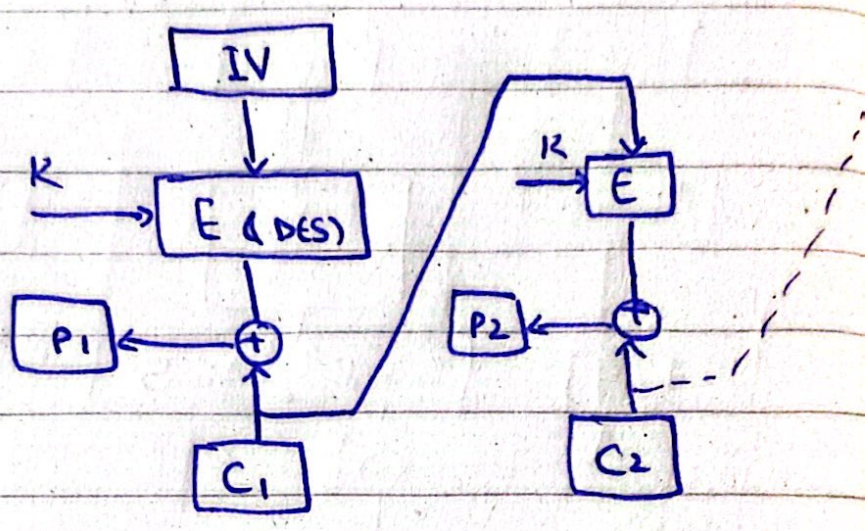
If we shift left this Register.

Register (64 bits)



Scanned with CamScanner

Decryption of CFB :



Scanned with CamScanner