09.01.2018

CRYPTOGRAPHY

Art of & science making coded message - ciphertext (c)

Encryption (m, key) = Sender → o/p
Decryption (c, key) — Receiver
} Share common key

o/p = m

Sent through insecured channel - interception may occur

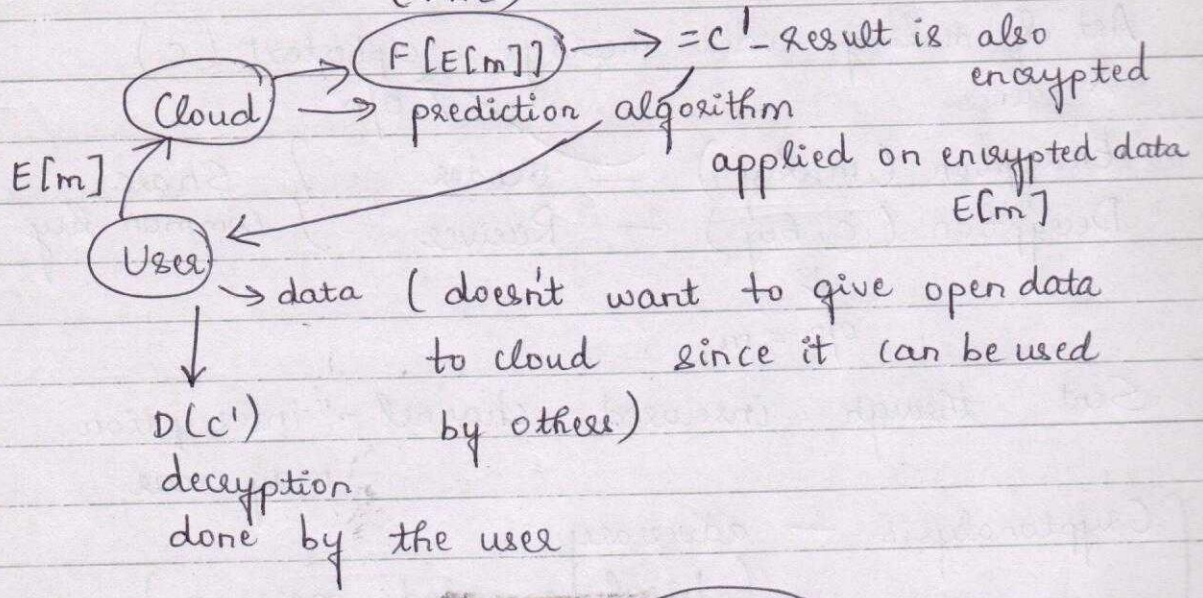
- Cryptanalysis — adversary (breaking coded message)
- Cryptography — creating coded message
- → both together - **CRYPTOLOGY**

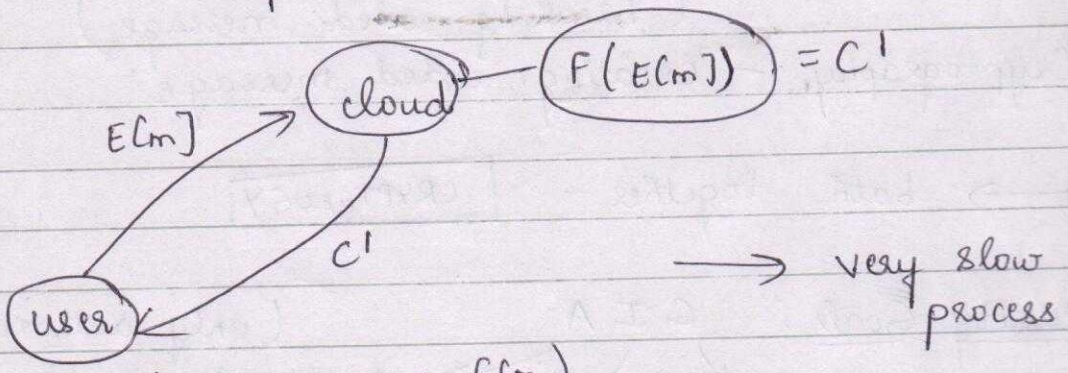
Security Goals: C I A

- Confidentiality — message not changed, if changed should be known to the receiver
- Integrity
- Availability — (only authorized users)

MOTIVATION :

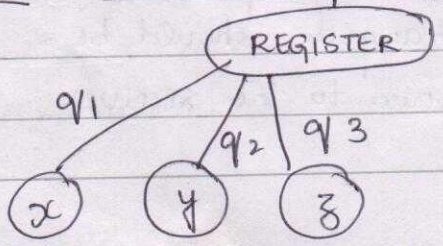
(1) Full Homomorphic Enc : (2009) Gentry (FHE)





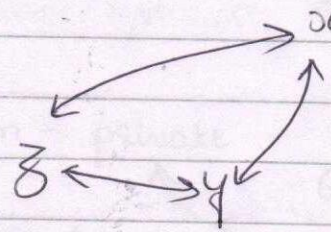
→ very slow process

(2) Secure Multi-Party Computation :



→ $f(q_1, q_2, q_3) = \min_i q$

x, y, z provides tender for mess to register.
But quotation of x is not known to y and z.
(Secret) — private
But all 3 quotations are known only to register & selects minimum.



communicates with each other without revealing their private key

(3) Bitcoin: (Decentralized cryptocurrencies)

Online transaction - transfer money using username & password

Most recent one

Classical Cryptography:

For communication — share common key

OR

Symmetric Cryptography / Private cryptography

Prerequisite: Share common key

First cryptography was given by Caesar

$K = 3$

Message contains only alphabets $m \in$ Alphabet

Encryption $E[m] = m + 3 \quad (K) \quad \underline{\underline{(m+K)}}$

Message : CRYPTO

Ciphertext : FUZSWR

Decryption $D(c) = C - 3$

Scheme :

$E[m] = m+K \mod 26$

$D[c] = C-K \mod 26$

Proof of Correctness –

$D(\underbrace{E(m)}_{\text{ciphertext}}) = m \leftarrow$ original message

$D(\overset{C}{\underbrace{m+K}}) = m$

$(m+K-K) = m$

Cryptanalysis:

Worst attack - Brute force method / trial - $O(26)$
complexity of attack

Kirchoff's Law: Algorithm – public ✓

try to find faults

Good ≥ 80
Bad < 20

Algorithm - private

try to find out

Good ≥ 80 (don't interfere)
Bad < 20

11.01.2018

Affine cipher:

$m \in Z_{26}$ {0 to 25}

$E[m] = am + b$ keys are a & $b \in Z_{26}$

$D[c] = a^{-1}(c - b)$

↓

should exist - choose key in such a way

$2^{-1} \bmod 4 = 1$ → doesn't exist

(may not exist for all nos)

a^{-1} exists if $\gcd(a, 26) = 1$

↓ elements which are relatively prime to 26

Cryptanalysis:

Given C → find m or key

Euler quotient = $\phi(m)$

No of integers less than 'm' and relatively prime to m

By trial, Complexity = $26 \times \phi(26)$

$= 26 \times 12 = 312$

Theorem:

$$m = \prod_{i=1}^{n} p_i^{e_i}$$

p_i are different primes and $e_i > 0$

Any no can be written as a multiple of primes

$$m = 26 = 2^1 \times 13^1$$

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{(e_i - 1)} \right)$$

$$\phi(26) = (2^1 - 2^0) \times (13^1 - 13^0)$$

$$= (2-1) \times (13-1) = 1 \times 12 = 12$$

Hill Cipher :

Key is a matrix should be invertible (non-singular)

$$K = \begin{bmatrix} K_{1,1} & \cdots & K_{m,1} \\ \vdots & & \\ K_{m,1} & \cdots & K_{m,m} \end{bmatrix}$$

Message

$$m = (m_1, m_2, \ldots m_m)$$

$m \times m$ elements instead of one element

$$E(m) = (m_1, m_2, \ldots m_m)K$$

$$D(c) = cK^{-1}$$

Cryptanalysis :

$K = (3 \times 3)$ $\quad O(26^9)$ → worst case

↓ 9 elements

Attacks : (depends on the adversary)

1. Ciphertext
2. Known-plaintext $\begin{pmatrix} m_1 \to c_1 \\ m_2 \to c_2 \end{pmatrix}$
3. Chosen-plaintext

   $m_1 \to c_1$ (m_1 will be choice of adversary)

   This is theoretical not feasible
4. Known-ciphertext $\begin{pmatrix} c_1 \to m_1 \\ c_2 \to m_2 \end{pmatrix}$

2 & 4 – same ability

5. Chosen-ciphertext $c_1 \rightarrow m_1$

↓ adversary chooses this

③ & ⑤ are different

Hill cipher is vulnerable under known-plaintext attack.

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \rightarrow \text{Key}$$

① $[a_1, a_2]\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = [c_1, c_2]$

a_1, a_2: known; $K_1 \ldots K_4$: don't know; c_1, c_2: known

② $[b_1, b_2]\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = [d_1, d_2]$

↓ Combine ① & ②

$$\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = \begin{bmatrix} c_1 & c_2 \\ d_1 & d_2 \end{bmatrix}$$

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}^{-1}\begin{bmatrix} c_1 & c_2 \\ d_1 & d_2 \end{bmatrix}$$

Mono-Alphabetic Substitution Cipher:

Permutation cipher — $26!$

key is one among these

Key = 26 characters (should remember all)

Cryptanalysis:

Worst case $= O(26!) = O(2^{80})$

↓ very large

Frequency analysis:

Single letter — 'E' highest frequency

Double — " — — th, he, - - -

Triple — " — — the, and, - - -

How to defeat frequency analysis?

The above are all one-to-one mappings. Hence, use one-to-many mapping.

Many-to-one mapping is not possible - creates ambiguity during decryption.

Polyalphabetic ciphers:

↳ Randomized

Mono-alphabetic - deterministic

Vigenere Cipher (16th Century, Rome)

Key = C R Y P T O

Divide message & apply same key repeatedly

Add message & key mod 26

Cryptanalysis:

Kasisky' test:

16.01.2018

Pseudorandom Generator:

Coin toss - unbiased - purely random nos generation - not practical since it takes too much time.

↳ not pure random numbers - they get repeated after sometime.

$$G: \{0,1\}^K \longrightarrow \{0,1\}^n$$

where $n >>> K$

↓

seed - purely random

Probabilistic Polynomial Time (PPT) algorithm

Adversary is an algorithm & has limited time.

- not able to differentiate b/w random nos & G

G is successful if it's o/p can't be distinguished from the purely random no by an efficient PPT algorithm

$$\delta_n^A = \left| P_n[A(G(x)) = 1] - P_n[A[y] = 1] \right|$$

(1 if it is random, else 0)

($P_n[A[y] = 1]$: pure random no)

< negligible - adversary cannot differentiate b/w G & pure random nos

(A: adversary)

$$\boxed{\delta_n^A < \text{negligible}} = 1/2^{80}$$

$2^n > n^{100}$ after $n \geq n_0$

$< \frac{1}{2n} \approx \frac{1}{2^{80}}$

Next bit unpredictability :

Knowing 'n' bits – predict (n+1) th bit with a probability 1/2+ negligible

Adversary is given first i bits of the output of G (pseudorandom generator), it has to predict (i+1) th bit

$$\beta_n^A = P_n\left[A\left(G(x)_{1,2,\ldots,i}\right) = G(x)_{i+1}\right] - \frac{1}{2}$$

$$< \text{negligible}$$

Definition : G is pseudorandom no if and only if it is next-bit unpredictability.

Linear Congential :

$$X_{n+1} = aX_n + C \bmod m$$

$$aC < m$$

$$X_0 = \text{seed}$$

If $a = C = 1$, we will get the o/p in alphabetical order 1, 2, 3 - - - - -

(1) $a = 7, C = 0, m = 32$ $\{7, 17, 23, 1, 7 - - -\}$ Period is 4

Choose a & c in such a way that 0 to m-1 values are used (mod m) or atleast close to 'm'
Not suitable for long sequences.

