

CS 304 (Theory)
Ph - 9474575596

Pre Midterm → 10 marks

Midterm → 10 marks + 10 marks

Pre Endterm → 15 marks

Endterm → 15 marks + 15 marks

Rem 25 marks = Attendance + Assignments
+ Class test

CS 364

All the Coding will be in C

Assignments → 3 or 4 (80 to 90 marks)

Continuous Assessment → 10 or 20 marks

- Cryptography → The part where we develop algorithms to get security / Designing the Algo
- Cryptanalysis → We try to break the security of designed algorithm

$$\underline{\text{Cryptology}} = \text{Cryptography} + \text{Cryptanalysis}$$

NIST → Standardizes cryptographic Algos.

$$\text{ATM } 1 \longrightarrow \text{PIN } 1 + X = Y_1 \rightarrow \text{write}$$

$$\text{ATM } 2 \longrightarrow \text{PIN } 2 + X = Y_2 \rightarrow \text{write}$$

$$\text{ATM } 3 \longrightarrow \text{PIN } 3 + X = Y_3 \rightarrow \text{write}$$

⋮ ⋮

$$\text{ATM } 10 \longrightarrow \text{PIN } 10 + X = Y_{10} \rightarrow \text{write}$$

X → Secret

↓
Secret Key

Crypto

| Symmetric Key
Crypto
||
One Secret
Key

| Public key
Crypto
||

| Two Keys
i) Public ✓
ii) Secret

■ Cryptography provides following Security Services :-

- i) Confidentiality ✓
- ii) Integrity ✓
- iii) Authentication ✓
- iv) Non-repudiation

i) Confidentiality (Secrecy)

Ensuring that no one can read the message except the intended receiver.

The original data can't be recovered without the proper credential even if the data is transferred via an insecure channel.

ii) Integrity (anti-tampering)

Assuring the receiver that the received message has not been altered in any way from the original.

iii) Authentication verification of one's identity.

iv) Non repudiation

A mechanism to prove that the sender really sent this message.

■ Confidentiality

i) Plaintext : \rightarrow original message

ii) Encryption Algorithm \rightarrow function

iii) Ciphertext \rightarrow un-readable form of plaintext

iv) Decryption Algorithm \rightarrow function

v) Encryption Key \rightarrow Key

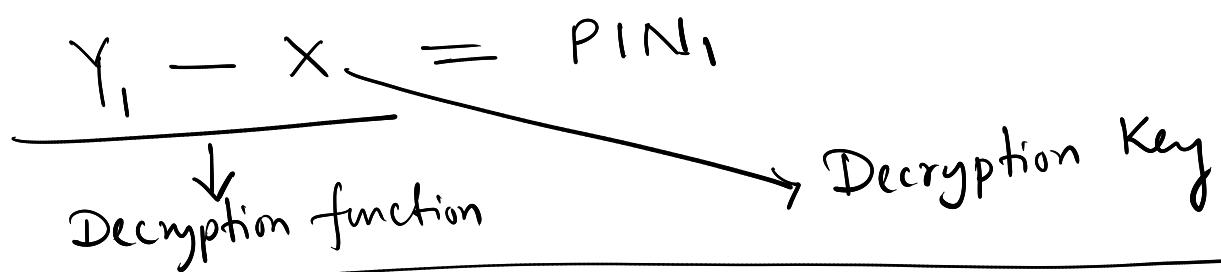
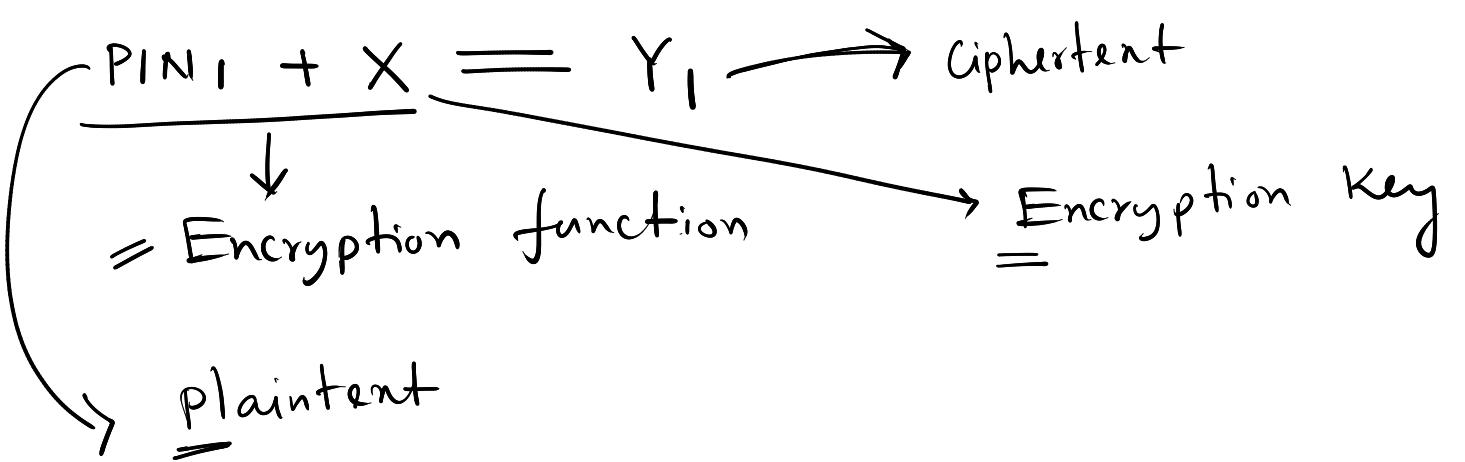
vi) Decryption Key \rightarrow Key

✓ Encryption function $(\overset{\text{Plaintext}}{M}, \overset{\text{Enc. Key}}{\underline{\text{Enc. Key}}}) = \underline{\text{Ciphertext}}$

Enc. func : $P \times \text{Enc. Key} \longrightarrow \text{Ciphertext}(c)$

✓ Decryption function $(\underline{\text{Ciphertext}}, \overset{\text{Dec. Key}}{\underline{\text{Dec. Key}}}) = \text{Plaintext} = M$

Dec. func : $C \times \text{Dec. Key} \longrightarrow P$



Cryptography

$\begin{aligned} & \dashv E \rightarrow \text{Encryption} \\ & \dashv D \rightarrow \text{Decryption} \end{aligned}$

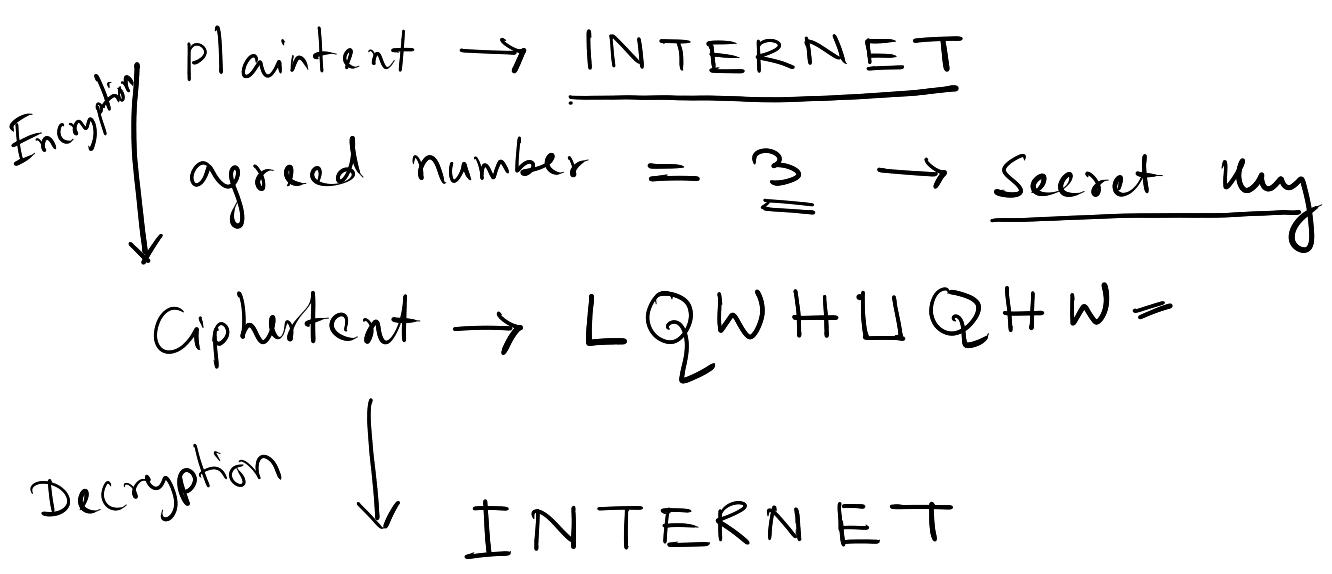
\downarrow
 Symmetric Key
 $E(M, K) = C$
 $D(C, K) = M$

\downarrow
 Public Key /
 Asymmetric Key
 $E(M, PK) = C$
 $D(C, SK) = M$
 $PK \neq SK$

CAESAR Cipher

This cipher is named after
Julius Caesar

It relies on shifting the letters of
 a message by an agreed number
 agreed number = 3



Function

$f: A \rightarrow B$ it is a relation
 between the elements of A and B
 with the property that if $a, b \in A$
 and $a = b$ then $f(a) = f(b)$

one to one function

$$f(a) = f(b) \Rightarrow a = b$$

onto function

$f: A \rightarrow B$
 then $\forall b \in B \exists a \in A$ s.t.
 $f(a) = b$

Bijective function

$f: A \rightarrow B$ is bijective function
 iff f is one to one and onto

Permutation

Let π be a permutation on a set S
 then $\pi: S \rightarrow S$ is a bijection from
 S to S

$$\pi: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

☒ One Way Function

$f: X \rightarrow Y$ is called a one way if given $x \in X$ it is easy to compute $f(x)$ but given $f(x)$ it is hard to find x .

Ex. P is a prime (large)
 q is a prime (large)] Given
 $N = P \times q \rightarrow$ this computation is easy
Given N find P, q s.t. $N = P \times q$
↓ ↓
large primes
is hard

☒ Substitution Box

$S: A \rightarrow B$ with $|B| \leq |A|$

$$S: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3\}$$

$$S(1) = 1 \quad S(2) = 3 \quad S(3) = 2 \\ S(4) = 1$$

Transposition Cipher

$M = m_1, m_2, \dots, m_t \rightarrow \text{Plaintext}$

ℓ : permutation on $\underbrace{\{1, 2, \dots, t\}}_{t \text{ elements}} \rightarrow \text{Secret Key}$

Encryption

$$C = m_{\ell(1)} m_{\ell(2)} \dots m_{\ell(t)} = c_1 c_2 \dots c_t$$

↙ Ciphertext

Decryption

$$M = c_{\ell^{-1}(1)} \dots \ell^{-1}(t)$$

Ex. Plaintext : CAESAR = m_1, m_2, \dots, m_6

Secret key ℓ :
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$
 Encryption

Ciphertext : RSCEAA = $c_1, c_2, c_3, \dots, c_6$

$d = \ell^{-1}$:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 5 & 1 \end{pmatrix}$$
 Decryption

Plaintext : CAESAR

□ Substitution Cipher

$$M = m_1 m_2 \dots m_L$$

$$\mathcal{A} = \{A, B, C, \dots, Z\}, m_i \in \mathcal{A}$$

e : Substitution from \mathcal{A} to \mathcal{A}
 $= e \rightarrow \text{Secret Key}$

Encryption $c = e(m_1) e(m_2) e(m_3) \dots e(m_L)$

~~Ex.~~ $e(A) = Z, e(B) = D, \dots e(C) = A$

ABC \rightarrow plaintext

ZDA \rightarrow ciphertext

□ Affine Cipher

$$\begin{array}{ccccccc} A & B & C & \dots & & Z \\ \downarrow & \downarrow & \downarrow & & & \downarrow \\ 0 & 1 & 2 & \dots & & 25 \end{array}$$

$\mathcal{A} \rightarrow$ set of alphabates

$$\mathcal{A} \longrightarrow \mathbb{Z}_{26}$$

$$K = \text{Secret Key} = (a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$$

Encryption function
 $e(x, K) = (a \cdot x + b) \bmod 26$
 $= c$

Decryption function

$$d(c, K) = ((c - b) \cdot a^{-1}) \bmod 26$$

■ Affine cipher

$$\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$$

$$\mathbb{Z}_{26}^* = \mathbb{Z}_{26} \setminus \{0\}$$

Secret key $K = (a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$

Plaintext $x \in \mathbb{Z}_{26}$

$$\boxed{\gcd(a, 26) = 1}$$

$$\text{Enc : } c = E(x, K) = (a \cdot x + b) \bmod 26$$

$$\text{Dec : } x = D(c, K) = (c - b) \cdot a^{-1} \bmod 26$$

$$\blacksquare \quad \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \quad x, y \in \mathbb{Z}_6$$

$$+ \bmod 6 : +_6 \xrightarrow{z = (x+y) \% 6}$$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

