Page No.
Date

Sec

* Substitution Cipher

1) Mono Alphabetic Substitution

→ known as simple substitution.
→ fixed replacement

~~types~~

2) Substitution cipher

→ caesar cipher ⇒ substitution of ~~letter~~ 3 places next

a → d. -- so on. mod 26.

→ Monoalphabetic = 26 keys

→ Play fair ⇒ fill key, remaining a to z, ~~not~~ repeated i/j

~~Play fair~~

K

P L A Y F

I R E X M*

B C D G H

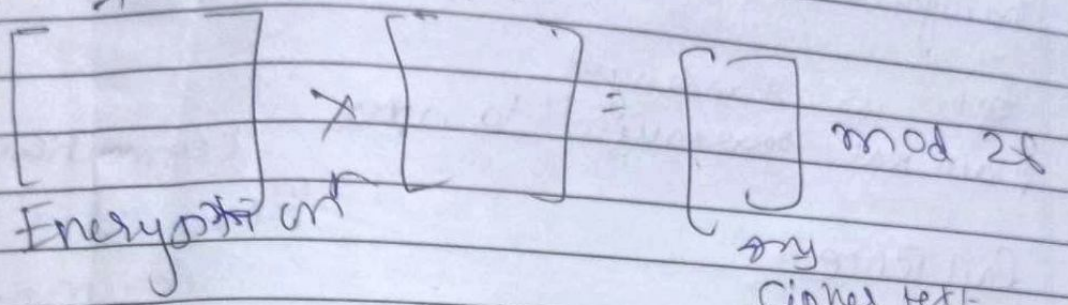
N O Q S

T U V W Z

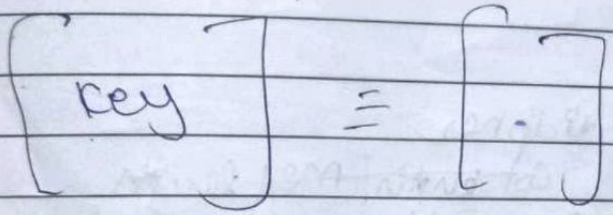
types

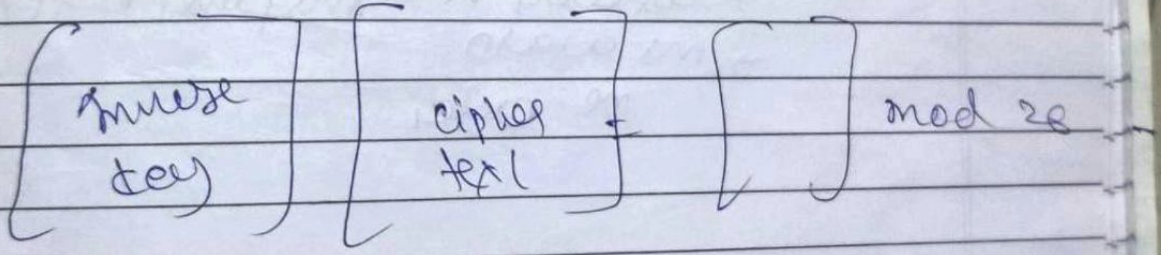
1) Rectangle 2) column ⇒ next key

→ Hill cipher



Decryption





→ Polyalphabic :⇒ one-to-many relationship

size size

vigenere ⇒ key ≠ text

(key + text) mod 26

vernand one ⇒ key size = text size.
time

* Transposition Cipher.

order is rearranged
plain text rearranged to cipher   keymentiond

Row trans

Rail Fence   Column.