Ex: Adversary knows 300 bits
$a, c, x_0 \simeq 100$ bits

$\begin{cases} S_1 - 100 \text{ bits} \\ S_2 - 100 \text{ bits} \\ S_3 - 100 \text{ bits} \end{cases}$

$S_2 = aS_1 + c$
$S_3 = aS_2 + c$

$S_2 - S_3 = a(S_1 - S_2)$

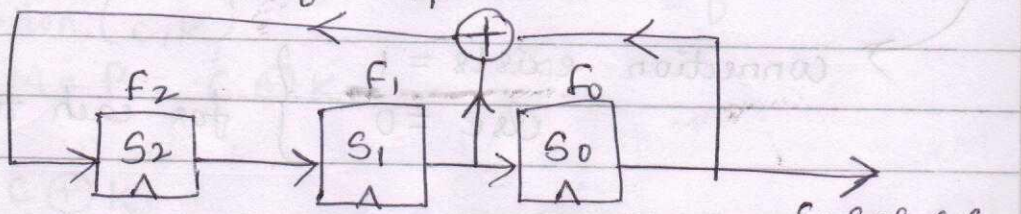
$a = (S_2 - S_3)(S_1 - S_2)^{-1}$

$a = \frac{S_2 - S_3}{S_1 - S_2}$

$c = S_2 - aS_1$

↓
Not suitable for security - good for programming

Linear Feedback Shift Register: (LFSR)

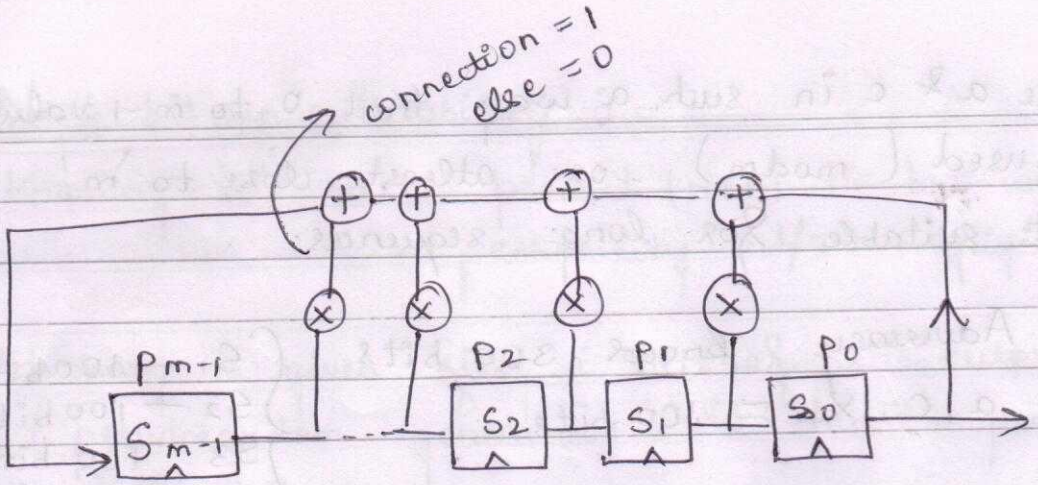


$S_{i+3} = S_i + S_{i+1} \mod 2$

Seed = $S_0 S_1 S_2$ = $S_2 S_1 S_0$
1 0 0

$S_3 = 0$
$S_4 = 1$
$S_5 = 1$

$S_0 S_1 S_2 S_3 S_4 S_5 S_6$ $2^3 - 1$
0 0 1 0 1 1 1 0 → S_7



Feedback co-efficient vector

$(p_{m-1}, p_{m-2} \cdots p_2, p_1, p_0)$

$p(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$

$p(m) = p_{m-1} \oplus p_{m2} \oplus \cdots \oplus p_0$ ✗

Periodicity : $\underline{2^m - 1}$ — choose the circuit in such a way

connection exists = 1
else = 0
} for each term

$\boxed{x^3 + x' + p_0} = \underline{x^3 + x + 1}$
polynomial

$x^2 = 0$ — no connection

irreducible / primitive

$x^3 + x^2 + x + 1$
$x^2(x+1) + 1(x+1)$
$(x^2+1)(x+1)$
} not good

(sequence)

One can get max. periodicity if corresponding polynomial is irreducible. (cannot be factorized)

18.01.2018

Symmetric Cryptosystem:

Requirement: Share common key

1. Stream Ciphers - encrypt one bit/byte at a time
2. Block Ciphers - encrypt block of 64-bits

Stream Ciphers:

1. Key generation - different for different stream ciphers
2. Encryption (M, K)

$$C = M \oplus K$$

↳ XOR-operation is fixed

3. Decryption (C, K)

$$M = P = C \oplus K$$

$$\begin{aligned} M &= C \oplus K \\ &= M \oplus K \oplus K \\ &= M \oplus 0 \\ &= M \end{aligned}$$

One-Time Pad (OTP) : Oldest type

E: $C = M \oplus K$

D: $M = C \oplus K$

$|K| = |M|$ Size of key = Size of plaintext (very long)

$M_1 \oplus K = C_1$ ----①

$M_2 \oplus K = C_2$ -----② Same key is used

$\Downarrow$ ① + ②

$M_1 \oplus M_2 = C_1 \oplus C_2$

adversary knows this

Hence he knows $M_1 \oplus M_2$

It is proved that, we can get M_1 & M_2 from this

M_1 ---- the ----

M_2 ---- [blank] ----

XOR = the

Security & Analysis - shows it is good
But not practical. (Ciphertext only attack is not possible)

k = 64 bits shared

$K = G(k)$
↳ pseudorandom generatore

$E(M, k)$ $C = M \oplus G(k)$

$D(C, k)$ $M = C \oplus G(k)$

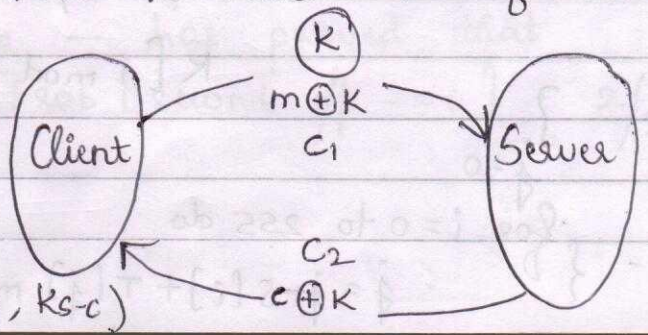
RC4 10^{100} → previously used

$G(k, \text{nonce})$ → modern stream cipher
↳ no used only once initialization value

by changing nonce $G()$ will change - k is constant
nonce is made public

C MS-PPTP (Windows NT)

MS - Point-to-Point Tranefer Protocol



Same key is used twice for encryption & decryption

$C_1 = m \oplus K$

$C_2 = c \oplus K$

$m \oplus c = C_1 \oplus C_2$

To overcome this use $K = (K_{c-s}, K_{s-c})$ — purely one-time

RC-4 : 1987 Ron-Rivest 10^{100}

Array $S[256]$: $S[0], S[1] - - - - S[255]$

1 byte — — — — — 1 byte

256 bytes

Array $K[keylength]$: $K[0], K[1] - - - -$

8

K = 64 bits = 8 bytes

1 byte

① Initialization

```
for i=0 to 255 do
{   S[i] = i;
    T[i] = K[i] %% keylength
           K[i mod keylength];
}.
j=0
for i=0 to 255 do
{   j = j+S[i]+T[j] mod 256;
```

```
    swap (S[i], S[j])
}
```

(2) Output - Key Stream

Stream Generation G(K) - pseudorandom no generator

```
i, j = 0
while (true)
{
    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]
}
```

Probability that any o/p is i = $1/256$

$$P[\text{any o/p} == i] = 1/256 + \epsilon\left(1/2^{80}\right)$$

↓ negligible

↓ Security requirement

Shamir — has proved that

Prob [second o/p == 0] = $2/256$

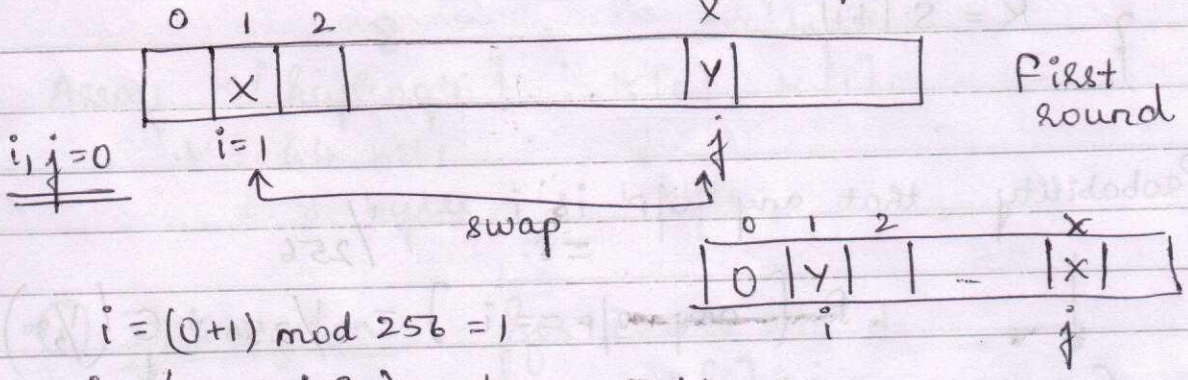
Shamir Theorem : (N = 256)

Assume that the initial permutation (initialization) is randomly chosen from the set of possible permutations of $\{0, \ldots, N-1\}$

Then, the probability that the second output byte/word of RC-4 is 0 is approximately $\frac{2}{256}$

$$Pr[\text{Second output} == 0] \approx \frac{2}{256}$$

Assume $S[2] = 0 \rightarrow$ probability $= 1/256$



$i = (0+1) \bmod 256 = 1$

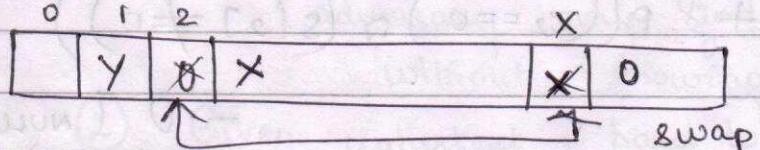
$j = (0 + \underset{X}{S[1]}) \bmod 256 = X$

swap $(S[i], S[j])$

$t = (\underset{X}{S[i]} + \underset{Y}{S[j]}) \bmod 256$

$k = S[t] = S[X+Y]$ – first byte of key

Second round $i = 2$



$i = 1$, $j = X$

$i = (1+1) \bmod 256 = 2$ → $i = 2$

$j = (X + S[i]) \bmod 256 = X$ → $j = X$

$S[2] = 0$

swap $(S[i], S[j])$

$t = (S[i] + S[j]) \bmod 256$

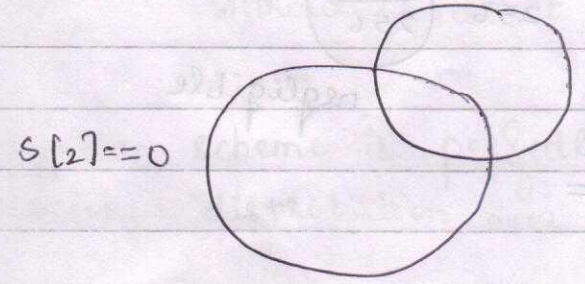
$S[2] + S[X] = 0 + X$

0

$k = S[X] = 0$ — second byte of the key

If $S[2] = 0$, second o/p $= 0$

$$Pr\left[\underbrace{\text{second o/p} == 0}_{Z_2} \,\middle|\, \underbrace{S[2] == 0}_{\text{given}}\right] = 1$$



$Z_2 == 0 =$

$(Z_2 == 0) \cap (S[2] == 0)$

$\cup (Z_2 == 0) \cap (S[2] \neq 0)$

$$P[z_2==0] = P([z_2==0] \cap [s[2]==0]) + P((z_2==0) \cap (s[2]\neq 0))$$

$- 0$ (NULL)

$P(A \cap B)$.

WKT $\longrightarrow$ $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

$$P[z_2==0] = P[(z_2==0)/(s[2]==0)] \cdot P[s[2]==0] + P[(z_2==0)/s[2]\neq 0] \cdot P[s[2]\neq 0]$$

Using conditional probability, $P(A \cap B) = P(A|B) \cdot P(B)$

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$$P[z_2==0] \approx 1 \cdot \frac{1}{256} + \underbrace{\frac{1}{256}}_{\text{if totally random or can be greater}} \cdot \left(1 - \frac{1}{256}\right)$$

$$= \frac{1}{256} + \frac{1}{256} \cdot \frac{255}{256}$$ (negligible)

$$\approx \frac{2}{256}$$

Security: (1) Given ciphertext - hard to find key ✗
(adversary may find plaintext without knowing key)

(2) Given ciphertext - hard to find plaintext ✗
Part of the plaintext may be known (not complete)

(3) Given ciphertext - hard to find any bit of the information ✗

(4) —— " —— - hard to find any function of plaintext ✓

General

Highest level (more of theoretical)

Perfect Security: By Shannon
Given the ciphertext one should not get any bit of information about plaintext.

$$P[M=m] = P[M=m \mid C=c]$$

without ciphertext — with ciphertext doesn't help

Encryption scheme is perfectly secure if for any/every probability distribution over M every message

$m \in M$ and every ciphertext $c \in C$

$$\frac{P[C=c]}{P[M=m]} \cdot P[M=m] = \frac{P[C=c]}{P[M=m]} \cdot P([M=m] / [C=c])$$

$$= \frac{P(M=m) \cap P(C=c)}{P(C=c)} \cdot \frac{P(C=c)}{P(M=m)}$$

$$P[C=c] = \frac{P(M=m) \cap P(C=c)}{P(M=m)}$$

$$\boxed{P[C=c] = P([C=c] / [M=m])}$$

23.01.2018

OTP is perfectly secure.