0 : additive identity

$$(x+y)\%6 = 0$$

Every element of \mathbb{Z}_6 with $+_6$ has an additive inverse

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ multiplication modulo 6

$$x, y \in \mathbb{Z}_6 \quad x *_6 y = \mathbb{Z} \% 6 = y = x *_6 y$$

$*_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1: is the multiplicative identity

$$(x * y) \% 6 = 1$$

$1, 2, 3, 4, 5$

$$0 \neq x \in \mathbb{Z}_6 \quad \text{if } \gcd(x, 6) = 1$$

then $\exists y$ s.t.

$$x *_6 y = 1$$

$$0 \neq x \in \mathbb{Z}_m \quad \cdot \quad \gcd(x, m) = 1$$

$$\Leftrightarrow x *_m y = 1$$

$$x * y \equiv 1 \pmod{m}$$

$$\Rightarrow m \mid (xy - 1)$$

$$\Rightarrow xy - 1 = t \cdot m$$

$$\Rightarrow 1 = t_1 m + x y$$

$$\Rightarrow \gcd(a, m) = t_1 m + a'y$$

To find (t_1, y) we have follow
Extended Euclidean Algorithm

□ \mathbb{Z}_m^* $a \in \mathbb{Z}_m^*$ $*_m$

Read a will be invertible iff $\gcd(a, m) = 1$

$\phi(m)$: Euler phi function

$$\rightarrow \# x, 0 < x \leq m-1 \\ \text{s.t. } \gcd(x, m) = 1$$

□ Playfair Cipher $I = J$

Secret key = Playfair example

P L A Y F

Plaintext : HIDE

* I R E X M *

H I D E

* B C D G H *

↓ ↓

K N O Q S

B M O D

T U V W Z

Ciphertext : BMOD

SACHIN

CSEX

msg \rightarrow CSE \rightarrow CSEX (odd length)

MSG → BALL

BA LX LX

Add extra X to make the msg of even length

Add extra X in between two repeated letter

- I) If both letters are the same (or only one letter is left) add an 'x' after the first (last) letter. Encrypt the new pair and continue.
- II) If the letters appear on the same row of your table, replace them with the letter to their immediate right respectively
- III) If the letters appear on the same column of your table, then replace them with the letters immediately below respectively
- IV) If the letters are not in the same row or column, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important — the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair

Hill Cipher

$A = (a_{ij})_{n \times n}$ \rightarrow invertible matrix
Secret Key

$M = (m_1, m_2, \dots, m_n)$ \rightarrow Plaintext

Encryption

$$C = \underline{A \cdot M} = \underline{(c_1, \dots, c_n)}$$

Decryption

$$M = A^{-1} \cdot C$$



$$S : \{A, \dots, Z\} \rightarrow \{A, \dots, Z\}$$

$$P \rightarrow C = S(P) \quad C \rightarrow \text{Known}$$

Secret Key

$$\# S = 26 \stackrel{26}{\approx} 2^{122}$$

Brute force attack / Exhaustive Search

Kerchoff's Rule

Design has to be public

Shanon's notion of perfect Secrecy

$E \rightarrow$ Encryption algo

$M \rightarrow$ Message

$C \rightarrow$ Ciphertext

$$E(M) = C$$

going via
public channel

E will be providing perfect secrecy
iff the ciphertext does not
reveal any information regarding the
plaintext/message

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

$$\Pr[\text{message} \mid \text{ciphertext}] = \Pr[\text{message}]$$

OTP

Symmetric Key Cipher

Block cipher

Stream cipher

Block cipher

$$M = m_0 \parallel m_1 \parallel m_2 \parallel \dots \parallel m_n$$

↓ ↓ ↓
Block Block Block

$$\text{length of } m_i = l$$

Enc → it can encrypt l length message
We can do the encryption on M
using Enc blockwise

In block cipher encryption is
done blockwise

Ex. $M = \underline{m_0} \parallel \underline{m_1} \parallel \dots \parallel \underline{m_e}$

Encryption $C = \underline{\text{Enc}(m_0, K)} \parallel \underline{\text{Enc}(m_1, K)} \parallel \dots \parallel \underline{\text{Enc}(m_e, K)}$

$$C = \underline{c_0} \parallel \underline{c_1} \parallel \dots \parallel \underline{c_e}$$

Decryption

$$M = \frac{\text{Dec}(c_0, K) \parallel \text{Dec}(c_1, K) \parallel \dots}{\parallel \text{Dec}(c_L, K)}$$

Stream cipher

$$M = m_0 \dots m_\ell$$

$$\text{where } m_i \in \{0, 1\}$$

Encryption \rightarrow It will be performed bit wise

$$C = (m_0 \oplus z_0, m_1 \oplus z_1, \dots, m_\ell \oplus z_\ell)$$

$m = c_0 \oplus z_0, c_1 \oplus z_1, \dots, c_\ell \oplus z_\ell$

Product cipher

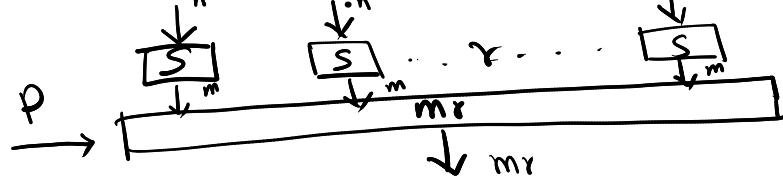
A product cipher Combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual transformation.

Substitution Permutation Network (SPN)

It is a product cipher based Substitution box and permutation box.

ex.

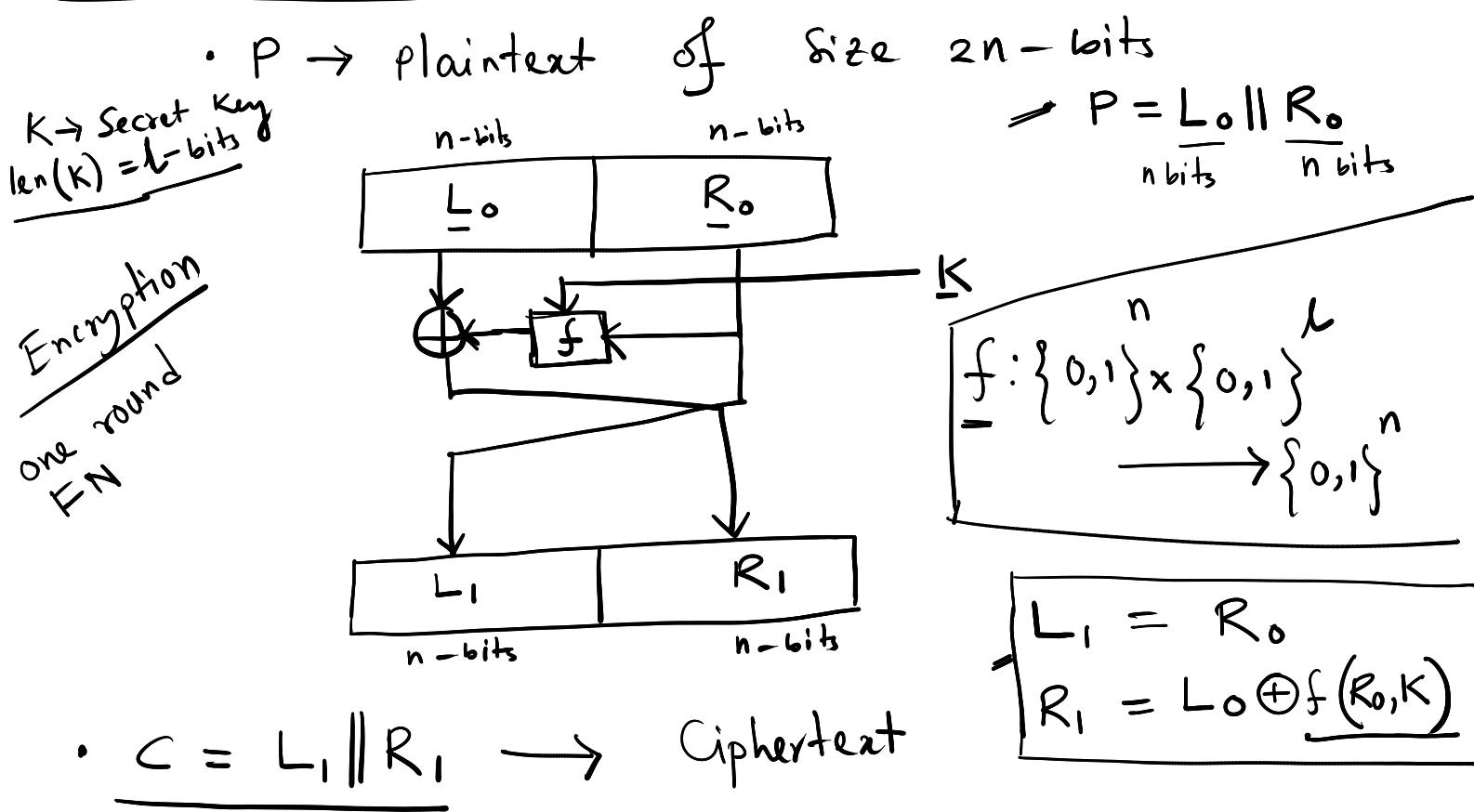
$$S: \{0, 1\}^n \rightarrow \{0, 1\}^m, P: \{0, \dots, m_r-1\} \rightarrow \{0, \dots, m_r-1\}$$



$$\text{len(input)} = nr$$

Feistel Network (FN)

Feistel Network (FN)

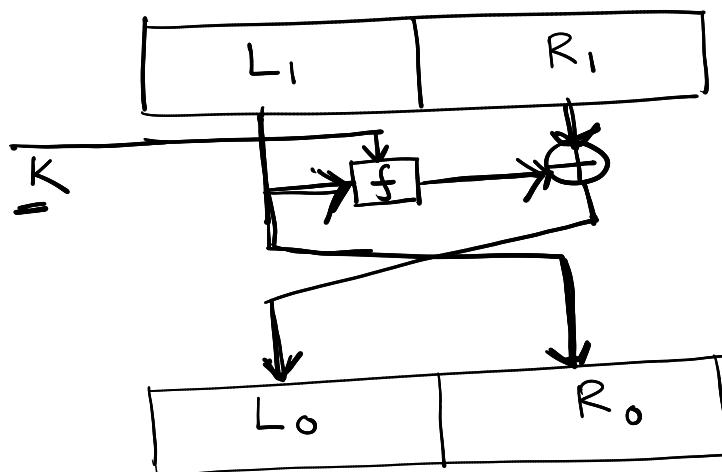


Decryption

$$- R_0 = L_1$$

$$- L_0 = R_1 \oplus f(L_1, K)$$

$$\underline{f(L_1, K) = f(R_0, K)}$$



Inversion of f is not required.

- i) Data Encryption Standard (DES)
 - is based on Feistel Network (FN)

- ii) Advanced Encryption Standard (AES)
 - is based on SPN

□ Iterated block cipher

An Iterated block cipher is block cipher involving the sequential repetition of an internal function (called as Round function).

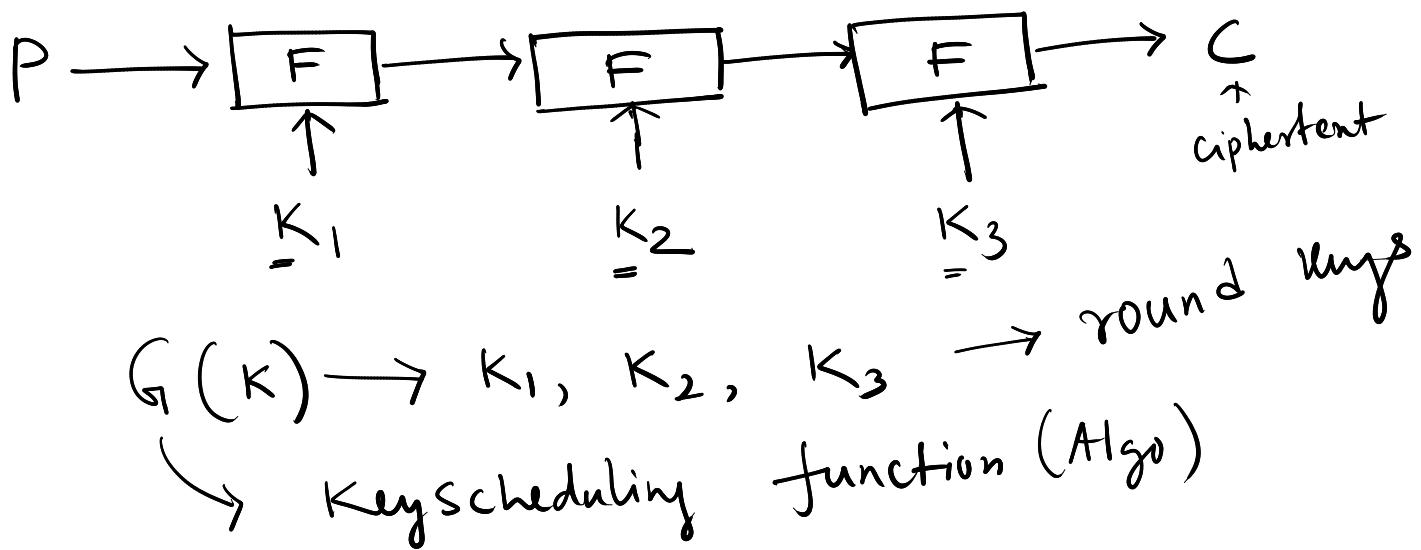
The parameters include the number of rounds r, the block size n, and the round keys K_i of length l generated from the original secret key K .