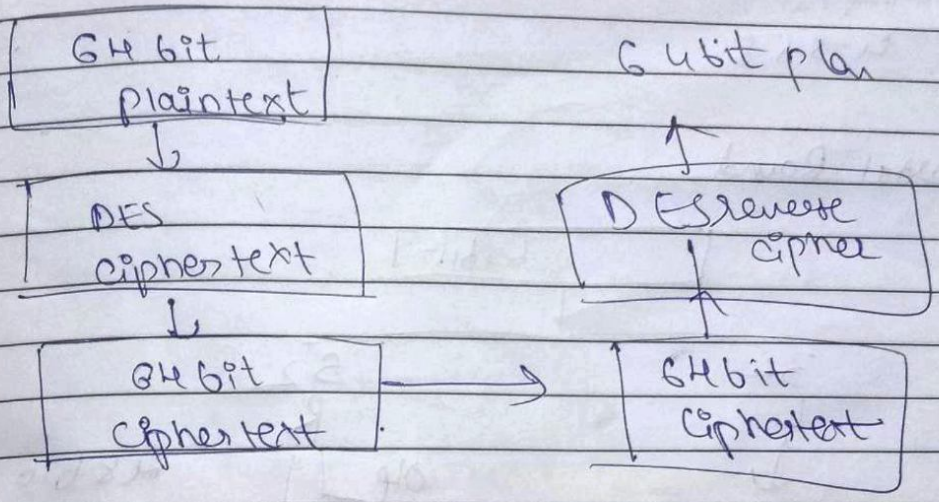
Column ⇒ decipher
~~Col length~~ ~~/ msg length~~
→ Col length = msg len / key len.
→ ms again
re-order

886

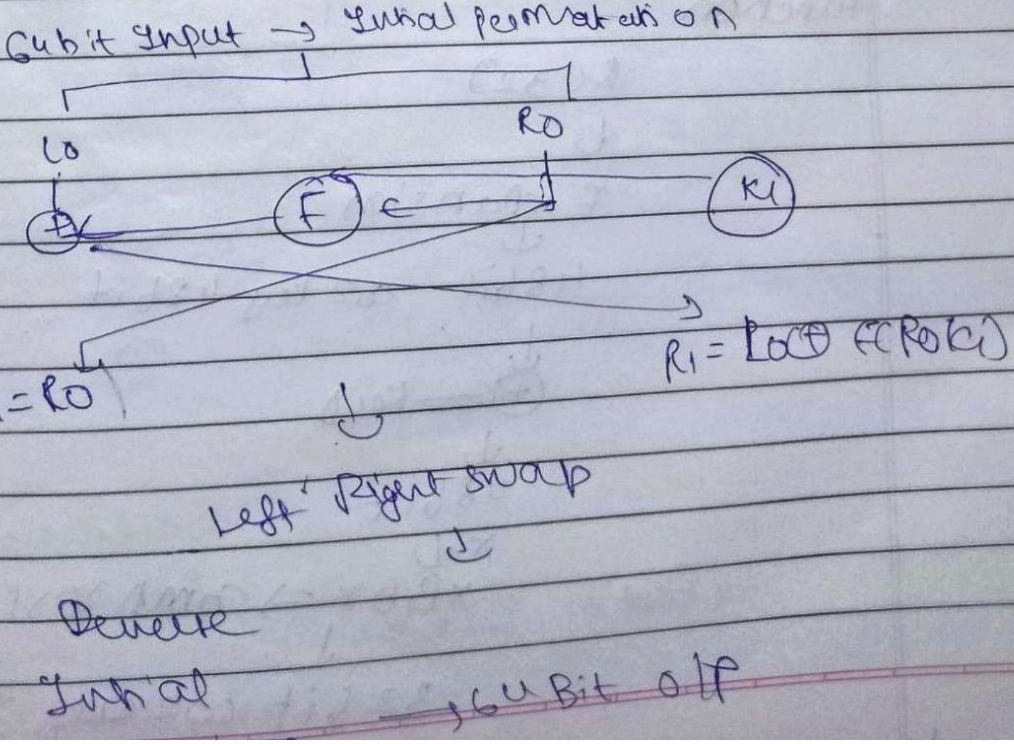
Page No.
Date

A Explain working DES

Data Encryption std



1) Initial Permutation
2) 16 Identical Rounds
3) Left Right swap.
4) final permutation