(1) $P(M=m) = P[M=m \mid C=c]$

Encryption: $M \oplus K = C$

RHS

$$P[M=m \mid C=c] = P[K \oplus C = m \mid C=c]$$

$$= P[K \oplus c = m]$$

By substituting $C=c$

$= P[K = c \oplus m] = \frac{1}{2^\ell}$ (RHS)

$K, M \in \{0,1\}^\ell$

Key can be any value with probability $1/2^\ell$.

$P(M) = 1/2^\ell$ (LHS)

$\therefore$ RHS = LHS

$\frac{1}{2^\ell} = P(M=m) = P[M=m \mid C=c]$

Shannon: A scheme is perfectly secure if and only if $|K| \geq |M|$

Perfect Security is not practical. ($\because$ OTP is not realistic)

(2) $P(C=c) = P[C=c \mid M=m]$ — already proved for all M

(3) $P(C=c \mid M=m_1) = P(C=c \mid M=m_2)$ Both are same probability

Cannot distinguish b/w encryption of m_1 & m_2.
Since, ciphertext doesn't reveal anything about the message.

From (3) $\Longrightarrow$ (2) can be proved.

$$\sum_{\text{all } m} P(C=c \mid M=m_1) \cdot P(M=m_1)$$

$$= P(C=c \mid M=m_1) \cdot 1 = P(C=c)$$

Check for all messages to verify whether it matches the ciphertext or not.

Π (gen, enc, dec)

Lemma: An encryption scheme Π is perfectly secure over message space M if and only if every probability distribution over M, every $m_0, m_1 \in M$ and every $c \in C$.

$$P[C=c \mid M=m_0] = P[C=c \mid M=m_1]$$

We can't say if c is ciphertext for m_0 or m_1, since the probability for both are same.

Adversarial

Adversary Indistinguishability (IND)

(Meaning same as previous Lemma)

Exp: (Experimental) any

1. Adversary outputs two messages m_0, m_1 to challenge.
2. Random bit $b \in \{0,1\}$ and encrypts $E[m_b]$ and sends to adversary.

OR

Random bit $b \in \{0,1\}$ computes ciphertext $C = E[m_b]$ and given to adversary A.

3. Adversary A outputs b'.
4. If $(b == b')$, A succeeded, else A failed to break. return 1

$$Adv_{A,\Pi} = P[Priv_{A,\Pi} = 1] - \frac{1}{2}$$

- $Adv_{A,\Pi}$: Advantage of adversary for Π scheme
- $Priv_{A,\Pi}$: Symmetric/Private cryptosystem
- $\frac{1}{2}$: m_0 or m_1 so probability = 1/2

Definition:

An encryption scheme is perfectly secure if for every A it holds that

$$\boxed{Adv_{A,\Pi} = 0}$$

or $P[Priv_{A,\Pi} = 1] = 1/2$

then, $Adv_{A,\pi} = 1/2 - 1/2 = 0$

Semantic Security: (IND)

↓ Required because perfect security is not possible

An encryption scheme is semantically secure if for every A it holds that

$$\boxed{Adv_{A,\Pi} = \text{negligible} < 1/2^{80}}$$

Ex: Real-time – Login password with 100 bits & 3 attempts. Probability $= \frac{3}{2^{100}}$

Hierarchy of Security:

Semantic Security

↓

IND-CPA attack

adversary knows his choice ($m_1 \rightarrow c_1$, $m_2 \rightarrow c_2$, ⋮, $m_k \rightarrow c_k$)

Known-plaintext attack is also possible.

In the above Exp, include this:

1(a) Adversary can ask ciphertext for plaintext of his choice. (Challenger has to respond)

OR

Adversary has encryption oracle (whatever you ask, give answer)

3(a) Adversary has encryption oracle

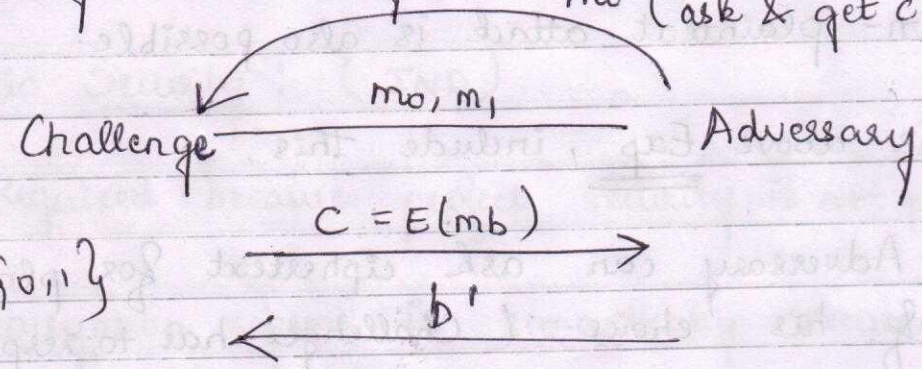
Encryption scheme is IND-CPA scheme if in this game, probability = 0 / negligible

29.01.2018

Semantic Security:

Adv_A^{π} = negl - can't distinguish b/w 2 messages of his choice with negligible probability

This is explained using a Game played b/w adversary & challenger.



If (b = b') then challenge broken

Adv_A^{π} = Prob (b - b') − 1/2

The adversary can win the game if the above probability is negligible.

(IND)

A scheme Π is said to be semantically secure if Adv_A^{Π} = negligible for all A (adversary) & in this GAME.

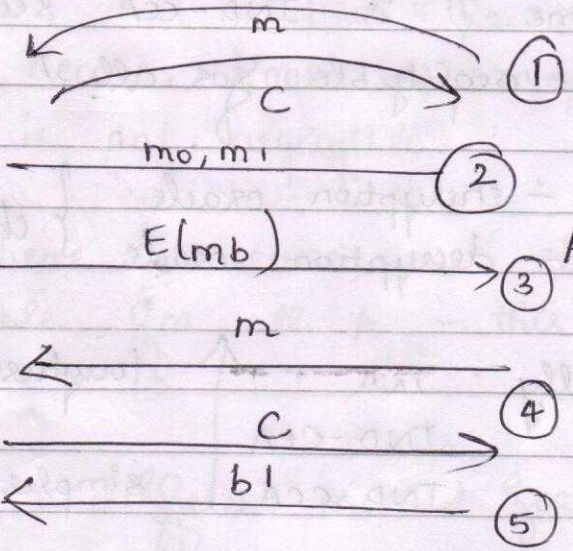
advantage — scheme — adversary

Semantically IND

IND-CPA (Chosen Plaintext Attack)

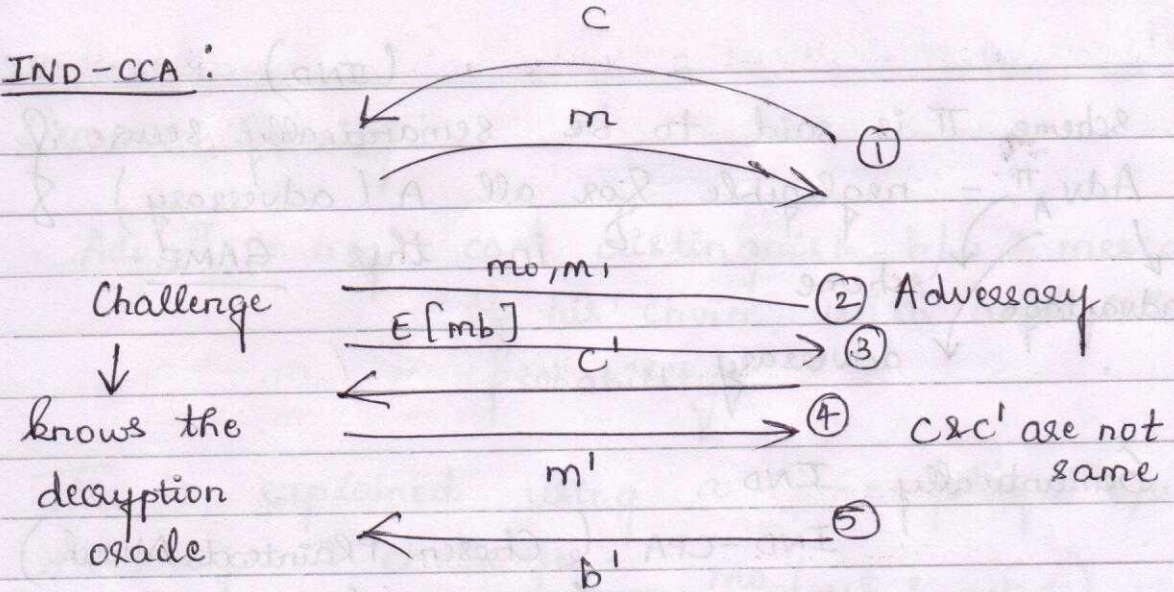
IND-CCA (—"— Ciphertext —"—)

IND-CPA:



Definition: Scheme Π is IND-CPA secure if Adv_A^{Π} = negligible for all A in this GAME

IND-CCA :



Def: Scheme Π is IND-CCA secure if Adv_A^{Π} = negligible for all A in this GAME.

IND-CPA — encryption oracle
IND-CCA — decryption oracle
} challenger

Semantically
IND
IND-CPA
IND-CCA
↑ toughest
simplest to achieve

(1) Not Secure

Ex: $E(\overset{Gen}{K}, Enc, Dec)$ is secure (already proved)

$E'_K(m) = E_K(m) \,||\, LSB(m)$

Show that E' is not semantically secure.

PROOF:

① $D'(c) = D(c - \text{last bit})$

This scheme reveals one bit of info - LSB of m.
Hence, not semantically secure.

OR

② Using GAME:

Choose 2 messages whose last bits are different
Prob = 1/2 - not negligible

To prove not secure, choose an example & prove that Prob is not negligible.

To prove scheme is secure, we should prove Prob - negligible for all A - this is impossible.

↓

Hence we use a different method for proof.

Proof by Reduction:

If adversary can break a scheme with non-negligible probability, then there exists

Proofs { Jonathan & Katy
Dan Boneh - Coursera

a challenger who can break a proved scheme or a solve a hard problem with non-negligible probability.