F → round function

P → plaintext block

K → Secret key

3-round block cipher



◻ OTP (one time padding)

OTP provides perfect secrecy under some conditions.

Encryption

$P \rightarrow \text{Plaintext}$

 bitwise
xor

$K \rightarrow \text{Secret Key}$

$$\textcircled{1} \quad \text{Enc}(P, K) = \underline{P \oplus K} = C$$

Decryption

$$\textcircled{2} \quad \text{Dec}(C, K) = C \oplus K = P$$

$$\bullet \Pr[\text{message} \mid \text{Ciphertext}] = \Pr[\text{message}]$$

Conditions

- I) The Secret key K Cannot be used to encrypt two messages
- II) length(K) \geqslant length(P)
- III) K is uniformly selected from the key space

OTP on one bit enc

message $\leftarrow m \in \{0, 1\}$, $\overset{\text{key}}{\leftarrow} K \in \{0, 1\}$

- $\Pr[m = 0] = p$ • $\Pr[K = 0] = \frac{1}{2}$
- $\Pr[m = 1] = (1 - p)$ • $\Pr[K = 1] = \frac{1}{2}$

Encryption

$$C = m \oplus K$$

$$\begin{aligned}\Pr[C = 0] &= \Pr[m = 0, K = 0] + \Pr[m = 1, K = 1] \\ &= \Pr[m = 0] \cdot \Pr[K = 0] \\ &\quad + \Pr[m = 1] \cdot \Pr[K = 1] \\ &= \left(p \times \frac{1}{2}\right) + \left(1 - p\right) \times \frac{1}{2} \\ &= \frac{1}{2}\end{aligned}$$

Similarly

$$\Pr[C = 1] = \frac{1}{2}$$

$$\Pr[M = m | C = c] \stackrel{?}{=} \Pr[M = m]$$

i) $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$
ii) $\Pr(A \cap B) = \Pr(B|A) \cdot \Pr(A)$

$$\Pr[M = 0 | C = 0] = \frac{\Pr[M = 0, C = 0]}{\Pr[C = 0]}$$

$$= \frac{\Pr[C = 0 | M = 0] \times \Pr[M = 0]}{\frac{1}{2}}$$

$$= \frac{\Pr[K = 0] \times \Pr[M = 0]}{\frac{1}{2}}$$

$$= \frac{\frac{1}{2} \times \Pr[M = 0]}{\frac{1}{2}}$$

$$= \Pr[M = 0]$$

$$\Pr[M = 0 | C = 0] = \Pr[M = 0]$$

Thus it provides perfect Secrecy

Conditions

$$\text{i) } M_1 \oplus K = C_1$$

$$M_2 \oplus K = C_2$$

} this will reveal information on messages.

$$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$$

$$= M_1 \oplus M_2$$

Ciphertexts difference will give you message difference

$$\text{ii) } \text{len}(K) < \text{len}(P)$$

$$C = P \oplus K$$

$$P = P_1 \dots P_l \quad P_n$$

$$\begin{array}{c} \oplus \\ \text{iii) } K = K_1 \dots K_l \underline{K_{l+1} \dots K_t} \\ \hline C = \frac{(P_1 \oplus K_1)}{c_1} \frac{(P_2 \oplus K_2)}{\dots} \frac{(P_l \oplus K_l)}{\dots} \frac{(P_{l+1} \oplus K_1)}{(P_n \oplus K_t)} \end{array}$$

$$\underline{C_1 \oplus C_{l+1}} = P_1 \oplus P_{l+1}$$

$$\# \quad \text{len}(K) \geq \text{len}(P)$$

* OTP is not usable in
real life

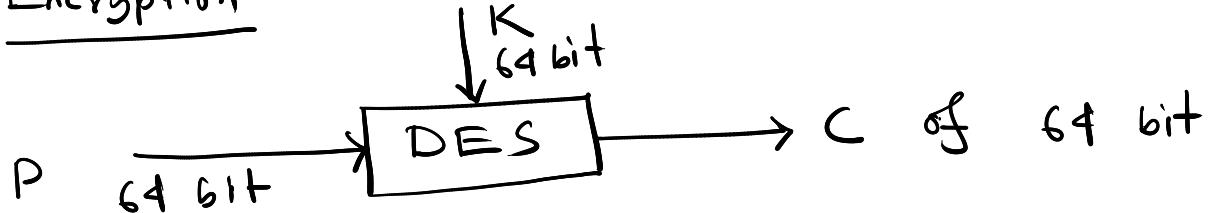
- ◻ OTP is not usable in daily life
- i) Secret key cannot be reusable.
Only one message can be encrypted using the key
- ii) $\text{length}(\text{Key}) \geq \text{length}(\text{message})$

Due to ①, ② OTP is not practical.

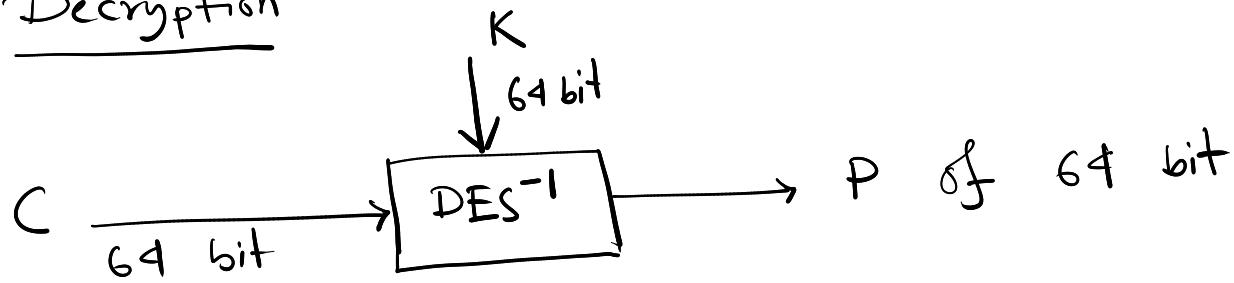
◻ Data Encryption Standard (DES)

- It is a block cipher
- Designed by IBM
- i) Block size = 64 bit
- ii) Number of rounds = 16
- iii) Secret key size = 64 bit with 8 parity check bits.
- iv) It is based on Feistel Network

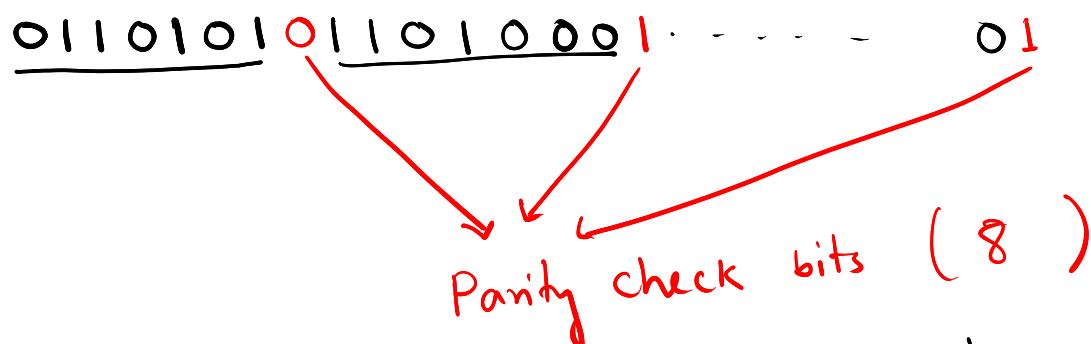
Encryption



Decryption



- ④ Secret Key is 64 bit with 8 parity check bits



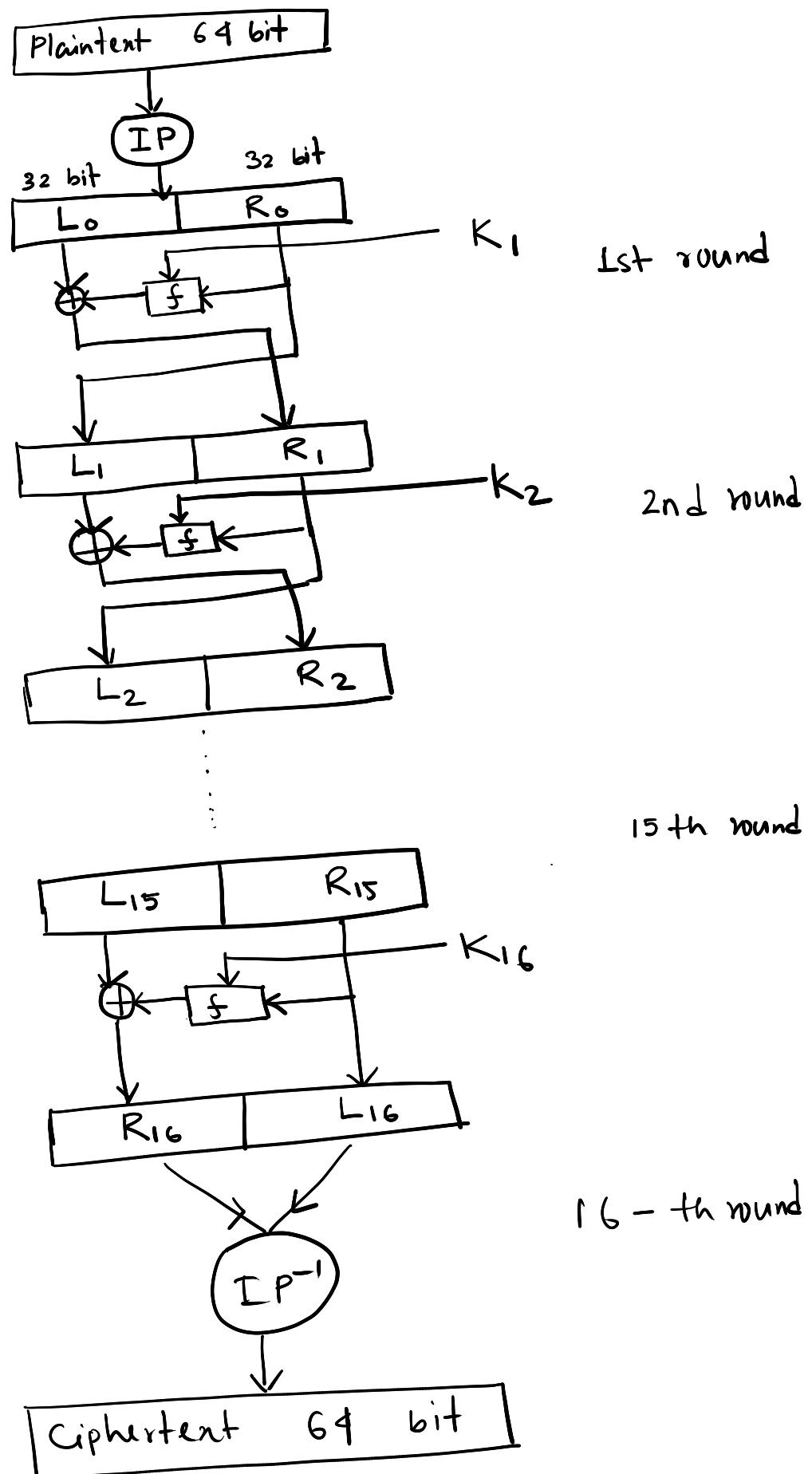
After discarding 8 parity check bits
 → the final secret key will be of 56 bit
 DES should provide 56 bit security

- ④ In DES we have 16 round keys K_1, K_2, \dots, K_{16} which are generated using key scheduling algorithm
 Key scheduling algo will take the secret key as an input

$$\text{length}(K_i) = 48 \text{ bits}$$

Structure of DES

Encryption



$$L_{i+1} = R_i \quad i=0, \dots, 15$$

$$R_{i+1} = L_i \oplus f(R_i, K_{i+1})$$

Think about Decryption

- We have to learn the followings
- I) IP, IP^{-1} ✓
 - II) what is f ? (round function)
 - III) How K_1, \dots, K_{16} (round keys)
are generated?