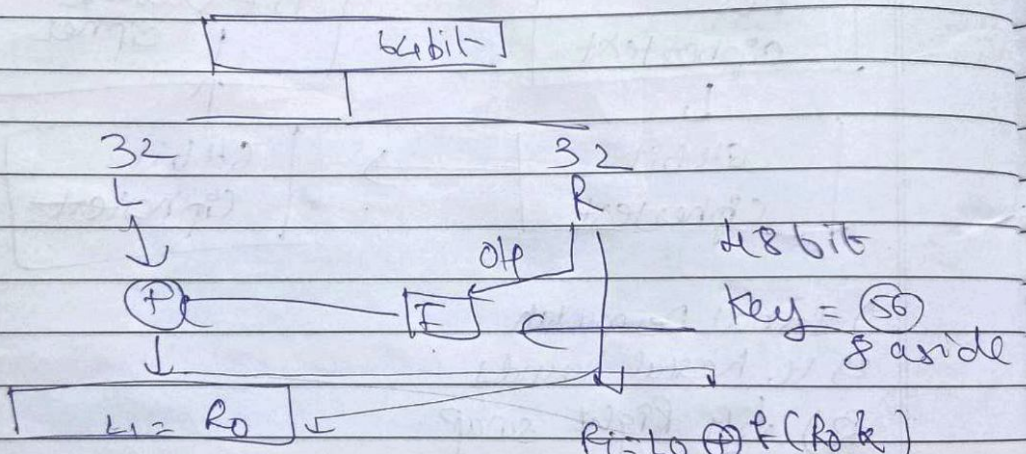
Initial Permutation

64bit => 64 op

1 → 2

4 → 58

Total Round



F function

R(32)