$A \rightarrow B \iff \neg B \rightarrow \neg A$

$\neg B \rightarrow T$

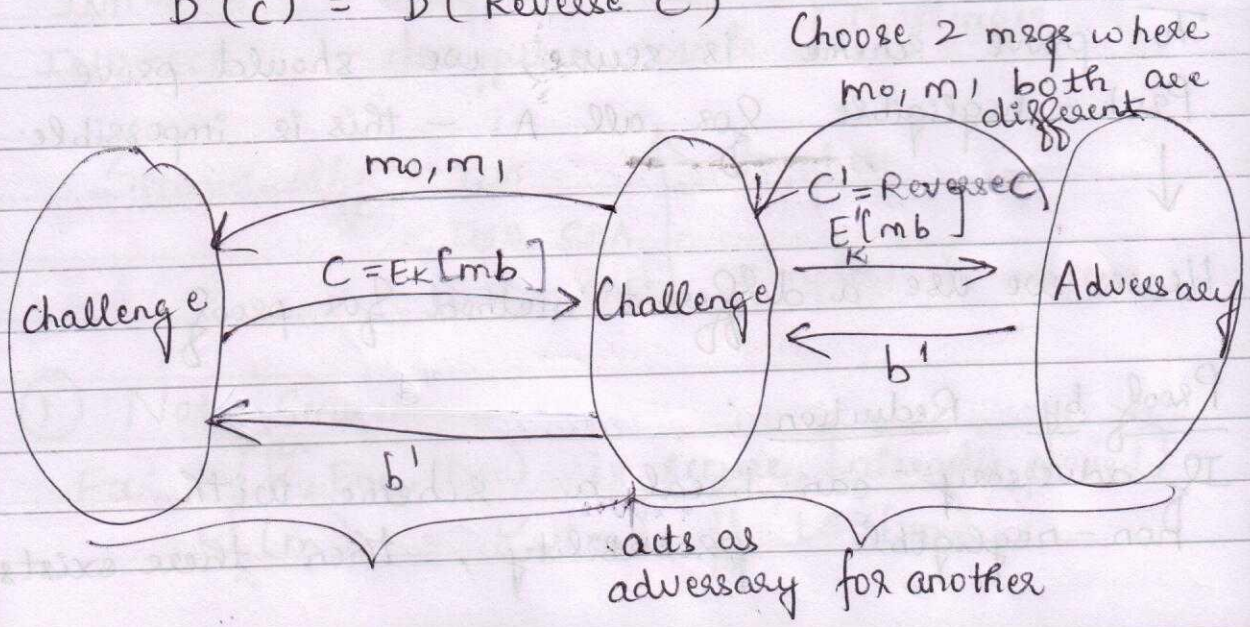
$\neg A$ is true

If this is true → then true (implies)

Given $E(Gen, Enc, Dec)$ is secure (proved)

$E'(m) = Reverse(E(m))$

$D'(c) = D(Reverse\ c)$



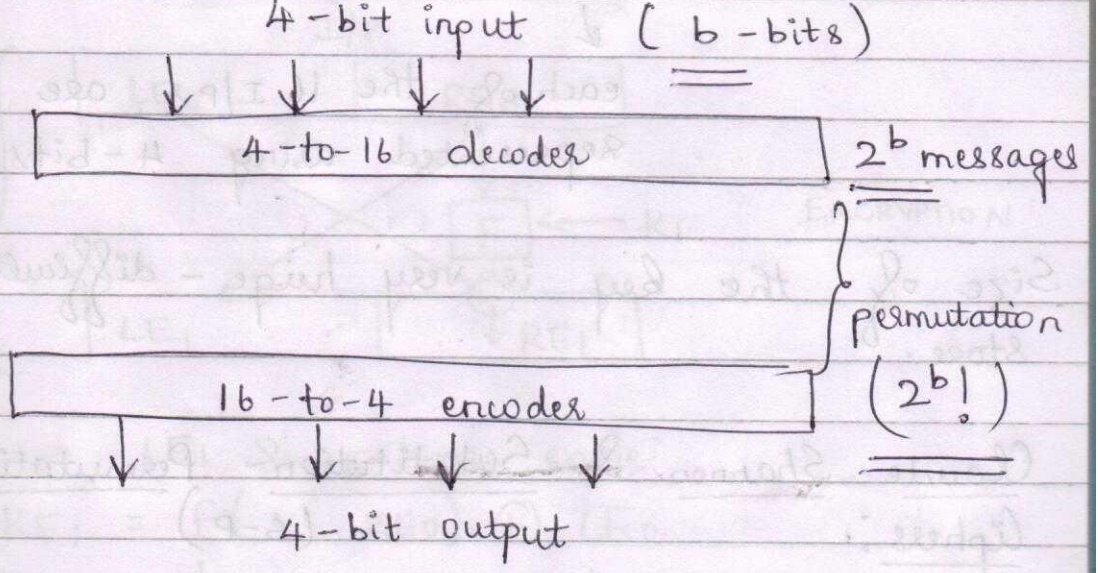
01.02.2018

DES: (Lecture Slides - William Stallings)

Block Ciphers:

Feistel Cipher Structure

Ideal block cipher



Suppose I/P is 'b' bits

No of different messages $= 2^b$

No of " " permutations $= 2^b!$

Key is one of the above permutation

Using brute-force method to break the message

$= O(2^b!)$ – worst case

Size of key $= b \cdot 2^b$

↓

for each permutation 'b' bits are required

In the above $b = 4$

$= 4 \cdot 2^4$

↓

each of the 16 I/P's are represented using 4-bits

Size of the key is very huge - difficult to store.

Claude Shannon & Substitution-Permutation (S-P) Ciphers:

S-P elements

Diffusion & confusion → relationship b/w key & ciphertext should be complex

↓

relationship b/w ciphertext & plaintext should be complex

Diffusion - Non-linear operations

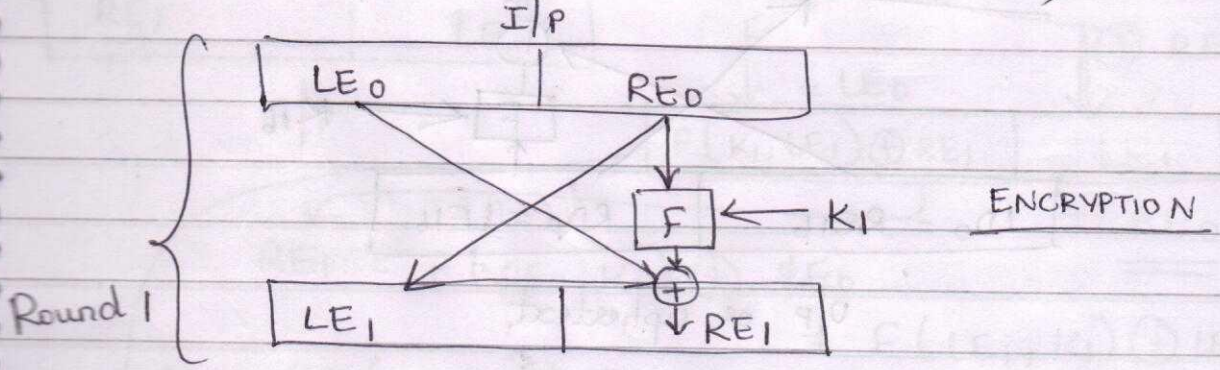
Confusion - Permutation, Shifting, Substitution

Feistel Cipher Structure;

DES is based on this

64-bit — 2 parts → 32-bit
→ 32-bit

DES - 16 rounds (all rounds are same)



LE1 & RE0 are same

$RE_1 = f(K_1, RE_0) \oplus LE_0$

↓

what is this function?

$K_1, K_2, \ldots K_{16}$ — keys for 16 rounds

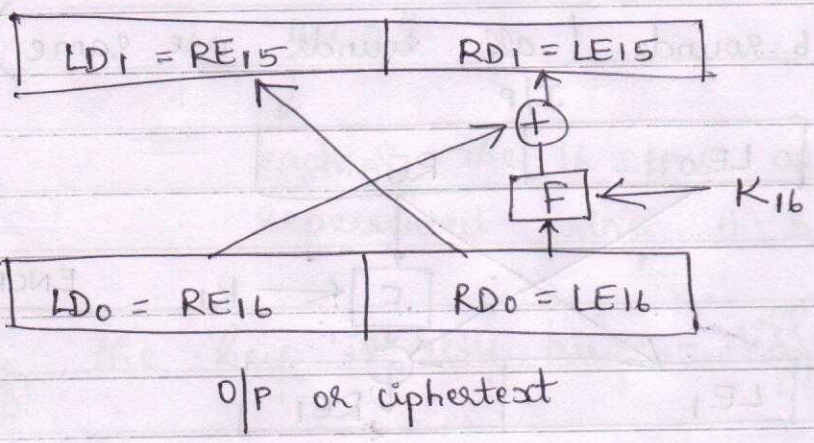
Size of Key = 56 bits

After 16th round, swapping is done to get the output.

DECRYPTION : Same as encryption

Start from o/p of encryption

Swapping is done at the last here also & not at the beginning.

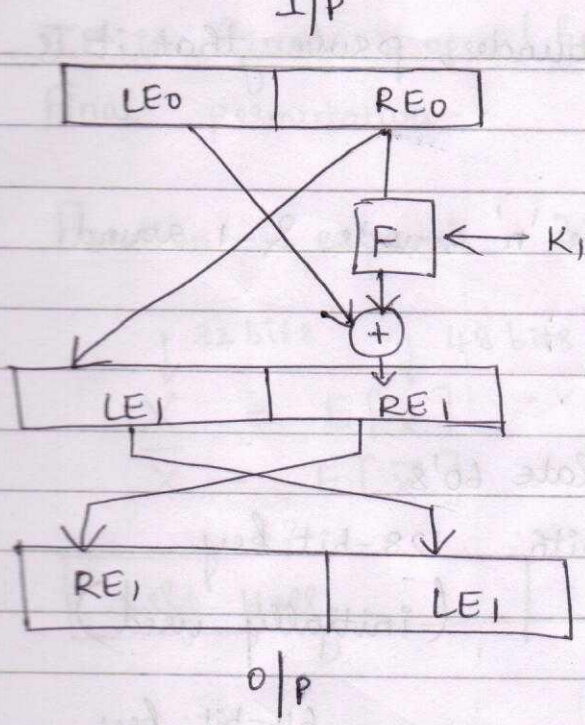


Proof for "Decryption is similar to Encryption" using mathematical induction.

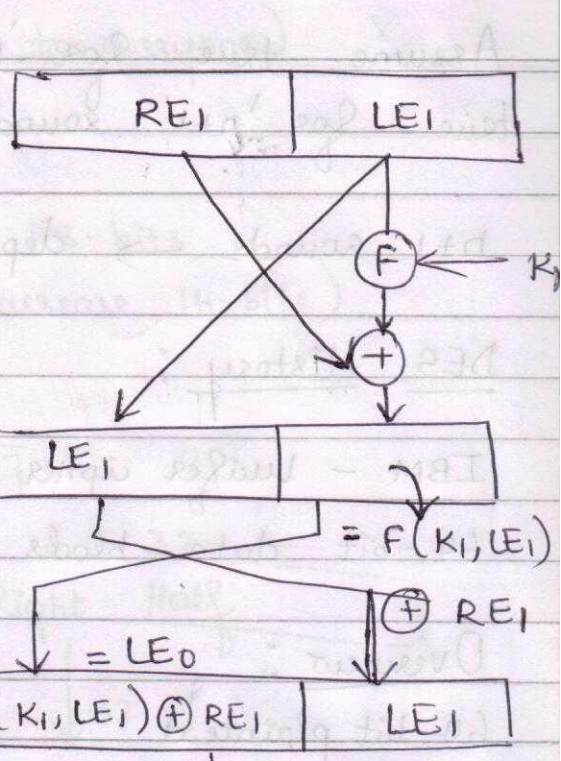
First prove for one round.

(Prove physically)

ENCRYPTION



DECRYPTION



$RE_1 = f(RE_0, K_1) \oplus RE_0$

$= f(LE_1, K_1) \oplus LE_0$

~~$f(K_1, LE_1) \oplus RE_1$~~

~~$f(K_1, RE_0) \oplus RE_1$~~

$f(K_1, LE_1) \oplus RE_1$

$f(K_1, LE_1) \oplus f(LE_1, K_1) \oplus LE_0$

$= 0 \oplus LE_0$

$= LE_0$

Assume true for 'n' rounds, prove that it is true for 'n+1' rounds.

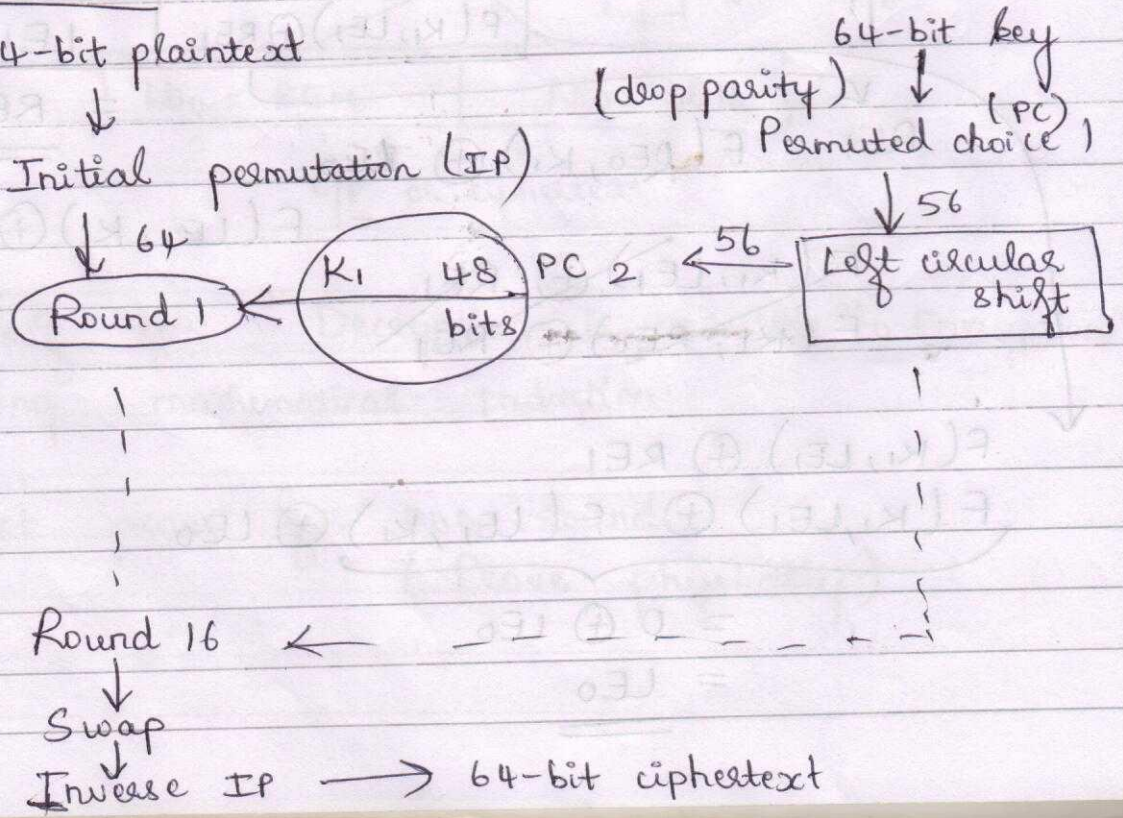
n+1 rounds → depict as 'n' rounds & 1 round.