■ IP (Initial permutation)

$$IP : \{0,1\}^{64} \longrightarrow \{0,1\}^{64}$$

Handbook (PP - 253)

$$\begin{matrix} & 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ IP : & 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ & 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \end{matrix}$$

:

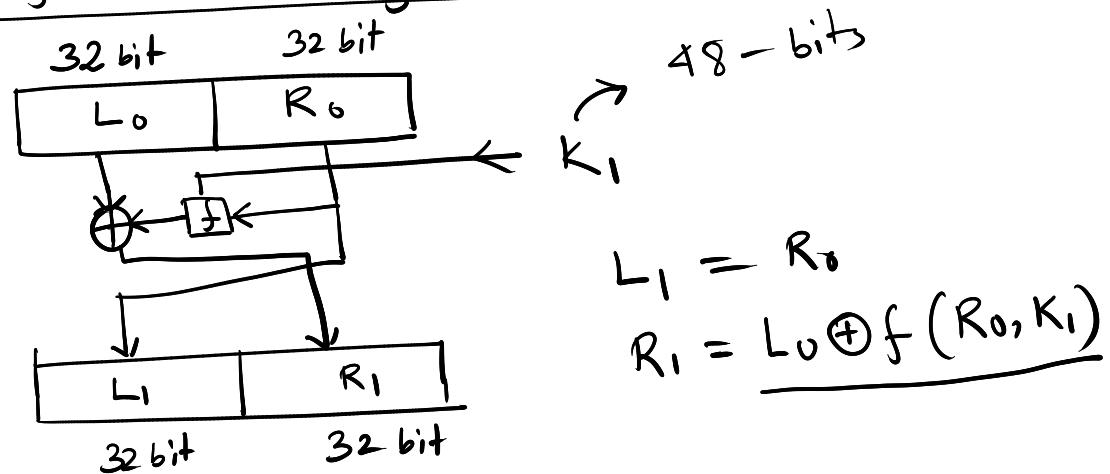
$$\begin{matrix} & 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{matrix}$$

$$IP(m_1, m_2, \dots, m_{64})$$

$$= (m_{58} \ m_{50} \ m_{42} \ m_{34} \ m_{26} \ \dots \ m_2 \ m_{60} \ m_{52} \ \dots \ m_4 \ \dots \ m_{63} \ m_{55} \ m_{47} \ \dots \ m_7)$$

$$IP^{-1}$$

Round function of DES



$$f: \{0,1\}^{32} \times \{0,1\}^{48} \rightarrow \{0,1\}^{32}$$

$$f(R_i, K_i) = X_i$$

where R_i is 32 bit

K_i is 48 bit

X_i is 32 bit

$$f(R_i, K_i) = P(S(E(R_i) \oplus K_i))$$

✓ $E: \{0,1\}^{32} \rightarrow \{0,1\}^{48}$ (Expansion function)

✓ $S: \{0,1\}^{48} \rightarrow \{0,1\}^{32}$ (Substitution box)

✓ $P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ (Permutation box)

$$\boxed{\square} E : \{0,1\}^{32} \longrightarrow \{0,1\}^{48}$$

$$E(x_1, x_2, \dots, x_{32}) = (y_1, \dots, y_{48})$$

E :	32	1	2	3	4 5
	4	5	6	7	8 9
	8	9	10	11	12 13
	12	13	14	15	16 17
	16	17	18	19	20 21
	20	21	22	23	24 25
	24	25	26	27	28 29
	28	29	30	31	32 1

Handbook \rightarrow PP 253

$$\begin{aligned} E(x_1, \dots, x_{32}) &= (x_{32} x_1 x_2 x_3 x_4 x_5 \\ &\quad x_6 x_7 x_8 x_9 x_9 \\ &\quad x_8 x_9 x_{10} x_{11} x_{12} x_3 \\ &\quad x_{12} x_{13} x_{14} x_{15} x_{16} x_{17} \\ &\quad x_{16} x_7 x_8 x_9 x_{20} x_{21} \\ &\quad x_{20} x_{21} x_{22} x_{23} x_{24} x_{25} \\ &\quad x_{24} x_{25} x_{26} x_{27} x_{28} x_{29} \\ &\quad x_{28} x_{29} x_{30} x_{31} x_{32} x_1) \end{aligned}$$

$$\boxed{\square} S : \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$$

$$S(X) = Y \quad \text{where } X \text{ is 48 bit} \\ Y \text{ is 32 bit}$$

- $X = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$

Where length of B_i is 6-bit

- $S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$

$$S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4 \quad \forall i = 1, 2, \dots, 8$$

$$S_i(B_i) = C_i$$

\downarrow
 6 bit \downarrow
 4 bit

$$S(x) = \left(\underline{S_1(B_1)}, \underline{S_2(B_2)}, \underline{S_3(B_3)}, \underline{S_4(B_4)} \right. \\ \left. \underline{S_5(B_5)}, \underline{S_6(B_6)}, \underline{S_7(B_7)}, \underline{S_8(B_8)} \right)$$

$S(x) \rightarrow 32 \text{ bit}$

$$S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$$

Handbook
→ PP 253

$$S_i(B_i) = c_i$$

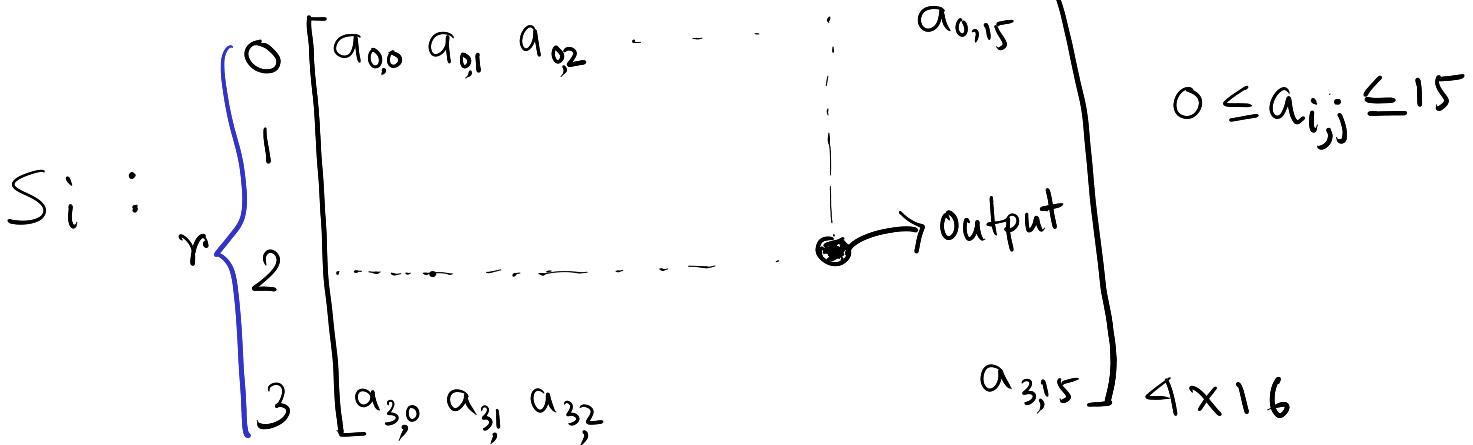
- $B_i = \underline{b_1} \underline{b_2} \underline{b_3} \underline{b_4} \underline{b_5} \underline{b_6} \quad b_i \in \{0, 1\}$

- $r = (2 \times b_1 + b_6) \quad 0 \leq r \leq 3$

r is the integer representation of $(b_1 b_6)$

- $c = \underbrace{\text{Integer representation of } (b_2 b_3 b_4 b_5)}_{4} \quad 0 \leq c \leq 15$

$$0 \quad 1 \quad 2 \quad 3 \quad \dots \quad 12 \quad \dots \quad 15$$



$r \rightarrow \text{row number}$

$c \rightarrow \text{column number}$

$$S_i(B_i) = a_{r,c} \rightarrow 4 \text{ bit}$$

Handbook
→ PP 260



Permutation P

$$P : \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$

	16	7	20	21
P :	29	12	28	17
	1	15	23	26
	5	18	31	10
	2	8	29	14
	32	27	3	9
	19	13	30	6
	22	11	4	25

$$\begin{aligned} & P(x_1, x_2, \dots, x_{32}) \\ &= (x_{16}, x_7, x_{20}, x_{21}, \\ & x_{29}, x_{12}, x_{28}, x_{17}, x_1, \\ & x_{15}, x_{23}, x_{26}, x_5, x_{18}, \\ & x_{31}, x_{10}, x_2, x_8, x_{24}, \\ & x_4, x_{32}, x_{27}, x_3, x_9, \\ & x_9, x_3, x_{30}, x_6, x_{22}, \\ & x_{11}, x_4, x_{25}) \end{aligned}$$

■ We have to understand Key Scheduling algorithm of DES

DES

- ✓ i) 16 rounds
 - ✓ ii) 64-bit block size
 - ✓ iii) Key size = 64 bit
 - ✓ iv) IP and IP^{-1}
 - ✓ v) Round function
 - ✓ vi) Key scheduling Algo
-

Key Scheduling Algo of DES

Input: 64 bit key K

Output: 16 round key K_i , $1 \leq i \leq 16$
where length of K_i is 48 bit

- i) Define $v_i, 1 \leq i \leq 16$, where $v_i = 1$
 $\text{if } i \in \{1, 2, 9, 16\} \text{ else } v_i = 2$
- ii) Discard 8 parity check bit from K .
The 56 bit key is \tilde{K} .
- iii) $T = PC_1(\tilde{K})$; $PC_1 : \{0,1\}^{56} \rightarrow \{0,1\}^{56}$
- iv) $(C_0, D_0) = T$ where C_0 is of 28 bit
 D_0 is of 28 bit
- v) for $i = 1$ to 16
 $C_i = (C_{i-1} \leftarrow v_i)$
 $D_i = (D_{i-1} \leftarrow v_i)$

\leftarrow left circular shift +
 $(x_1, x_2, \dots, x_{28}) \leftrightarrow 2$
 $= (x_3, x_4, \dots, x_{28}, x_1, x_2)$

$$K_i = PC2(C_i, D_i)$$

$$PC2 : \{0,1\}^{56} \rightarrow \{0,1\}^{48}$$

vi) Round keys = $(K_1, K_2, \dots, K_{16})$

\square $PC1 : \{0,1\}^{56} \rightarrow \{0,1\}^{56}$ Handbook → PP 256

$$PC1 : \begin{array}{|c|ccccccccccccc|} \hline C_i & 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ \hline 1 & 58 & 50 & 42 & 34 & 26 & 18 & \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 & \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 & \\ \hline \end{array}$$

$$D_i \begin{array}{|c|ccccccccccccc|} \hline & 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ \hline 7 & 62 & 54 & 46 & 38 & 30 & 22 & \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 & \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 & \\ \hline \end{array}$$

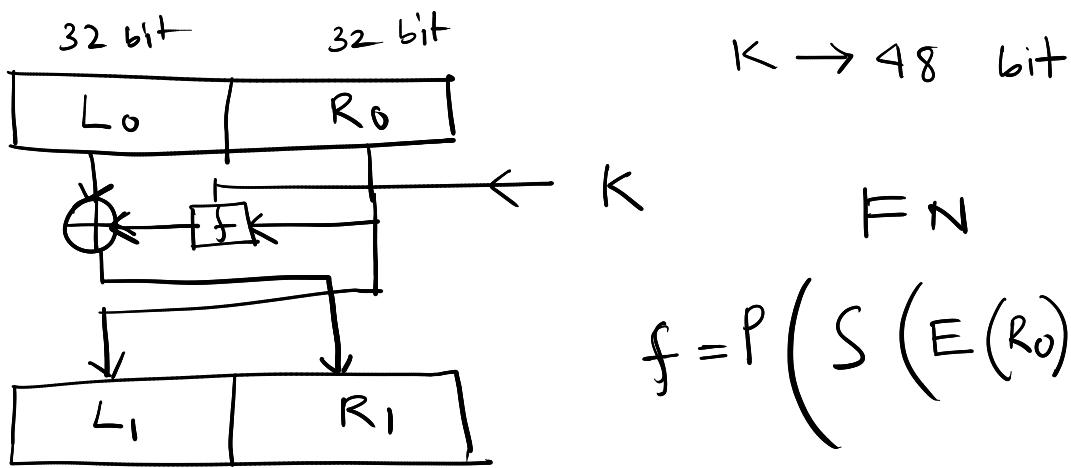
$$PC1(K_1, K_2, \dots, K_7, K_9, \dots, K_{63})$$

$$= (K_{57}, K_{49}, K_{41}, K_{33}, \dots, K_9, K_1, K_{58}, \dots, K_{36}, K_{63}, K_{55}, \dots, K_4)$$

$$PC2 : \begin{array}{ccccccc} & 19 & 17 & \dots & & 5 \\ & 3 & 28 & \dots & & 10 \\ & \vdots & & \ddots & & \vdots \\ \end{array}$$