↓

Expansion

↓

48bit co2 key 48bit

↓

⊕ ← key

↓

48bit

↓

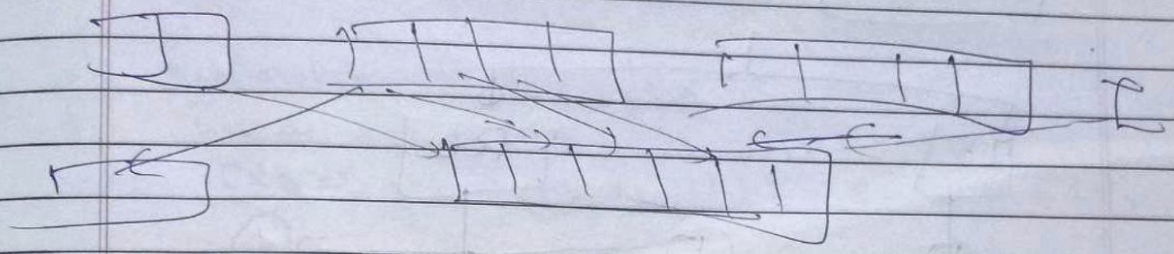
xBox => compress

↓

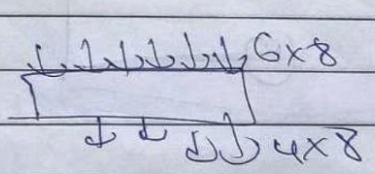
32 bit co2 of 32

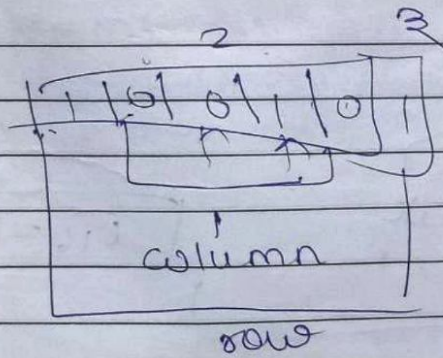
Page No.
Date

Expansion

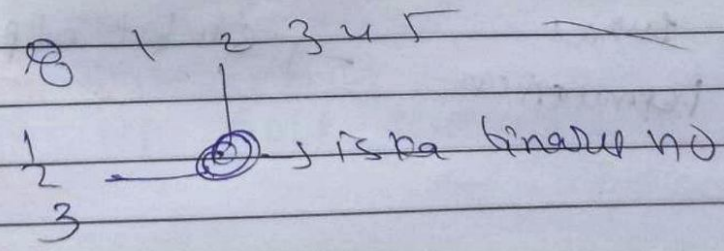


* S-box substitution





11 = 2+1 = 3

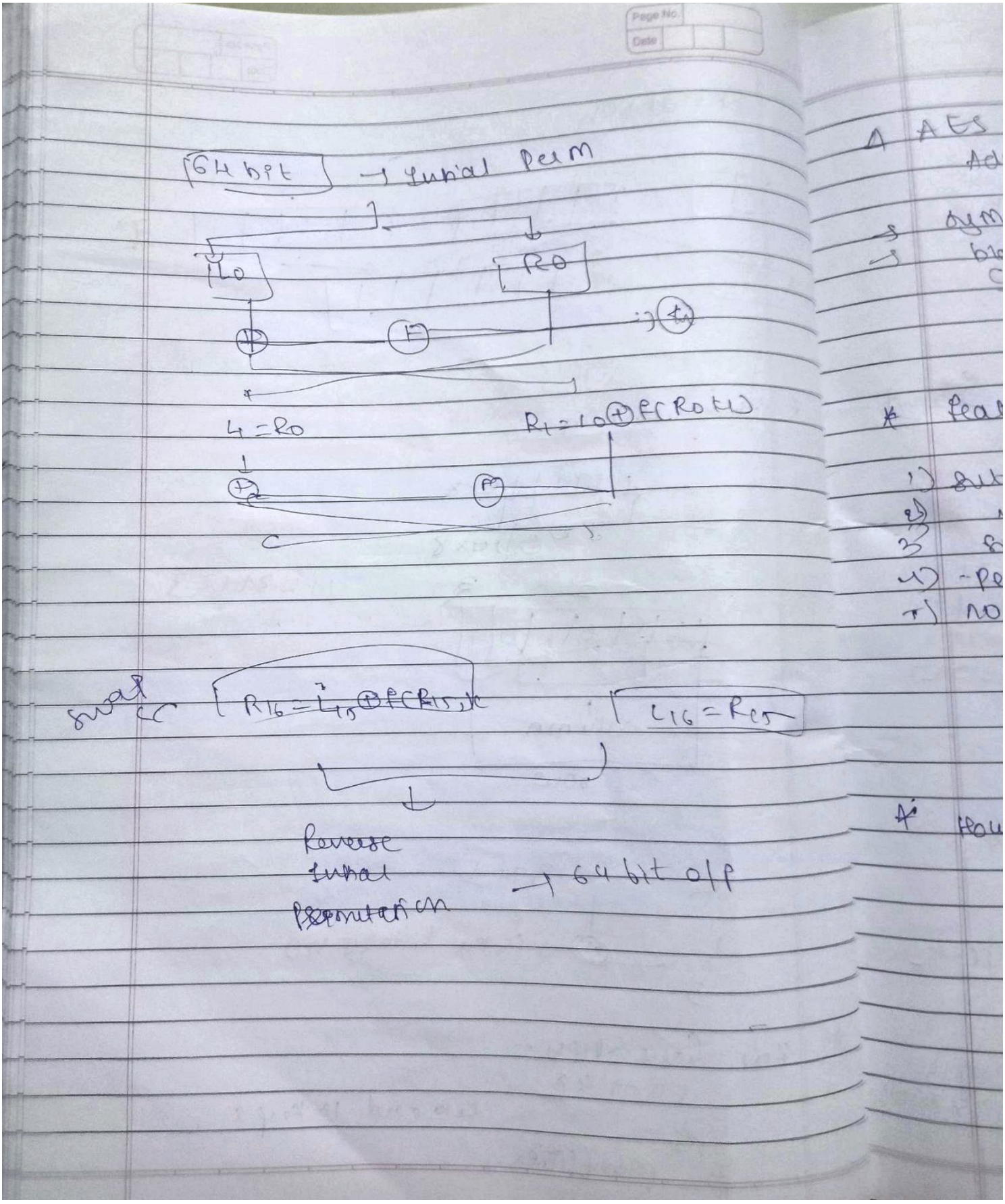


* Key Generation.

56 → 48

2^{56} possibilities

we need 16 keys.