DES History:

IBM - Lucifer cipher - late 60's

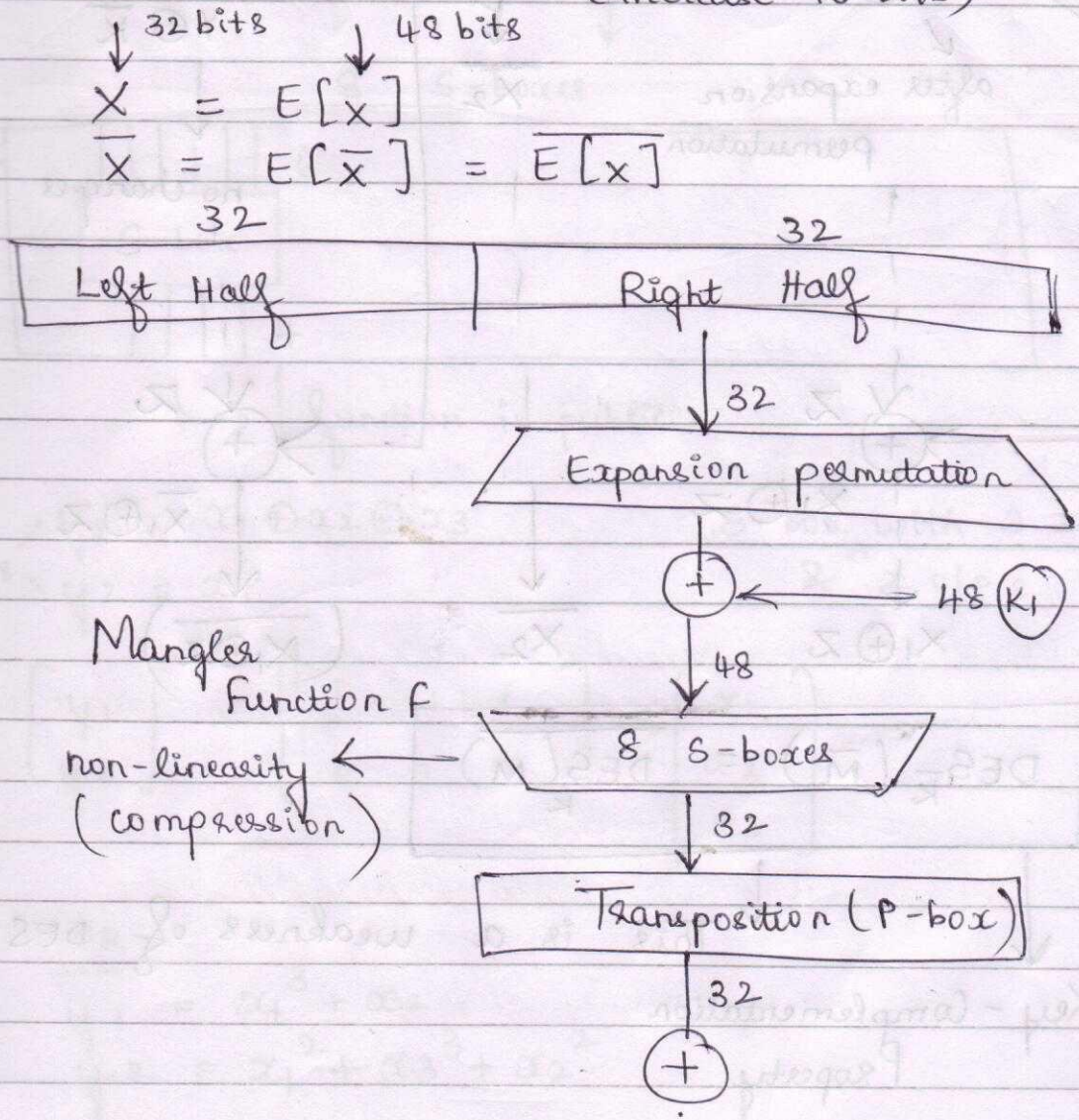
64-bit data blocks with 128-bit key (initially used)

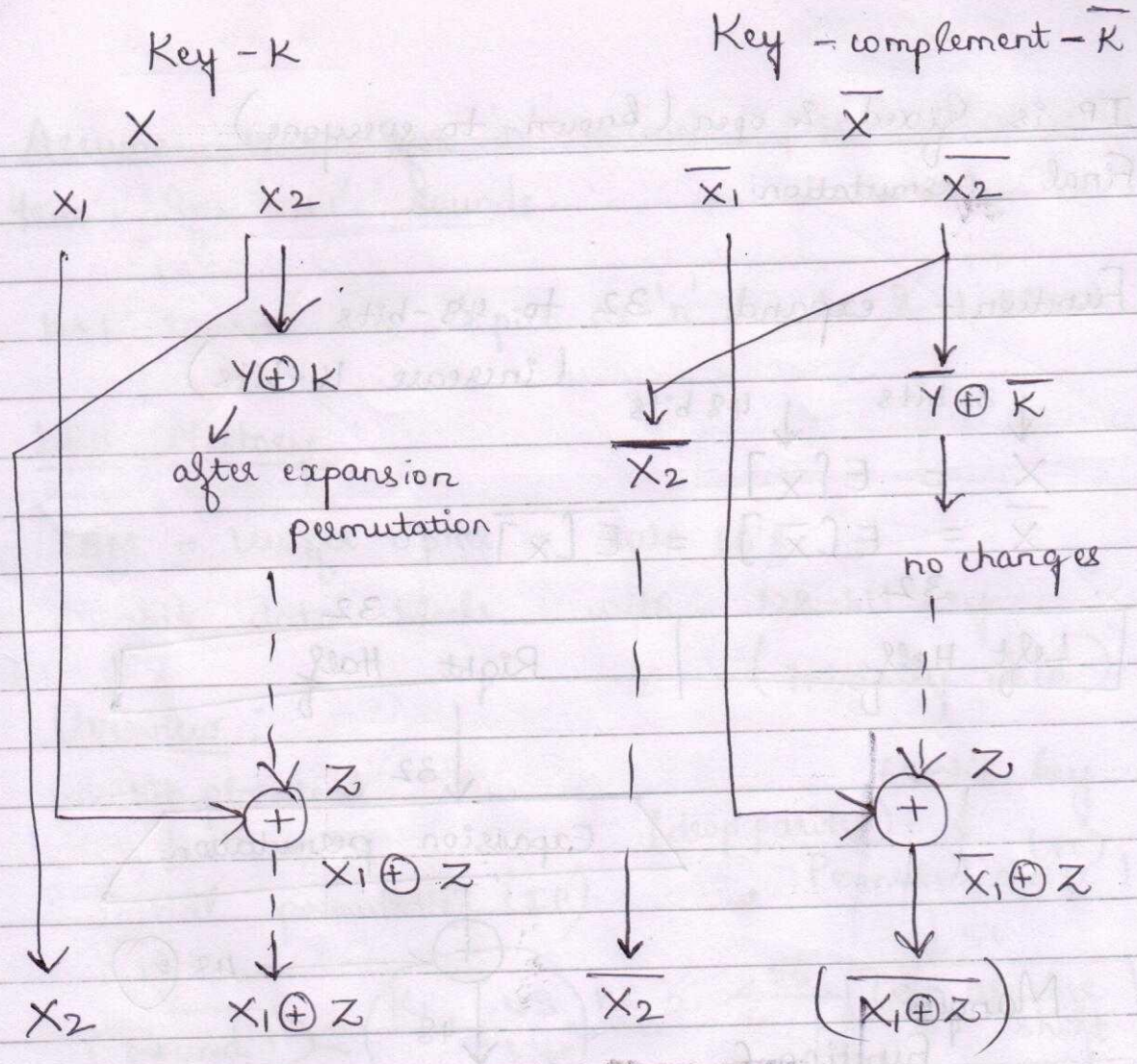
Overview:



IP is fixed & open (known to everyone)
Final permutation

Function - expand 32 to 48-bits
(increase 16-bits)



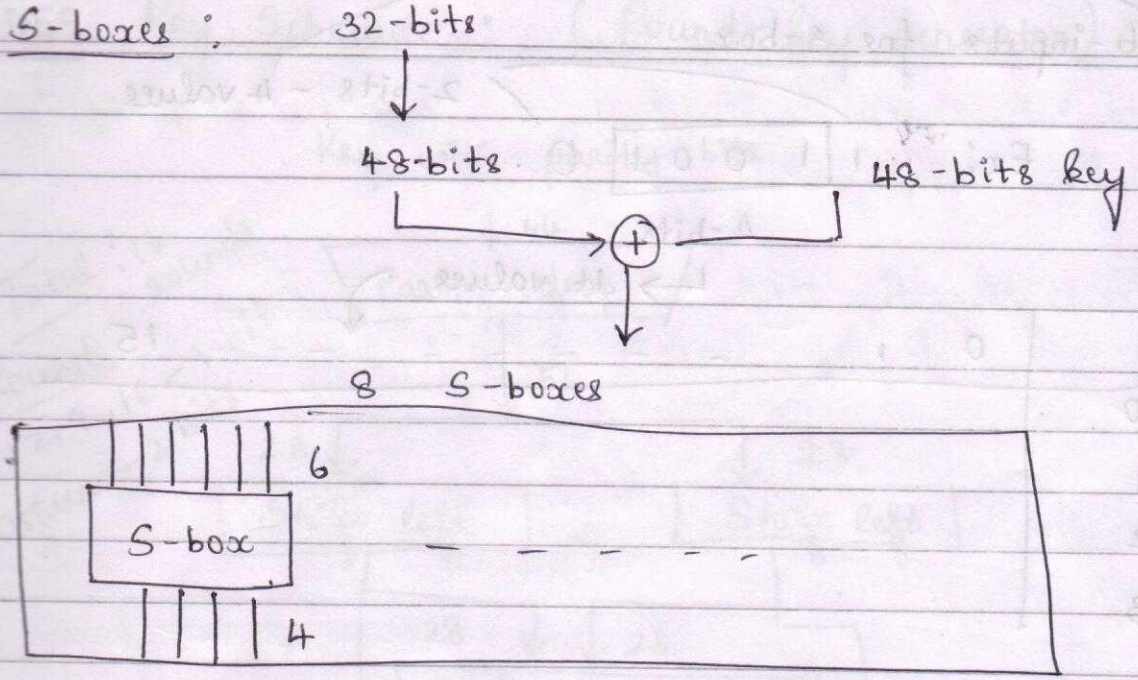


$$DES_{\bar{K}}(\bar{M}) = \overline{DES_{K}(M)}$$

This is a weakness of DES

Key - Complementation Property

S-boxes :