8×6

$$46 \quad 42 \quad - \quad 32$$



$$M = L_0 \parallel R_0$$

$$C_1 = L_1 \parallel R_1$$

$$F_N(M, K) = C_1$$

$$F_N(\bar{M}, \bar{K}) = C_2$$

\bar{x} : bitwise complement of x

$$x = (x_1, \dots, x_{32})$$

$$\bar{x} = (1 \oplus x_1, \dots, 1 \oplus x_{32})$$

What will be the relation between C_1 and C_2 ?

$$L = R_0$$

$$R_1 = L_0 \oplus f(R_0, K)$$

$$\begin{aligned} \bar{K} \oplus E(\bar{R}_0) &= \overline{E(R_0) \oplus \bar{K}} \\ &= E(R_0) \oplus K \end{aligned}$$

$$P(S(\bar{K} \oplus E(\bar{R}_0))) = P(S(E(R_0) \oplus K))$$

$$M, \quad K$$

$$L_0 \parallel R_0 = M$$

$$L_1 = R_0$$

$$R_1 = L_0 \oplus f(R_0, K)$$

$$\boxed{f(R_0, K) \\ = f(\bar{R}_0, \bar{K})}$$

$$\bar{M}, \quad \bar{K}$$

$$\bar{L}_0 \parallel \bar{R}_0 = \bar{M}$$

$$\bar{L}_1 = \bar{R}_0 = \bar{L}_1$$

$$\bar{R}_1 = \bar{L}_0 \oplus f(\bar{R}_0, \bar{K})$$

$$= \bar{L}_0 \oplus f(R_0, K)$$

$$= \left(L_0 \oplus f(R_0, K) \right)$$

$$= \bar{R}_1$$

$$\bar{L}_1 \parallel \bar{R}_1 = \bar{L}_1 \parallel \bar{R}_1$$

$$C_2 = \bar{C}_1$$

■ $(b_1, b_2, \dots, b_{56})$

PC2 $(b_1, b_2, \dots, b_{56})$

$$= \left(\begin{array}{cccccccccc} b_{14} & b_{17} & b_{11} & b_{24} & b_1 & b_5 & b_3 & b_{28} & \dots & b_{10} & b_{23} & \dots & b_8 \\ \hline b_{16} & \dots & b_2 & b_{91} & \dots & b_{55} & b_{30} & \dots & b_{48} & b_{49} & \dots & b_{53} \\ \hline b_{96} & \dots & b_{32} \end{array} \right) \rightarrow 48 \text{ bits}$$

■ Attack models

1) Ciphertext only Attack

Attacker Knows only Ciphertexts

goal :- Recover the plaintexts Corresponding to the ciphertexts or recover the Secret key

2) Known plaintext Attack

Attacker Knows some plaintexts and Corresponding ciphertexts.

goal :- generate new plaintext, ciphertext pair or recover the secret key

3) Chosen Plaintext Attack

Attacker chooses plaintexts according to his/her choice and (s)he will be provided the corresponding ciphertexts.

goal :- generate new plaintext, ciphertext pair or recover the secret key

4) Chosen Ciphertext Attack

Attacker chooses some ciphertext and he/she is allowed to get the corresponding plaintexts

goal: Generate a new plaintext and ciphertext pair or recover the secret key

□ $\text{DES}(M, K) = C$

$$\text{DES}(\overline{M}, \overline{K}) = \overline{C}$$

Key = 56 bit
Brute force attack / Exhaustive search
 $= 2^{56}$

\Rightarrow Attacker chooses two plaintexts

i) M ii) \overline{M}

challenge is to find the key K

$$C_1 = \text{DES}(M, K)$$

CPA
chosen
plaintext
attack

$$C_2 = \text{DES}(\overline{M}, K)$$

Attacker is getting C_1 and C_2

$$\text{DES}(\overline{M}, \overline{K}) = \overline{C}_2$$

$$\Rightarrow \text{DES}(M, \overline{K}) = \overline{C}_2$$

$$\text{Keys} = \{K_1, K_2, \dots, K_{2^{56}}\}$$

Attacker selects $K_1 \in \text{Keys}$

He knows that $\bar{K}_1 \in \text{Keys}$

Attacker performs $\text{DES}(M, K_1) = \tilde{C}$

if $\tilde{C} \neq C_1$ or $\tilde{C} \neq \bar{C}_2$

then discard K_1, \bar{K}_1 (why?)



If $\tilde{C} \neq C_1 \Rightarrow K_1 \neq K$

If $\tilde{C} \neq \bar{C}_2 \Rightarrow K_1 \neq \bar{K} \Rightarrow \bar{K}_1 \neq K$

In every search the attacker is able to discard two keys from the list

$$\frac{2^{56}}{2} = 2^{55} \rightarrow \text{Complexity for finding the key } K.$$

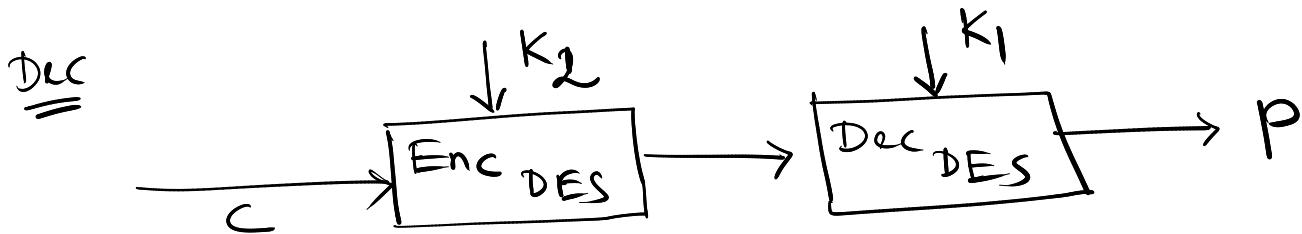
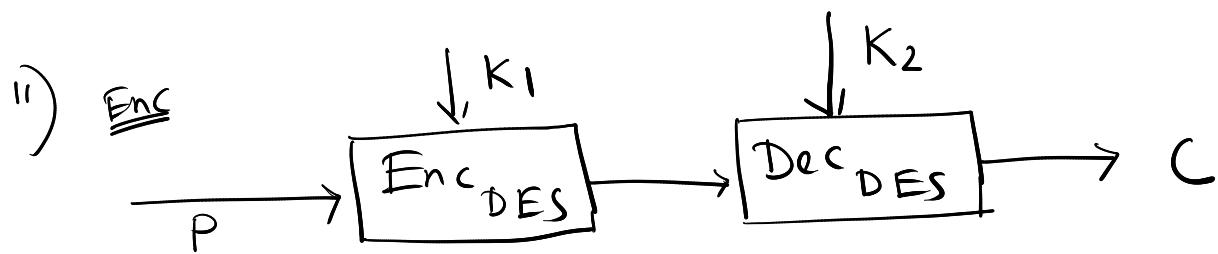
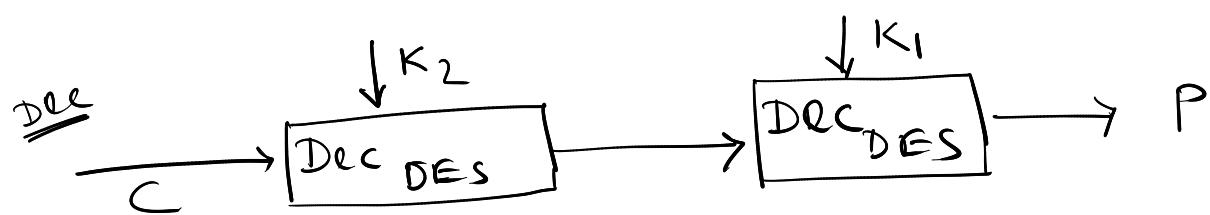
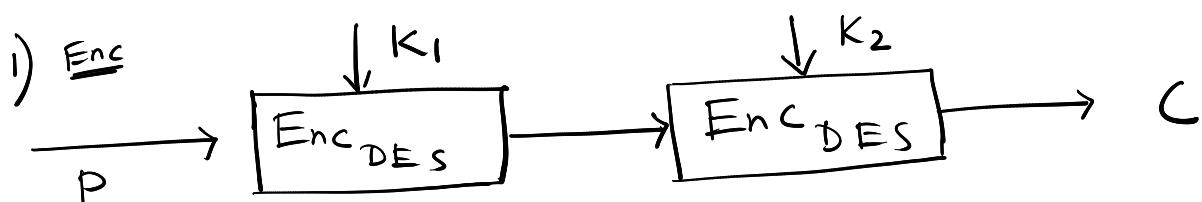
☒ DES → is not secure due to multiple attacks

☒ Increase the length of the Secret Key

☒ Double Encryption

$$K = K_1 \parallel K_2$$

length of $K_1 = 56$ bit
n a $K_2 = 56$ bit] $\Rightarrow \text{len}(K) = 112$ bit



- EE, ED, DE, DD

$$\square \quad K = K_1 \parallel K_2$$

Attacker Knows Plaintext M and the corresponding ciphertext C

$$C = \text{Enc} \left(\text{Enc}(M, K_1), K_2 \right)$$

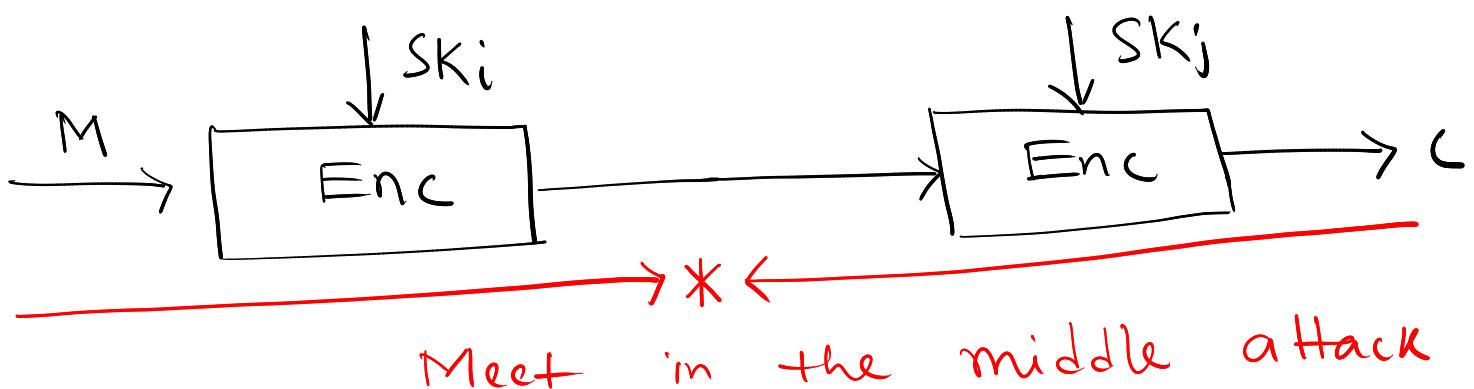
$$\text{Keys} = \{SK_1, \dots, SK_{2^{56}}\}$$