64 bit
Initial Perm
L0
R0
f
K1
L1 = R0
R1 = L0 ⊕ f(R0, K1)
swap
L16 = R15
Reverse
Initial
Permutation
64 bit o/p

1 AES

Advanced Encryption Standard

→ Symmetric block cipher

→ block size ⇒ 128 bits. Converts plaintext to ciphertext using 128, 192 & 256 bits.

Des → Triple → AES
Des

* Features of AES

1) Substitution & Permutation ie SP network
2) multiple rounds
3) Any key ⇒ used multiple rounds.
4) Performs on byte data
5) No of rounds → key size

128 bit ⇒ 10 rounds,

192 ⇒ 12

256 → 14

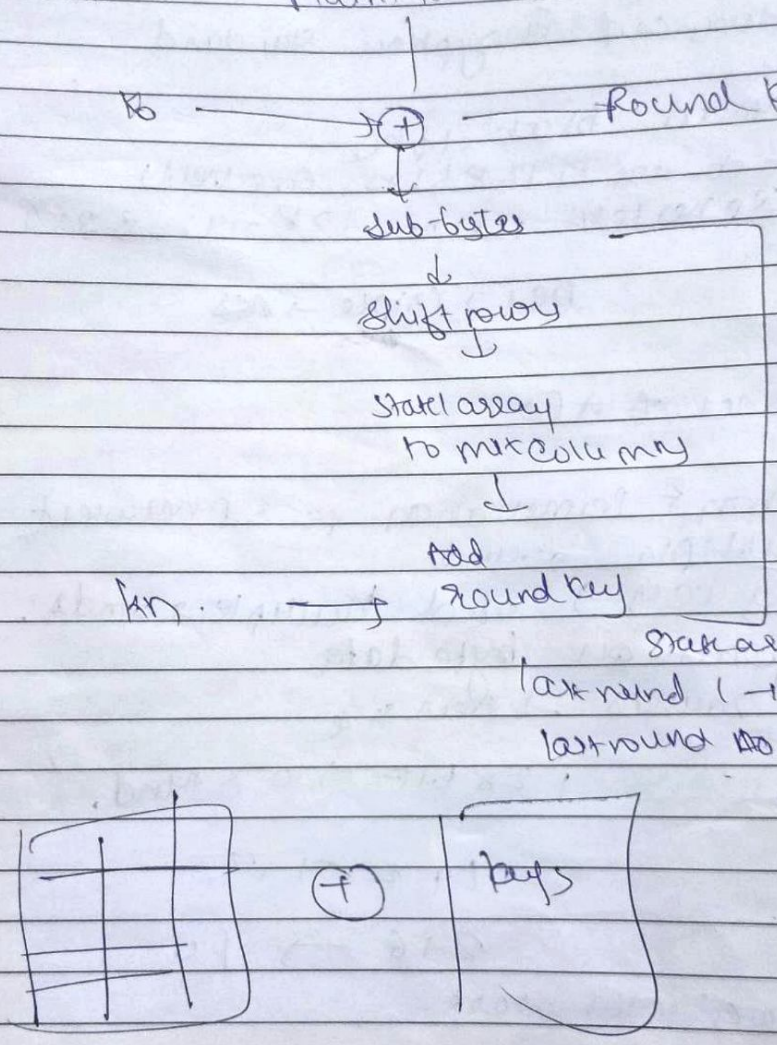
6) How does AES work.

4x4 matrix

State array

i/p & o/p state array

(n+1) keys



* Byte substitutions.

Innal state array → | sbox | → final state

each byte ⇒ hexadecimal
first part row
then column

key length
Block size

simple
Rijndael

Shift rows

1 2 3 4 → 1 2 3 4
5 6 7 8 → 6 7 8 5
9 10 11 12 → 11 12 9 10
13 14 15 16 → 16 13 14 15

Mix columns

1 2 3 4 C0 = NC0
5 6 7 8 C1 NC1
9 10 11 12 C2
13 14 15 16 C3

Add round key
16 byte → 128 bit ⊕

Applications

1) Wireless security ⇒ Auth router & clients
2) General file encryption
3) Prevent hijacking

	AES	DES
Key length	256	128 / 192 / 256
Block size	64 bits	128 bits
	16 rounds	10 / 12 / 14 (depends key length)
	simpler	faster