↳ function is public

$y_1 = x_1 \oplus x_2 \oplus x_3$

o/ps

$y_2 = x_1$

S-box with 3 I/ps & 2 o/ps

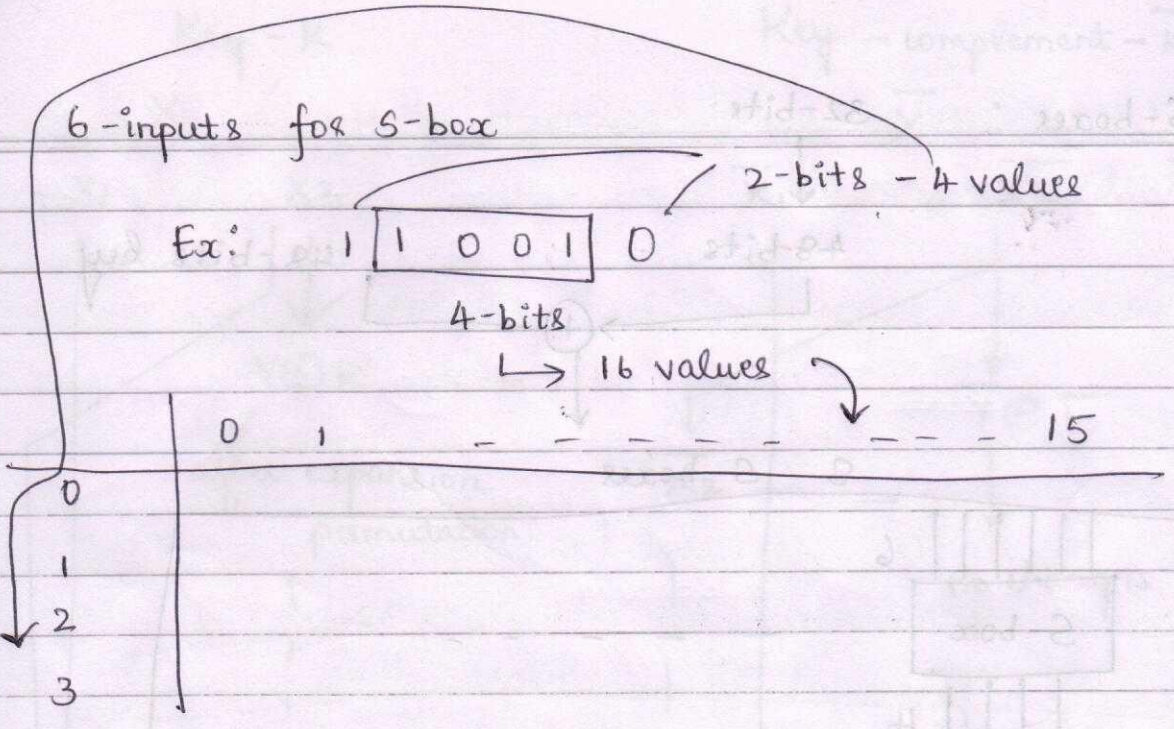
$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

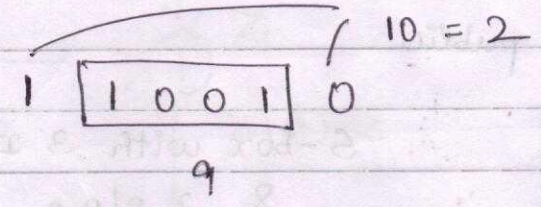
OR

$y_1 = x_1^3 + x_2$

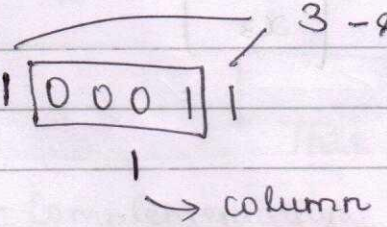
$y_2 = x_1^2 + x_3^3 + x_2^2$

6-inputs for S-box

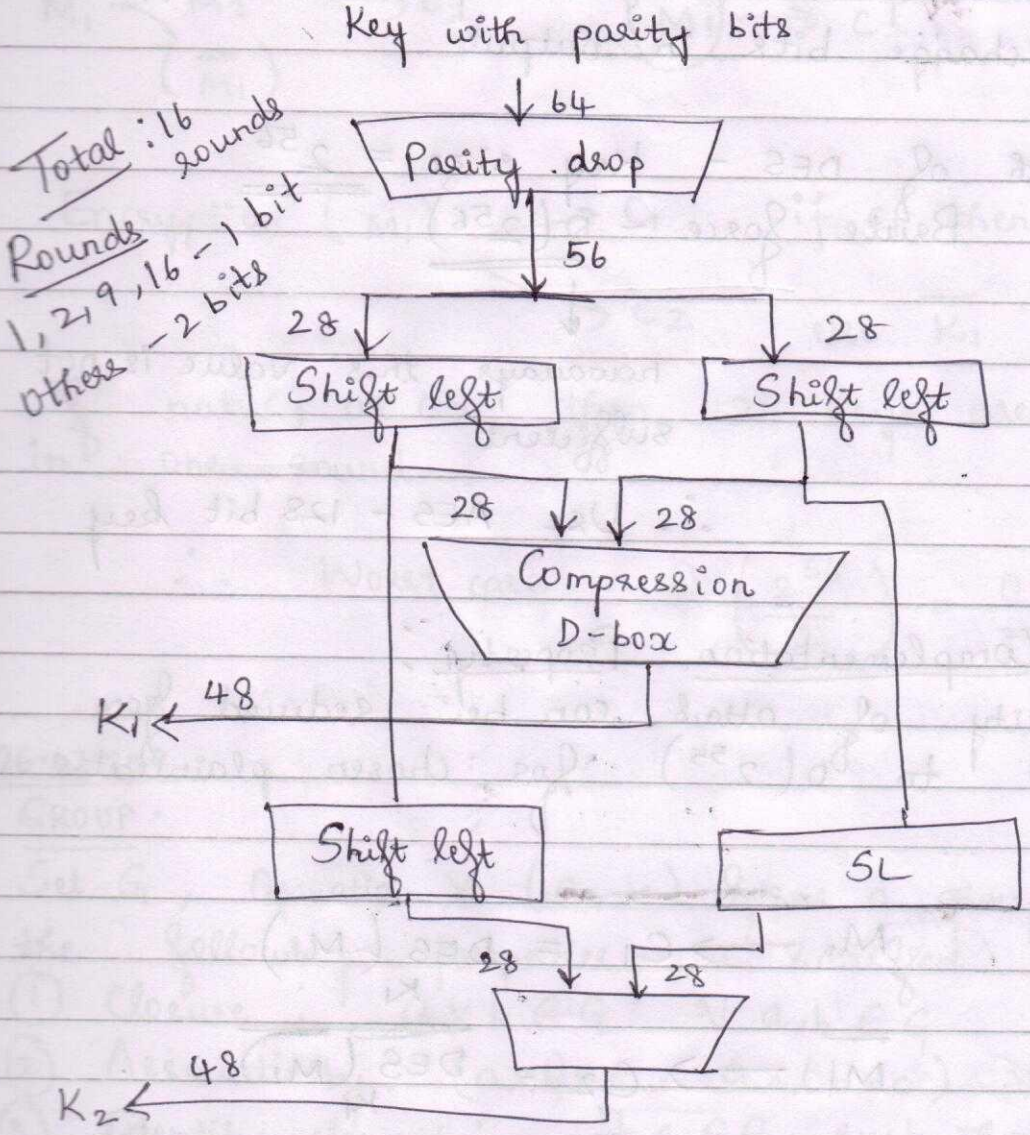




Check Row = 2, Colum = 9, get the 4-bit value as o/p



DES Key Schedule : (Round-key generator)



Avalanche Effect :

One bit change in key or plaintext - approx. half change bits in output.

Strength of DES - Key size = 2^{56}

Brute force - $O(2^{56})$

↓

nowadays this value is not sufficient

∴ Use AES - 128 bit key

Key - Complementation Property :

Complexity of attack can be reduced from $O(2^{56})$ to $O(2^{55})$ for chosen plaintext attack.

$$M_1 \longrightarrow C_1 = DES_{K_1}(M_1)$$

$$\overline{M_1} \longrightarrow C_2 = \overline{DES_{K_1}(M_1)}$$

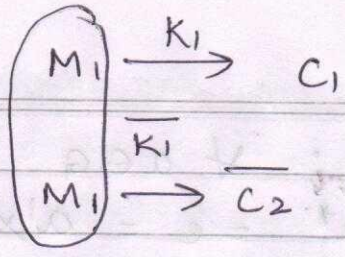
$\overline{C_2} = DES_{K_1}(M_1)$ by using

$DES_{\bar{K}}(\bar{M}) = DES_K(M)$

$\therefore M_1 \xrightarrow{K_1} C_1$

$\overline{M_1} \xrightarrow{\overline{K_1}} \overline{C_2}$

$M_2 = (\overline{M_1})$



Encryption $(M_1) \rightarrow C_1$ if C_1 then key $= K_1$

$\rightarrow C_2$ else $\overline{K_1}$

If not C_1 or C_2, then 2 keys are removed in one round.

$\therefore$ Worst case $= O\left(\frac{2^{56}}{2}\right) = \underline{\underline{O(2^{55})}}$

06.02.2018

GROUP:

Set G, Operation $\times$ $(G, \times)$ forms a group if the following properties are satisfied:

1. Closure: $a \times b \in G \quad \forall a, b \in G$
2. Associativity: $(a \times b) \times c = a \times (b \times c) \quad \forall a, b, c \in G$
3. Identity element: $\exists e \in G$ such that (there exists, unique) $e \times a = a \times e = a \quad \forall a \in G$

④ Inverse : $\forall\ a \in G \quad \exists$ unique a' such that
$a \times a' = e = a' \times a$

Ex: 1. p is prime
$Z_p = \{1, 2, - - - p-1\}$
Operation $*$ mod p
Show that the above forms a group

0 is not included since p is prime
$\neq mp$
↓ multiple of p

① Closure : mod p hence all elements belong to Z_p
② Associativity
③ Identity : 1 is identity element
④ Inverse : Use Fermat's theorem (to find inverse)

∴ Z_p is a GROUP.

Fermat's Theorem :

$a^{p-1} \equiv 1 \bmod p$

OR $a^{p-1} \bmod p = 1$

$a * a^{p-2} = 1$

↓

inverse of a

Ex: 2. $Z_p = \{0, 1, 2, \ldots p-1\} * \bmod p$

This is not a group.

Inverse of 0 does not exist

$(0 * \_ \neq 1)$

Ex: 3. $Z_5 = \{1, 2, 3, 4\} * \bmod 5$

$= \{3, 4, 2, 1\}$

$3 \quad 3^2 \quad 3^3 \quad 3^4$ (3^5 will again be 3)

$3^2 = 9 \bmod 5 = 4$

$3^3 = (4 \times 3) \bmod 5 = 2$

$3^4 = (2 \times 3) \bmod 5 = 1$

$3^5 = (1 \times 3) \bmod 5 = 3$

∴ Z_5 can be re-written as

$$Z_5 = \{ 3, 3^2, 3^3, 3^4 \} * \bmod 5$$

3 → generator

$3^2, 3^3, 3^4$ → CYCLIC GROUP

All the elements can be written as power of an element. (generator)

$$Z_p = \{ g, g^2, \cdots g^{O(a)} \} * \bmod p$$

g → generator

Z_p is always a CYCLIC GROUP

Order of a = $O(a)$ = { least positive integer such that $a^{O(a)} \equiv 1 \bmod p$

$a^{O(p)} \bmod p = 1$ }

1 → identity

$Z_5 = \{ 3, 4, 2, 1 \}$

$O(2) = 3^2 \bmod 5 = 9 \bmod 5 = 4$

$O(1) = 1^1 \bmod 5 = 1$

$O(3) = 3^3 \bmod 5 = 4$

$O(4) = 2$ $\quad 4^4 \bmod 5 = 1$

$4^2 \bmod 5 = 1$

$\therefore o(2) = 4,\ o(3) = 4,\ o(4) = 2,\ o(1) = 1$

Schnorr Group: Cyclic subgroup of size 'q' (prime).

$p = 11$

$11 - 1 = (p-1) = 2 \cdot q = 2 \cdot 5$ (2: prime, 5: prime)

$(p-1)$ may not be prime

Choose p and q (primes) such that $p - 1 = 2 \cdot q$

$Z_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ * mod 11

Theorem:
$(Z_p, * \bmod p)$ is CYCLIC GROUP.

Z_{11} is cyclic group.
First find generator element.

$Z_{11} = \{3, 9, 5, 4, 1, 3\}$
$\quad\quad\ 3\quad 3^2\quad 3^3\quad 3^4\quad 3^5\quad 3^6$

$\therefore$ 3 is not the generator

$Z_{11} = \{ \underset{2}{2}, \underset{2^2}{4}, \underset{2^3}{8}, \underset{2^4}{5}, \underset{2^5}{10}, \underset{2^6}{9}, \underset{2^7}{7}, \underset{2^8}{3}, \underset{2^9}{6}, \underset{2^{10}}{1} \}$

$\therefore$ 2 is the generator

$Z_{11} = \{ \underset{5}{5}, \underset{5^2}{3}, \underset{5^3}{4}, \underset{5^4}{9}, \underset{5^5}{1}, \underset{5^6}{5} \}$

$\therefore$ 5 is not generator

$H = \{ 3, 9, 5, 4, 1 \} * \text{mod } 11$

$H = \{ \underset{3, 3^2, 3^3}{3}, \underset{3^4}{9}, \underset{3^5}{5}, 4, 1 \}$

$\therefore$ 3 is the generator here

H is set of elements chosen from Z_{11}.
H is a group — Identity $= 1 \ (3^5)$
Inverse of 5 is 9 $(3^3)(3^2)$
$3+2=5$

$a \in Z_p$
$H = \{ a, a^2, a^3, \text{----} a^{o(a)} \}$
$\downarrow$
identity $= e$

H is always finite.