$$\text{Enc}(M, SK_i) = X_i$$

$$\text{Dec}(C, SK_j) = Y_j$$

If $X_i = Y_j$ for some i, j

then the key is $SK_i \parallel SK_j$



$$X_i$$

$$2^{56}$$

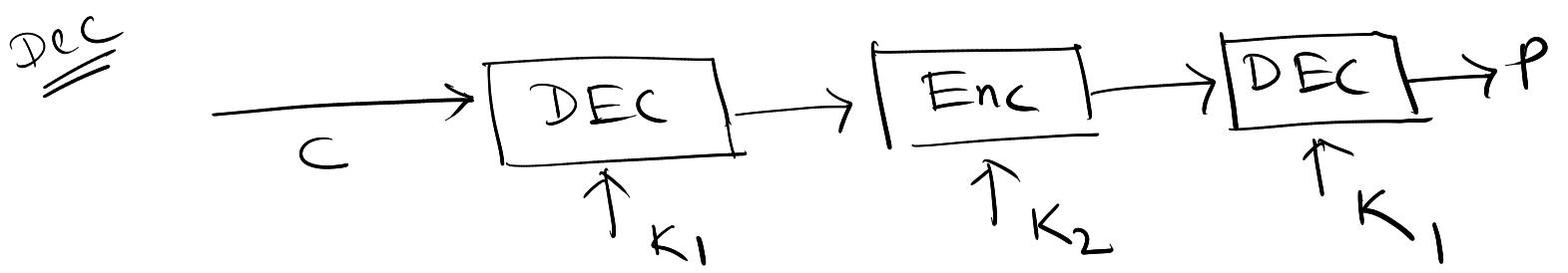
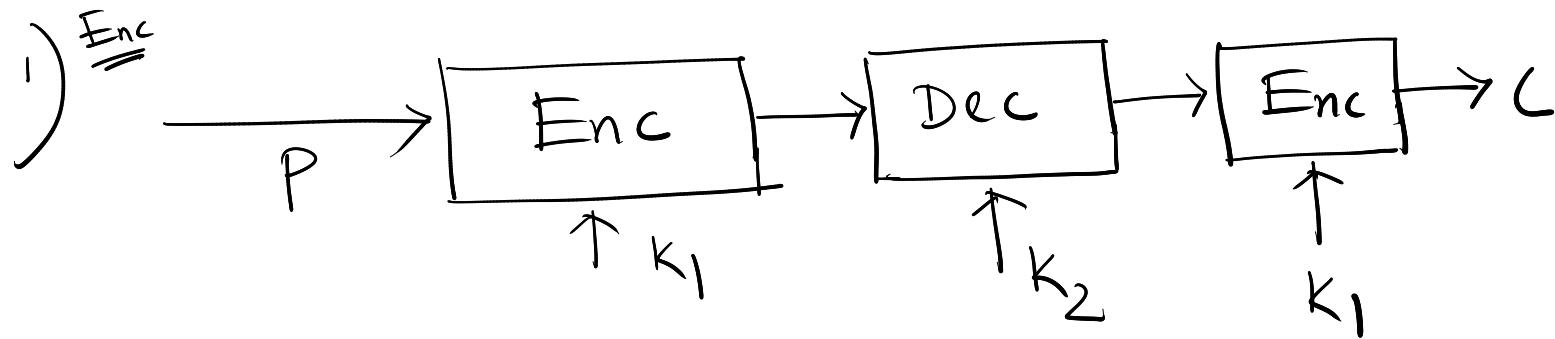
$$Y_j$$

$$2^{56}$$

■ Triple Encryption

$$K = K_1 \parallel K_2$$

$2n$ -bit security



■ EEE, EDE, DED ---

■ If DES is used in Triple encryption Setup then it is known as Triple DES (3-DES)

■ Advanced Encryption Standard (AES)

→ We have to understand Certain Mathematical results

■ A binary operation $*$ on a set S is a mapping from $\underline{S \times S}$ to \underline{S} . That is $*$ is a rule which assigns to each ordered pair of elements from S to an element of S

$$*: S \times S \longrightarrow S$$

$$*(a, b) = c, \quad a, b, c \in S$$

$$*(b, a) = d \quad d \in C$$

it is not necessary that $d = c$

Group

A group $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following axioms

1) $*$ is associative on G

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$$

2) There is an element $e \in G$ called the identity element such that

$$\underline{a * e} = \underline{a} = \underline{e * a} \quad \forall a \in G$$

3) For each $a \in G$ there exists an element $a^{-1} \in G$ called the inverse of a s.t. $a * a^{-1} = e = a^{-1} * a \quad \forall a \in G$

• A group G is called abelian
(or commutative) if

$$a * b = b * a \quad \forall a, b \in G$$

Ex. $*$: matrix multiplication over
square matrices of order $n \times n$

M : set of $n \times n$ matrices over \mathbb{R}

$(M, *) \rightarrow$ is it a Group? (No)

a) $*$ is associative

$$A * (B * C) = (A * B) * C$$

b) $A * I_n = A = I_n * A$

c) $\forall A \in M \exists A^T \in M$ s.t

$$A * A^T = I_n = A^T * A$$

$M = \left\{ \begin{array}{l} \text{Set of all invertible } n \times n \\ \text{matrix} \end{array} \right\}$

$(M, *) \rightarrow$ Groups

$(M, *) \rightarrow$ Commutative?

$A * B \neq B * A$
not commutative group

Ex. \mathbb{Z} : Set of all integers
 $(\mathbb{Z}, +) \rightarrow$ Group?
— yes

i) $a + (b + c) = (a + b) + c$

ii) $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$

iii) $\forall a \in \mathbb{Z} \quad \exists -a \in \mathbb{Z}$

B.t. $a + (-a) = 0 = (-a) + a$

Ex. $(\mathbb{Z}, \times) \rightarrow$ not a group

i) $a \times (b \times c) = (a \times b) \times c$

ii) $a \times 1 = a = 1 \times a$

iii) $a \in \mathbb{Z} \nexists a^{-1} \in \mathbb{Z}$

Ex. \mathbb{Q} : Set of all rational numbers

$(\mathbb{Q}, \times) \rightarrow$ not group

$(\mathbb{Q} \setminus \{0\}, \times) \rightarrow$ group.

□ If $|G|$ is finite then
 $(G, *)$ is a finite group.

$|G|$: Cardinality of G

$\Leftarrow (Z_n, +_n) \rightarrow$ group

$$Z_n = \{0, 1, 2, \dots, n-1\}$$

$$x +_n y = (x+y) \bmod n$$

$\Leftarrow (Z_n \setminus \{0\}, *_n)$

$$x *_n y = (x \cdot y) \bmod n$$

$*_n$: multiplication modulo n .

i) $x *_n (y *_n z) = (x *_n y) *_n z$

$$y *_n z = t \Rightarrow y \cdot z = d \cdot n + t$$

$$x *_n t \Rightarrow x \cdot y \cdot z = d_1 \cdot n + t_1$$

$$2) x *_n 1 = 1 *_n x = x$$

$$3) a *_n b = 1 = b *_n a$$

$$a *_n b = 1$$

$$\Rightarrow a \cdot b = 1 + t \cdot n$$

$$\Rightarrow 1 = a \cdot b + t \cdot n$$

$$\Rightarrow \gcd(a, n) = 1$$

$$* Z_n^* = \{x \mid \gcd(x, n) = 1\}$$

$$(Z_n^*, *_n) \rightarrow \text{group.}$$

■ A non empty subset H of a group $(G, *)$ is subgroup of G if H is itself a group with respect to the same operation $*$ of G .

If H is a proper subset of G ($H \neq G, H \subset G$) then H is called a proper subgroup of G .

check

- i) $H \subseteq G$ or not
- ii) H is itself a group with $*$ or not

■ $(G, *) \rightarrow$ group

$$a \in G \Rightarrow a * a \in G \quad a * a = a^2$$

$$a * a * a \in G \quad a * a * a = a^3$$

$$a * a * \dots * a \in G \quad (i \text{ times})$$

$$a^i \in G$$

\square $e = \text{Identity element of } G$
 $a^{\alpha} = e \Rightarrow \underbrace{\alpha}_{\text{smallest}} \text{ is}$
called the order of a

$|G| : \text{order of } G.$

■ Group $\rightarrow (G, *)$

[G is closed under $*$]

$\alpha \in G$

$\alpha^0, \alpha^1, \alpha^2, \alpha^3, \dots \in G$

\downarrow

Identity

for any $b \in G$ $b = \alpha^i$

if $\exists i \geq 0$ s.t.

then α is called the generator of $(G, *)$

• $(G, *) = \langle \alpha \rangle$

■ A group G is cyclic if there is an element $\alpha \in G$ such that for every $b \in G$ there is an integer i with $b = \alpha^i$. This α is called the generator of G

$G = \langle \alpha \rangle$

$(G, *)$ $|G|$: finite

$o(a) = m$, $a^m = e$

$a \in G$

$e = a^0, a^1, a^2, \dots, a^{m-1} \in G$

$H = \{e = a^0, a^1, a^2, \dots, a^{m-1}\}$

i) $H \subseteq G$ ✓

ii) H is group under $*$

$$\begin{aligned} & \text{if } x, y \in H \\ & \Rightarrow x * y \in H \end{aligned}$$

for every $a^i \in H$ \exists the
inverse of a^i

H is group with *

H is a subgroup of G

$$H = \langle a \rangle$$

H is a cyclic subgroup of G .

$$\begin{aligned} |H| &= |\langle a \rangle| \rightarrow \text{order of the} \\ &\quad \text{cyclic subgroup} \\ &= o(a) \end{aligned}$$

Lagrange's theorem

If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$

\square G is a finite group

$$a \in G$$

$$o(a) \mid |G|$$

$$\Rightarrow a \in G,$$

$$H = \left\{ e = a^0, a^1, a^2, \dots, a^{o(a)-1} \right\}$$

H is a Subgroup of G

From Lagrange's theorem

$$\begin{array}{c} |H| \mid |G| \\ \Rightarrow o(a) \mid |G| \end{array}$$

\square If the order of $a \in G$ is t

$$\text{then } o(a^k) = \frac{t}{\gcd(t, k)}$$

\square If $\gcd(t, k) = 1$

$$\text{then } o(a^k) = t = o(a)$$

$$\Rightarrow |\langle a^k \rangle| = |\langle a \rangle|$$

$$x \in \langle a^k \rangle \qquad \langle a \rangle$$

$$\Rightarrow x = (a^k)^i = a^{ki} \in \langle a \rangle$$

$$\langle a^k \rangle \subseteq \langle a \rangle$$

$$\Rightarrow \langle a^k \rangle = \langle a \rangle$$

a^k is also a generator of $\langle a \rangle$

$\langle a^k \rangle = \underline{\langle a \rangle}$ Subgroup generated by a

$\underline{\langle a \rangle} = \underline{\langle a^k \rangle}$ Subgroup generated by $\underline{a^k}$

□ $Z_{19}^* = \{x \mid \gcd(x, 19) = 1, 1 \leq x \leq 18\}$

$*_{19}$: multiplication modulo 19

$$x *_{19} y = (x \cdot y) \bmod 19$$

Find the generators of $(Z_{19}^*, *_{19})$

$$\Rightarrow x \in Z_{19}^*$$

$$S = \{x^0, x^1, \dots\}$$

H.T

Ring

A ring $(R, +_R, \times_R)$ consists of one set R with two binary operations arbitrarily denoted by $+_R$ (addition) and \times_R (multiplication) on R satisfying the following properties

i) $(R, +_R)$ is a abelian group with the identity element 0_R

ii) The operation \times_R is associative

i.e.; $a \times_R (b \times_R c) = (a \times_R b) \times_R c \quad \forall a, b, c \in R$

iii) There is a multiplicative identity denoted by 1_R with $1_R \neq 0_R$ s.t.

$1_R \times_R a = a \times_R 1_R = a \quad \forall a \in R$

iv) The operation \times_R is distributive over $+_R$

i.e. $(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$

$a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$

Ex. $(\mathbb{Z}, +, \cdot)$: check it
is Ring or not H.T.

$\mathbb{Z} \rightarrow$ set of all integers

① $(R, +_R, \times_R) \rightarrow$ Ring

$$\bullet a \times_R b = b \times_R a \quad \forall a, b \in R$$

then $(R, +_R, \times_R)$ is a commutative
Ring

② $(\mathbb{Z}, +, \cdot) \rightarrow$ Ring

$$\Rightarrow a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$$

commutative ring

③ An element 'a' of a ring R
is called unit or an invertible element
if there is an element $b \in R$
s.t. $a \times_R b = 1_R$

- The set of units in a Ring R forms a group under multiplication operation.
⇒ This is known as group of units of R
-

Field

A field is a nonempty set F together with two binary operations $+$ (addition) and $*$ (multiplication) for which the following properties are satisfied

- i) $(F, +)$ is an abelian group
- ii) If 0_F denotes the additive identity element of $(F, +)$ then $(F \setminus \{0_F\}, *)$ is a commutative/abelian group
- iii) $\forall a, b, c \in F$ we have
$$a * (b + c) = (a * b) + (a * c)$$

- $\not\in$ i) $(\mathbb{Z}, +, \cdot)$ \rightarrow Not a field
 ii) $(\mathbb{Q}, +, \cdot)$ \rightarrow Field or not?

$(\mathbb{Q}, +)$ \rightarrow abelian group

0 : additive identity

1 : multiplicative identity

$(\mathbb{Q} \setminus \{0\}, \cdot)$: abelian group

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

\square $P \rightarrow$ prime number

$$\mathbb{F}_P = \{0, 1, 2, \dots, P-1\}$$

$(\mathbb{F}_P, +_P, *_P)$ \rightarrow Field or not?

$$x +_P y = (x + y) \bmod P$$

$$x *_P y = (x \cdot y) \bmod P$$

$$\begin{aligned}
 x+y &= t_1 P + r_1 \\
 z &= t_2 P + r_2 \\
 &= t_2 P + r_3 \\
 x+y+z &= t_2 P + r_3
 \end{aligned}$$

i) $(\mathbb{F}_p, +_p) \rightarrow$ abelian group

ii) $(\mathbb{F}_p \setminus \{0\}, *_p)$

1 : Identity element
(multiplicative)

$$\forall a \in \mathbb{F}_p \setminus \{0\} \quad \exists b \in \mathbb{F}_p \setminus \{0\}$$

$$\text{s.t. } a *_p b = 1$$

$$\Rightarrow (a \cdot b) \bmod p = 1$$

$$(a \cdot b - 1) = t \cdot p$$

$$\Rightarrow 1 = \frac{a \cdot b}{t} + t \cdot p$$

$$\boxed{\gcd(a, p) = a \cdot b + t \cdot p}$$

Extended Euclidean
Algo

田 Field Extension

Suppose K_2 is a field with
addition (+) and multiplication (*).

Suppose $K_1 \subseteq K_2$ is closed
under both these operation such
that K_1 it self is a field
with the restriction of + and *
to the set K_1 .

Then K_1 is called a subfield
of K_2 and K_2 is called
a field extension of K_1 .

田 $F \rightarrow \text{field } (F, +, *)$

$$F[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \dots \mid a_i \in F \right\}$$



Polynomial ring

$$(F[x], \underline{+}, \underline{*})$$

■ $F \rightarrow \text{field } (F, +, *)$

$$F[x] = \left\{ a_0 + a_1x + a_2x^2 + \dots \mid a_i \in F \right\}$$

$(F[x], +, *) \longrightarrow \text{Polynomial Ring}$

$+$: polynomial addition

$*$: polynomial multiplication

$$P_1(x) \in F[x]$$

$$P_1(x) = a_0 + a_1x + a_2x^2$$

$$P_2(x) \in F[x]$$

$$P_2(x) = b_0 + b_1x + b_2x^2$$

$$\begin{aligned} P_1(x) + P_2(x) &= (a_0 + a_1x + a_2x^2) \\ &\quad + (b_0 + b_1x + b_2x^2) \\ &= (\underline{a_0 + b_0}) + (\underline{a_1 + b_1})x \\ &\quad + (\underline{a_2 + b_2})x^2 \end{aligned}$$

$(a_i + b_i) \rightarrow \text{Field addition}$

$$a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$$

$$b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1}$$

+

$$\underline{(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_{n-1} + b_{n-1})x^{n-1}}$$

$(a_i + b_i)$: additive operation on F
as $a_i, b_i \in F$

$$\begin{aligned}
 & (a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}) \\
 * & (b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1}) \\
 = & (a_0 * b_0) + (a_0 * b_1 + a_1 * b_0)x \\
 & + \dots + (a_{n-1} * b_{n-1})x^{2n-2}
 \end{aligned}$$

$a_i * b_i \rightarrow$ Field multiplication in F
as $a_i, b_i \in F$

addition between the elements has
to be done in the Field.

④ $(F[x], +, *)$ is a polynomial ring

i) $(F[x], +)$ must be an abelian group

$$\begin{array}{c}
 + \begin{pmatrix} a_0 + a_1x + a_2x^2 \\ b_0 + b_1x + b_2x^2 \end{pmatrix} \quad a_i \in F \\
 \hline
 (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 = 0
 \end{array}$$

ii) $*$ is associative

iii) 1 is the multiplicative identity

iv) $*$ is distributive over $+$

■ $\mathbb{F}_2 = \{0, 1\}$ $(\mathbb{F}_2; +_2, *_2) \rightarrow \text{Field}$.

$$\mathbb{F}_2[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \dots \mid a_i \in \mathbb{F}_2 \right\}$$

$$P(x) = x + 1 \in \mathbb{F}_2[x]$$

$$q(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$$

$$\begin{aligned} P(x) * q(x) &= (x + 1) * (x^2 + x + 1) \\ &= x^2 + (1+1)x + (1+1) \\ &= x^2 \end{aligned}$$

$$\begin{aligned} P(x) + q(x) &= (x + 1) + (x^2 + x + 1) \\ &= (x^3 + x^2 + x) + (x^2 + x + 1) \\ &= x^3 + (1+1)x^2 + (1+1)x + 1 \\ &= x^3 + 1 \end{aligned}$$

■ A polynomial $P(x) \in F[x]$ of degree n ($n \geq 1$) is called irreducible if it cannot be written in the form of $P_1(x) * P_2(x)$ with $P_1(x), P_2(x) \in F[x]$ and degree of $P_1(x), P_2(x)$ must be ≥ 1

$$P(x) \neq P_1(x) * P_2(x)$$

$$\textcircled{1} \quad x^2 + 1 \in \mathbb{F}_2[x]$$

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

$$(x^2 + 1) = (x+1) * (x+1) \text{ in } \mathbb{F}_2[x]$$

$x^2 + 1$ is reducible in $\mathbb{F}_2[x]$

$$\textcircled{2} \quad I = \langle P(x) \rangle = \left\{ q(x) \cdot P(x) \mid q(x) \in F[x] \right\}$$

$I \rightarrow$ ideal generated by $P(x)$

$$\textcircled{3} \quad F[x] / \langle P(x) \rangle$$

$$q(x) \in F[x]$$

$$\boxed{\deg(r(x)) < \deg(P(x))}$$

$$q(x) = d(x) * P(x) + r(x)$$

$$r(x) \in F[x] / \langle P(x) \rangle$$

If $P(x)$ is irreducible polynomial then

$(F[x] / \langle P(x) \rangle, +, *)$ becomes
a field.

$$\mathbb{F}[x] / \langle P(x) \rangle$$

\rightarrow containing Poly^n of degree $< \deg(P(x))$

□ $x^2 + x + 1 \in \mathbb{F}_2[x]$, $\mathbb{F}_2 = \{0, 1\}$

$P(x) = x^2 + x + 1$ is irreducible.

* $\mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle$

$$q(x) = d(x) \cdot P(x) + r(x)$$

$$\deg(r(x)) < 2$$

$$r(x) \in \{0, 1, x, x+1\}$$

$$\begin{array}{r} x^2 + x + 1 \\ \underline{-} x^2 - x - 1 \\ \hline x \end{array}$$

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

- $x^2 + 1$

$$x^2 = x + 1$$

- $x^2 + 1 = (x+1) + 1$
 $= \underline{x}$

$$\begin{array}{r} x^2 + x + 1 \\ \underline{-} x^3 - x^2 - x \\ \hline x^2 + x + 1 \\ \underline{-} x^2 - x - 1 \\ \hline 0 \end{array}$$

$$\begin{aligned}
 x^3 + 1 &= x \cdot x^2 + 1 \\
 &= x \cdot (x+1) + 1 \\
 &= x^2 + x + 1 \\
 &= (x+1) + (x+1) \\
 &= 0
 \end{aligned}
 \quad \left| \begin{array}{l} x^2+1 \\ \hline x^2+1 \\ = 1+1 \\ = 0 \end{array} \right.$$

$$(x^2+x+1) \quad g(x) \quad ($$

$$g(x) = d(x) \cdot (x^2+x+1) + r(x)$$

$$\mathbb{F}_2[x] / \langle x^2+x+1 \rangle$$

$$x^2+x+1 = 0$$

α is the root of $x^2+x+1 = 0$

$$\alpha^2 + \alpha + 1 = 0$$

$$\Rightarrow \alpha^2 = \alpha + 1$$

$$\langle \alpha \rangle$$

$$\{0, 1=\alpha^0, \alpha^1, \alpha^2 = \alpha+1\} = \quad , \text{ord } \alpha = 2$$

$$\Rightarrow \{0, 1, \alpha, \alpha+1\}$$

$$\begin{aligned}
 \alpha^3 &= \alpha \cdot \alpha^2 \\
 &= \alpha(\alpha+1) \\
 &= \alpha^2 + \alpha \\
 &= 1
 \end{aligned}$$

$$\{0, 1, \alpha, \alpha+1\} \rightarrow \{0, 1, \alpha, \alpha+1\}$$

$$\mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle$$

all such poly^n of
 $\deg < 2$

$x^2 + x + 1 \rightarrow$ is known as
primitive Poly^n .

□ Advanced Encryption Standard (AES)

It is Standardized by NIST

- Rijndael
Winner of Advanced Encryption Standard Competition.
- Winner of Competition was named as AES

AES → i) Iterated block cipher
ii) It is based on SPN

AES - 128

- i) Block Size = 128 bit
- ii) Number of rounds = 10
- iii) Secret key size = 128 bit

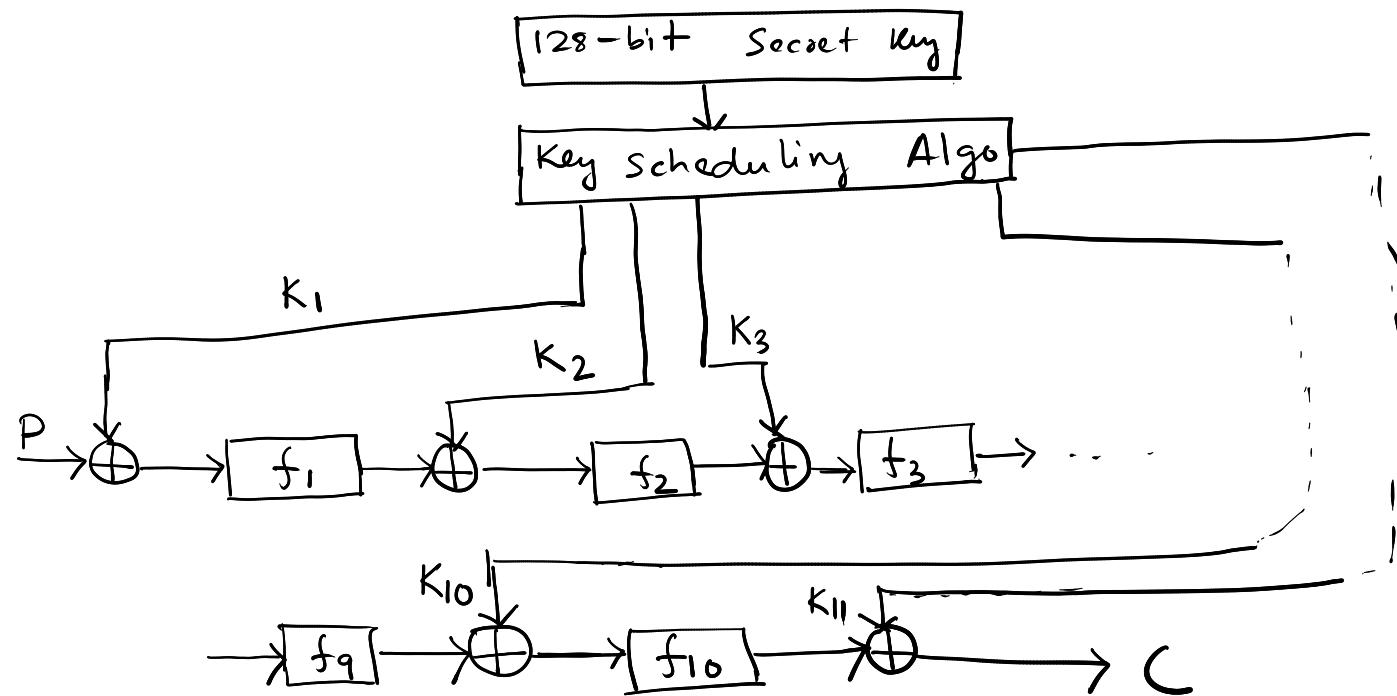
AES - 192

- i) Block Size = 192 bit
- ii) Number of rounds = 12
- iii) Secret key size = 192 bit

AES - 256

- i) Block Size = 128 bit
- ii) Number of rounds = 14
- iii) Secret Key Size = 256 bit

AES - 128



$P \rightarrow$ Plaintext block = 128 bit

$C \rightarrow$ Ciphertext block = 128 bit

$K_i \rightarrow$ round keys = 128 bit

□ We have to understand the followings:

i) Round functions

ii) Key Scheduling Algo

□ Round functions of AES-128

f_1, f_2, \dots, f_{10}

i) $f_1 = f_2 = f_3 \dots = f_9$

ii) f_{10} is different from $f_i, i=1, \dots, 9$

First 9 round functions are exactly same
10-th round function is different from
other 9 round function

□ The first 9 round functions (i.e., f_1, \dots, f_9)
are based on the following functions