H is subgroup of Z_p.

∴ H is cyclic subgroup of Z_p.

Z_p maybe equal to H also.

Here $H = \{3, 9, 5, 4, 1\}$

$Z_{11} = \{1, \dots 10\} * \bmod 11$

H is cyclic subgroup of Z_{11}

Also, H is Schnorr group since no. of elements in H = 5 (which is prime)

Euler's Theorem :

$$\phi(a) = \left| \{ 1 \leq b < a : GCD(b, a) = 1 \} \right|$$

1 to a-1

↓

b & a are relatively prime

$$\phi(10) = \left| \{1, 3, 7, 9\} \right| = 4$$

↓

no. of elements relatively prime to 10 & less than 10

Theorem :

Any number 'n' can be written as primes

$p_1, p_2, \ldots p_K$

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_K^{a_K}$$

$25 = 5 \times 5 = 5^2$

$50 = 2 \times 25 = 2^1 \times 5^2$

$100 = 4 \times 25 = 2^2 \times 5^2$

$15 = 3^1 \times 5^1$

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \ldots (p_K^{a_K} - p_K^{a_K-1})$$

$\phi(10) = (2^1 - 2^0) \times (5^1 - 5^0)$

$= (2-1) \times (5-1) = 1 \times 4 = 4$

$\phi(10) \downarrow 2 \times 5$

07.02.2018

Extended Euclidian Algorithm :

- $GCD(a, n) = GCD(n, a \bmod n)$
- Terminating
  - $GCD(0, x) = x$
  - $GCD(1, x) = 1$

↳ Recursive

To find GCD of 2 numbers.

To find $a^{-1} \bmod n$

$GCD(a, n) = 1$ only then inverse exists

Given a, b ∃ x and y such that

$ax + by = GCD(a, b)$" — THEOREM

$a = 9$

$b = 15$

$9 \times x + 15 \times y = GCD(9, 15)$

$9x + 15y = 3$

$9 \times +2 + 15 \times -1 = 3$

$x = 2$ and $y = -1$

Extended Eucledian Algorithm (a, b) r_0 r_1

Output (x, y)

$r_0 = 1 \cdot r_0 + 0 \cdot r_1 = 1$

$r_1 = 0 \cdot r_0 + 1 \cdot r_1 = 0$

r_0 / r_1 = quotient $\quad \boxed{q_i = \frac{r_{i-1}}{r_i}}$

$r_2 = r_0 \bmod r_1$

$r_3 = r_1 \bmod r_2$

$\boxed{r_i = r_{i-2} \bmod r_{i-1}}$

	q_i			
r_0		1	0	initial values
r_1	r_0/r_1	0	1	
r_2	r_1/r_2	PP − q P	PP − q P	
r_3	r_2/r_3	↓ previous		
1		$1 - r_0/r_1 \cdot 0$		
⋮				
GCD (r_0, r_1)		x	y	
Repeat till 0				

Ex: $r_0 = 15$, $r_1 = 9$

	q_i		
15		1	0
9	1	0	1
6	1	1	-1
3	2	(-1)	(2)
0		x	y

$x = -1$

$y = 2$

Suppose, $ax + by = 1$ i.e GCD $(a, b) = 1$

$b^{-1} \bmod a = ?$

$ax + by = 1$ (Multiply $b^{-1} \bmod a$)

$(b^{-1}ax + b^{-1}by) \bmod a = b^{-1} \bmod a$

$(b^{-1}\underline{a}x + y) \bmod \underline{a} = b^{-1} \bmod a$ ($\because a \bmod a = 0$)

$0 + y = b^{-1} \bmod a$

$b^{-1} \bmod a = y$

To find $28^{-1} \bmod 75$

	q_i			
75		1	0	
28	2	0	1	
19	1	1	-2	
9	2	-1	3	
1	9	3	(-8)	$-8 \bmod 75$
0				$(67-75) \bmod 75$

$-8 = 75 - 8 = (67)$ is inverse

$Z_{11} = \{1, 2, 3, \ldots p-1\}$ * mod p is a group.

Compute

$K = \{1 \le a < 8 \quad GCD(a, n) = 1\}$ * mod n is also a group.

For example,

Closure: $K_{\phi}(10) = \{1, 3, 7, 9\}$

$GCD(a, 10) = 1$

Given:

$GCD(a, n) = 1 = GCD(b, n) = 1$

then $GCD(ab \bmod n, n) = 1$

$\rightarrow GCD(ab, n) = 1$

a is relatively prime to n

b is relatively prime to n

$\therefore$ axb is relatively prime to 1

$GCD(ab, n) = 1$

$\downarrow$ ~~Extended~~ Eucledian algorithm

$GCD(ab \bmod n, n) = 1$

Inverse:

Eular's theorem:

$a^{\phi(n)} \bmod n = 1$

$a^{-1} = a^{\phi(n)-1} \bmod n$

RING:

Set $(R, \boxplus, *)$ form a ring (2 operations and 1 set)

(commutative group)

1. $(R, \boxplus)$ forms an Abelian group
2. $(R, *)$ closed associative

Closure, Associative, Identity, Inverse & Commutative

① Ex: $(R, +, \times)$ ring

↓ real nos

$(R, +)$ forms an abelian group

Identity = 0, Inverse of $x = -x$

$(R, \times)$ closed & associative

② $(I, +, \times)$ ring

$(I, +)$ is abelian group

Identity = 0, Inverse of $x = -x$

$(I, \times)$ closed & associative.

↓ set of integers (+ve & -ve)

FIELD :

Set $(F, \boxplus, *)$ forms a field if:

① $(F, \boxplus)$ is an Abelian group

② $(F, *)$ – closed, associative, identity (this is different from identity of $(F, \boxplus)$), except identity of $(F, \boxplus)$ all other elements must have inverse (Same as group)

$a * (b \boxplus c) = (a * b) \boxplus (a * c)$

↳ Distributive property (only 1 & not both)

Ex: ① $(R, +, \times)$

$(R, +)$ forms an Abelian Group

Identity $= 0$

$(R, \times)$ – except 0 all other elements have inverse $\left(\text{Inverse} = \frac{1}{x}\right)$

$1/0$ is not defined ∴ 0 does not have inverse.

∴ Forms a field.

② $(I, +, \times)$ is not a field

For $(I, \times)$ inverse $= 1/x \notin I$

In cryptography, we require finite fields.
∴ Use modulo operation.

Finite field:

$G = \{0, 1, 2, \dots p-1\}$ + mod p, * mod p

Field of size 'p'

① $G = \{0, 1, 2, \dots p-1\}$ + mod p

Identity = 0, Inverse exists $a^{-1} = p - a$

∴ Abelian group

② $G = \{0, 1, 2, \dots p-1\}$ * mod p

Identity = 1

Inverse exists for all except 0

① & ② satisfied

Also distributive ∴ forms a FIELD

$G = \{0, 1\}$ + mod 2, * mod 2 is a FIELD.

↓ is a prime number

Additive inverse of 1 = 1 (-1)

Field (2^n) OR FIELD (p^n)

p is less than 2^n. For ex, p = 19 we

Require 5-bits to represent but $2^5 = 32$ $(19 < 32)$, so remaining space is wasted.

Prime Polynomial:

prime
x^2+1 over the field (R)

x^2+1 over the field of complex numbers
$(x+i)(x-i)$
↳ not prime

Field (2^n):

$\{0,1\}$, $+ \bmod 2$, $* \bmod 2$

Choose prime polynomial of degree 'n' over GF(2).

$$G = \{ a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \} \quad a_i \in GF(2)$$

Set of polynomial of degree atmost $n-1$.

Two operations are:

1. $+$ mod prime polynomial of degree 'n'
2. $*$ mod " "

No of elements of $G = 2^n$

Each of the 'n' elements can be either 0 or 1.

① $(G, +)$ is a group

1. Closure : Add 2 polynomials of degree 'n-1' the sum will be of degree 'n-1'
2. Associativity
3. Identity : 0 or $(0, \underbrace{0, 0 - - - - 0}_{n \text{ times}})$
4. Inverse : Same polynomial
   ($\because$ + mod 2 is same as XOR)
5. Commutative

② $(G, *)$

1. Closure
2. Associativity
3. Identity : 1 $(1, 0, 0, - - - - 0)$
4. Inverse : Euclidian algorithm
   Only 0 does not have inverse

③ Distributive property

Ex: Prime polynomial : x^3+x+1
of degree 3
Field (2^3) can be constructed

(1)

$(x+1)^{-1} \mod (x^3+x+1)$ $\quad a_i \in GF(2)$

↓ degree 1 ↓ degree 3

	q_i		
x^3+x+1		1	0
$x+1$	x^2+x	0	1
~~x^2+x+1~~		1	$-(x^2+x) = x^2+x$

↓ inverse

x^2+x

$x+1$ | x^3+x+1

x^3+x^2

x^2+x+1

x^2+x

1

$x^3 - x^3$

↓ not operation in GF(2)

∴ Apply operation of GF(2)

$-x^2 = x^2$

Inverse is itself

(2)

Inverse of $(x^2+1) \mod (x^3+x+1)$

(3) Inverse of x^2+x+1 mod (x^3+x+1)

	q_i		
x^3+x+1		1	0
x^2+x+1	$x+1$	0	1
x	$x+1$	1	$-(x+1)$ = $x+1$
1		$-(x+1)$ = $x+1$	$1-(x+1)(x+1)$
			$1+x^2+1+2x$
			$= x^2+2x+2$

$$\begin{array}{r|l} & x+1 \\ \hline x^2+x+1 & x^3+x+1 \\ & x^3+x^2+x \\ \hline & x^2+1 \\ & x^2+x+1 \\ \hline & x \end{array}$$

$$\begin{array}{r|l} & x+1 \\ \hline x & x^2+x+1 \\ & x^2 \\ \hline & x+1 \\ & x \\ \hline & 1 \end{array}$$

Inverse $= 1-(x+1)(x+1)$

$= 1+x^2+1 = (1+1)+x^2$

$= 0+x^2$

$= x^2$

$$\begin{array}{r} x+1 \\ \times\ x+1 \\ \hline x^2+x \\ x+1 \\ \hline x^2+(1+1)x+1 \end{array} = x^2+1$$

(Apply GF(2) operations)

15.02.2018

Field (p^n) prime p

$F = \{$ Set of polynomial of degree atmost $n-1$ $\}$ + mod degree of polynomial $n \cdot x$ mod degree polynomial n.

Field (Z_p)

$a_0 + a_1x + a_2x^2 + \_\_\_\_ a_{n-1}x^{n-1} \quad \forall a_i \in Z_p$

Construct Field (3^3)

$F = \{a_0 + a_1x + a_2x^2\}$. Prime polynomial of degree (x^3+x+1)

Totally, there will 27 elements.

0	x	x^2	x^2+x	~~x^2+x+3~~
1	$x+1$	x^2+1	x^2+x+1	~~x^2+x+4~~
2	$x+2$	x^2+2	x^2+x+2	

a_2x^2	a_1x	a_0
0	0	0
0	0	1
0	0	2
0	1	0
0	1	1
0	1	2
0	2	0

$GF(3) = \{0, 1, 2\}$

Inverse of $2x^2+x+2$ modulo (x^3+x+1)

	q_i		
x^3+x+1		1	0
$2x^2+x+2$	$2x+2$	0	1
x	x	1	$-(2x+2)$
2			

$$
\begin{array}{r|l}
 & 2x+2 \\
\hline
2x^2+x+2 & x^3+x+1 \\
 & \underline{2\cdot 2x^3 + 2x^2 + 2x \quad (2\cdot 2)} \\
 & \quad -2x^2+1 = x^2+1 \\
 & \underline{(2\cdot 2)x^2 + 2x + 2\cdot 2} \\
 & \quad -2x+0 = 2x \\
 & \quad = x
\end{array}
$$

$[-2 = -2+3 = 1]$

$2x^2$ to get x^3

$\frac{1}{2}x$

$\frac{1}{2}$ is not an element of GF

$\therefore$ Find $2^{-1} = 2$ here

Use $2^{-1} = 2$ during division

$$
\begin{array}{r|l}
 & 2x+1 \\
\hline
x & 2x^2+x+2 \\
 & \underline{2x^2} \\
 & \quad x+2 \\
 & \quad \underline{x} \\
 & \quad 2
\end{array}
$$

$$
\begin{array}{r|l}
 & 2x \\
\hline
2 & x \\
 & \underline{x} \\
 & \quad 0
\end{array}
$$

Not possible

Problem with DES :

Size of key is small = 56 bits

$$\therefore \text{Use 2-DES} \rightarrow K = (\underset{56}{K_1}, \underset{56}{K_2}) = 112 \text{ bits}$$

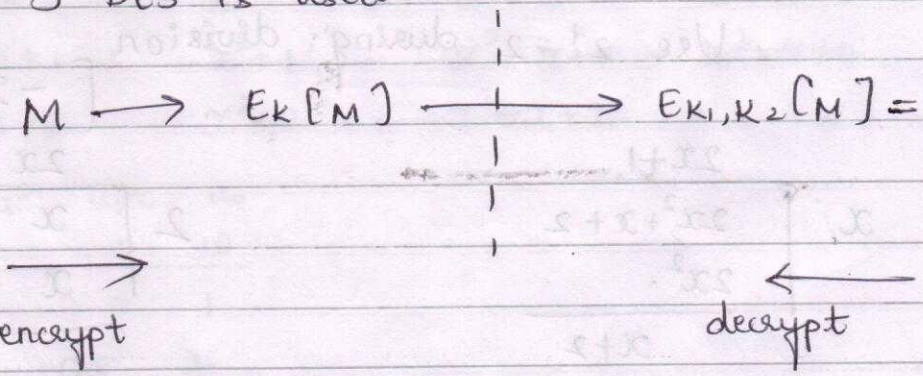
$$E_{K_2}\left[E_{K_1}(M)\right] = E_K(M)$$

Trial method $-O(2^{112})$

2-DES method is very slow.

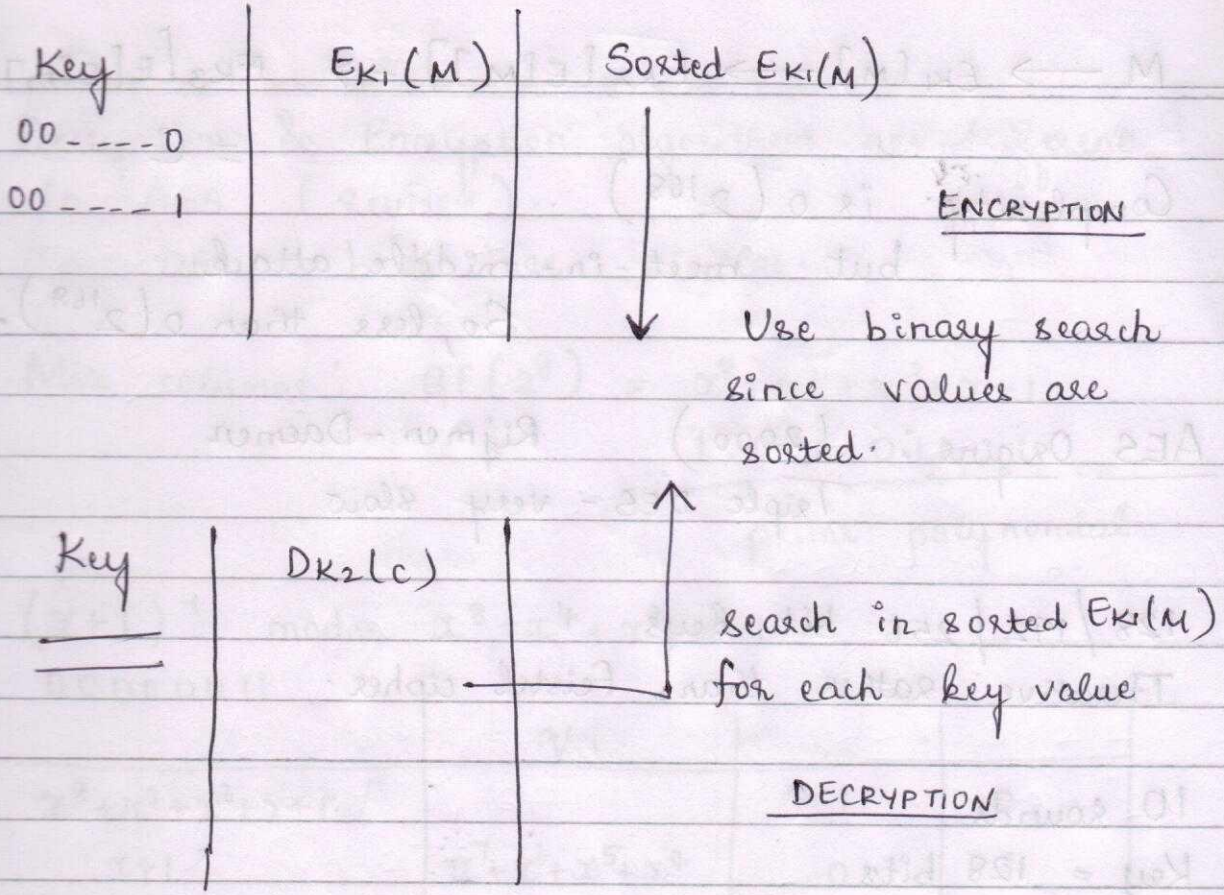
Meet-in-middle attack :

2-DES is not used because of meet-in-middle attack. 3-DES is used.



$M \rightarrow C$

For whichever value encryption & decryption are same, value of key is found.



1. Find $E_{K_1}(M)$ for all K_1.
2. Sort $E_{K_1}(M)$
3. For each K_2 find $D_{K_2}(c)$
4. Search in sorted $E_{K_1}(M)$

$$O(2^{56}) + O(2^{56}\log(2^{56})) + O(\log 2^{256})$$

↓ encryption ↳ sorting ↳ searching

$$O(2^{56+7}) \approx O(2^{63})$$

$M \longrightarrow E_{K_1}[M] \longrightarrow E_{K_2}[E[M]] \longrightarrow E_{K_3}[E[E[M]]] = C$

Complexity is $o(2^{168})$
but meet-in-middle attack
So, less than $o(2^{168})$.

AES Origins: (2000) Rijmen-Daemen
Triple DES - very slow

128/192/256 bit keys
Iterative rather than Feistel cipher.

10 rounds
Key = 128 bits
I/p will considered as 4x4 matrix
128 bits = 16 bytes (128/8)
- provides confusion

1. Byte substitution (s-box) - non-linear
2. Shift rows
3. Mix columns - not in last round } diffusion
4. Add round key

Each round

View as alternating XOR key & scramble data types

Decryption & Encryption algorithms are different in AES (reverse).
In DES, both are similar.

Mix columns; $GF(2^8) = x^8+x^4+x^3+x+1$

100011011

prime polynomial

$(x+1)^{-1} \bmod x^8+x^4+x^3+x+1$

00000011

	q_i		
$x^8+x^4+x^3+x+1$		1	0
$x+1$	$x^7+x^6+x^5+x^4+x^2+x$	0	1
1		1	$x^7+x^6+x^5+x^4+x^2+x$

$x+1 \;\big|\; x^5+x^4+x^3+x+1$

x^5+x^4

x^3+x+1

x^3+x^2

x^2+x+1

x^2+x

1

$x+1 \;\big|\; x^8+x^4+x^3+x+1$

x^8+x^7

$x^7+x^4+x^3+x+1$

x^7+x^6

$x^6+x^4+x^3+x+1$

x^6+x^5

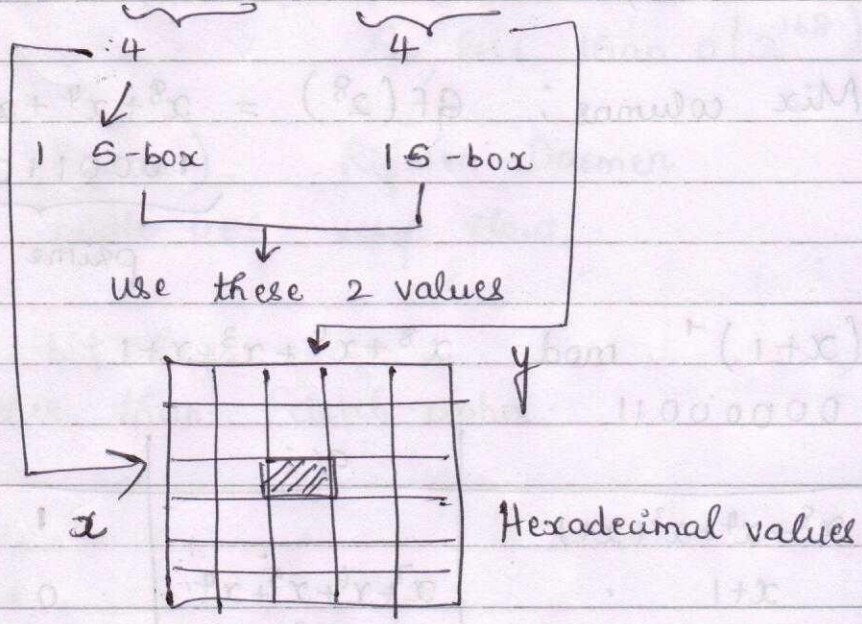
$x^5+x^4+x^3+x+1$

$x^7+x^6+x^5+x^4+x^2+x$

Totally 16 S-boxes (all are same)

Byte substitution – contains inverse (non-linear)

Suppose 0000 = 0 0011 = 3



Shift Rows :

First row is not shifted

Mix columns :

$$\begin{bmatrix} A \end{bmatrix} * \begin{bmatrix} B \end{bmatrix} = \begin{bmatrix} \text{Result} \end{bmatrix}$$

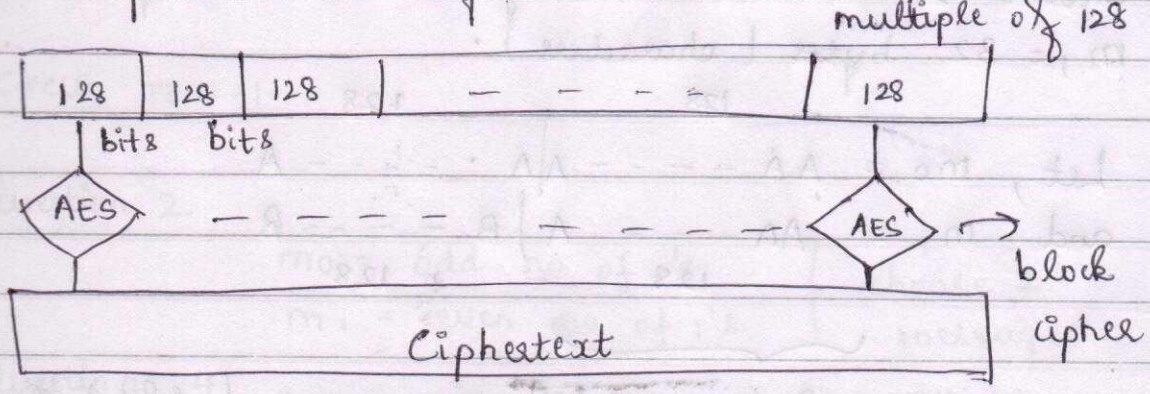
$$\mod\left(x^8+x^4+x^3+x+1\right)$$

AES Key Expansion

Key Whitening:
Encryption: XOR with subkeys.
To prevent attack from adversary.

Insecurity of ECB Mode: (Electronic Code Book)

To represent 2^{10} bytes



ECB mode: Used to encrypt very large messages

If 128-bits of first part & second part is same - then ciphertext for both will be same.
∴ Deterministic in nature - AES with ECB mode

∴ We need to introduce pseudo-randomness

Prove that AES is not semantically secure.
(ECB mode)

256 bits - message - 32-bytes

128 | 128

Choose 2 random messages m_0 = 32 bytes & m_1 = 32 bytes (characters).

Let, m_0 = AA---A | A---A (128 | 128)

and m_1 = AA---A | B---B (128 | 128)

m_0 & m_1 - 128 bits are same (left half)

∴ Can easily find

Bank A	Account A	Bank B	Account B	$ 100

ECB is used we can guess

10 times - transaction & intercept ciphertext

(1) Amount is same, bank is same
Attack possible

(2) Any transaction - change account or change amount

∴ Use randomized mode for security purposes, not ECB mode.

CYCLE TEST-1

Question 2

m_0 = odd no of 1's
m_1 = even no of 1's
} choose 2 messages

Question 4

$C = pq + m \quad m \in \{0,1\}$

$C_1 = pq_1$
$C_2 = pq_2$
} can ask twice

$GCD(q_1, q_2)$ - answer