• i) Subbytes

$$f_i : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

• ii) Shift rows

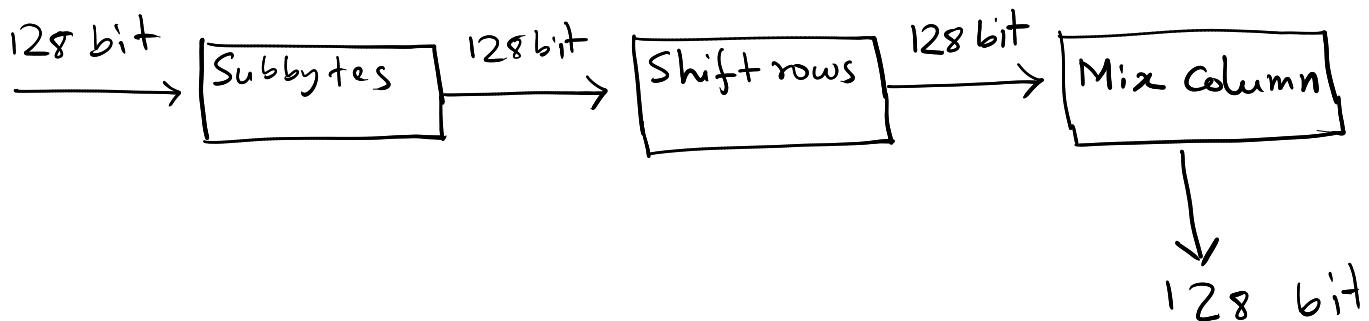
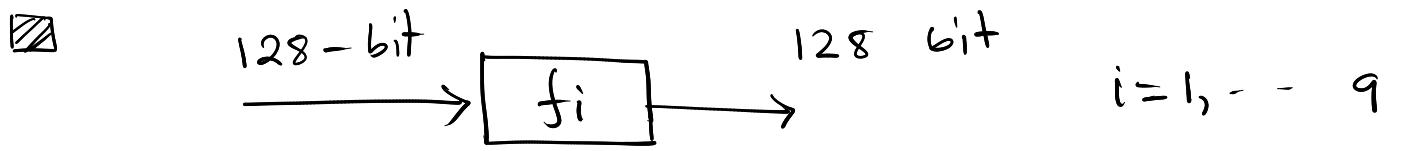
• iii) Mix Column

The 10-th round function (i.e., f_{10})
is based on

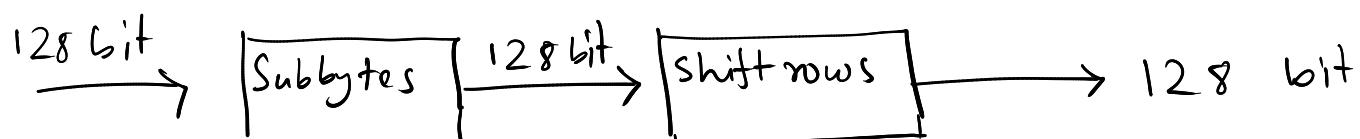
i) Subbytes

$$f_{10} : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

ii) Shift rows

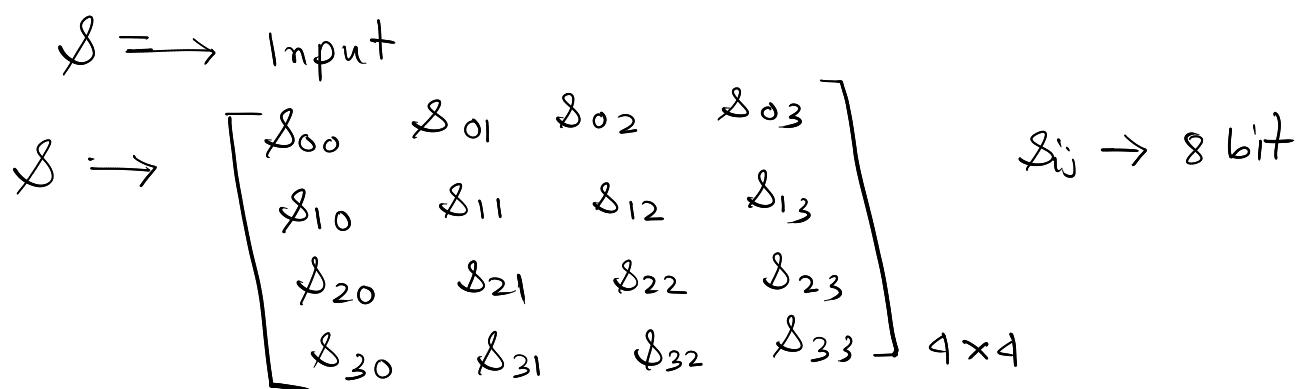


For 10th round



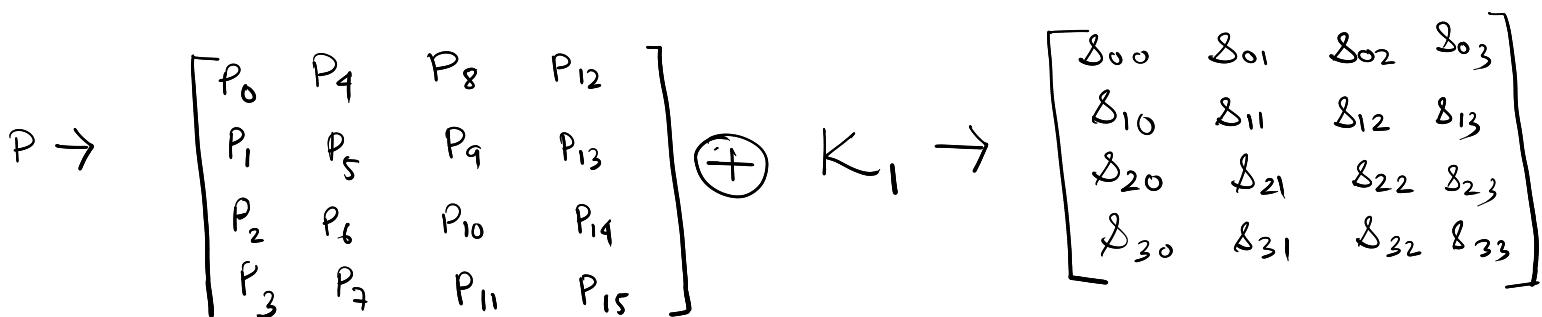
■ Subbytes

$$\text{Subbytes} : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$$



P \rightarrow plaintext 128 bit

$$P = P_0 P_1 \dots P_{15} \quad \text{len}(P_i) = 8 \text{ bit}$$



■ Subbytes

$$S = (s_{ij})_{4 \times 4}$$

- $S: \{0,1\}^8 \rightarrow \{0,1\}^8$ $s(0) = 0$

- $(c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0) = (01100011)$

- $S(s_{ij}) = (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$

- For $i = 0$ to 7

$$\begin{aligned} b_i = & (a_i + a_{(i+4) \% 8} + a_{(i+5) \% 8} \\ & + a_{(i+6) \% 8} + a_{(i+7) \% 8} + c_i) \bmod 2 \end{aligned}$$

- $(b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)$

- $s'_{ij} = (b_7 b_6 \dots b_0)$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \rightarrow \begin{bmatrix} s'_0 & s'_1 & s'_2 & s'_3 \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

128 bit

128 bit

We have to learn $S: \{0,1\}^8 \rightarrow \{0,1\}^8$

$$\square P \rightarrow P_0 P_1 \dots P_{15} \quad \text{len}(P_i) = 8 \text{ bit}$$

$$\left(\begin{array}{cccccc} P_0 & P_4 & \dots & P_{12} \\ P_1 & \vdots & & P_{13} \\ P_2 & \vdots & & P_{14} \\ P_3 & P_7 & & P_{15} \end{array} \right) \oplus K_1 = \underline{\underline{(s_{ij})_{4 \times 4}}}$$

$$S : \{0,1\}^8 \rightarrow \{0,1\}^8$$

$$S(s_{ij}) = (a_7 \dots a_0)$$

$$(c_7, \dots, c_0)$$

$$(b_7, \dots, b_0)$$

$$S : \{0,1\}^8 \rightarrow \{0,1\}^8$$

$$S(0) = 0$$

$$a_i \in \mathbb{F}_2$$

$$x \neq 0 \in \{0,1\}^8$$

$$S(x) = Y \in \{0,1\}^8$$

$$x = (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0), \quad a_i \in \{0,1\}$$

$$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

$$\deg(P(x)) \leq 7$$

$$P(x) \in \mathbb{F}_2[x]$$

$$(\mathbb{F}_2[x], +, *)$$

$$\bullet g(x) = x^8 + x^4 + x^3 + x + 1$$

$g(x)$ is a primitive polynomial

$$\left(\frac{\mathbb{F}_2[x]}{\langle g(x) \rangle}, +, \cdot, * \right) \rightarrow \text{Field}$$

Find the multiplicative inverse of $P(x)$ under modulo $(x^8 + x^4 + x^3 + x + 1)$

$$P(x) \cdot q(x) \equiv 1 \pmod{(x^8 + x^4 + x^3 + x + 1)}$$

$$\Rightarrow P(x) \cdot q(x) - 1 = h(x) \cdot (x^8 + x^4 + x^3 + x + 1)$$

$$\Rightarrow 1 = P(x) \cdot q(x) + h_1(x) \cdot (x^8 + x^4 + x^3 + x + 1)$$

$$\gcd(a, b) = a \cdot s + b \cdot t$$

$$\gcd(P(x), x^8 + x^4 + x^3 + x + 1) = 1$$

How to find $q(x)$?

\Rightarrow Extended Euclidean Algo finds $q(x)$

$q(x) \rightarrow \text{Poly}^n$ of degree atmost 7

$$q(x) = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 + r_5 x^5 + r_6 x^6 + r_7 x^7$$

$$q(x) \rightarrow (r_7 \ r_6 \ r_5 \ \dots \ r_0) \in \{0, 1\}^8$$

$$S(x) = Y = (r_7 \ r_6 \ \dots \ r_0)$$

Ex

Find

$$S(01010011) = ?$$

$$x = \begin{matrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ \downarrow \\ P(x) \end{matrix}$$

$$P(x) = x^6 + x^4 + x + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

$$\begin{array}{r}
 x^6 + x^4 + x + 1 \\
 \times x^8 + x^4 + x^3 + x + 1 \\
 \hline
 x^6 + x^4 + x^2 + x + 1 \\
 - x^6 - x^4 - x^3 - x^2 - x \\
 \hline
 x^4 + x + 1 \\
 - x^4 - x^2 - x \\
 \hline
 x^2 \\
 - x^2 - x \\
 \hline
 x \\
 - x - 1 \\
 \hline
 1
 \end{array}$$

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

$$= x^2 + (x+1) [(x^6 + x^4 + x + 1) + x^2(x^4 + x^2)]$$

$$\begin{aligned}
 &= (x+1)(x^6 + x^4 + x + 1) \\
 &\quad + [1 + (x+1)(x^4 + x^2)] x^2
 \end{aligned}$$

$$= (x+1)(x^5 + x^4 + x + 1) \\ + (1 + x^5 + x^3 + x^4 + x^2) \cdot x^2$$

$$= (x+1)(x^5 + x^4 + x + 1) \\ + (1 + x^5 + x^4 + x^3 + x^2) \left[(x^8 + x^4 + x^3 + x + 1) \right. \\ \left. + (x^2 + 1)(x^5 + x^4 + x + 1) \right]$$

$$= (1 + x^5 + x^4 + x^3 + x^2)(x^8 + x^4 + x^3 + x + 1) \\ + \left[(x+1) + (1 + x^5 + x^4 + x^3 + x^2)(x^2 + 1) \right] \\ (x^5 + x^4 + x + 1)$$

$$= h_1(x) \cdot g(x) + (x+1 + x^2 + x^7 + x^6 + x^5 + x^4 \\ + x^3 + x^2)(x^5 + x^4 + x + 1)$$

$$= h_1(x) \cdot g(x) + (x^7 + x^6 + x^3 + x)(x^6 + x^4 + x + 1)$$

$$\Rightarrow 1 = h_1(x) \cdot g(x) + (x^7 + x^6 + x^3 + x)(x^6 + x^4 + x + 1)$$

$$g(x) = x^7 + x^6 + x^3 + x$$

which is the multiplicative inverse of
 $(x^6 + x^4 + x + 1)$

$$\begin{aligned} \cdot S(01010011) &= (11001010) \\ c = (01100011) &= (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0) \\ b_i &= (a_i + a_{(i+4) \times 8} + a_{(i+5) \times 8} + a_{(i+6) \times 8} \\ &\quad + a_{(i+7) \times 8} + c_i) \bmod 2 \end{aligned}$$

$$\begin{aligned} b_0 &= (a_0 + a_4 + a_5 + a_6 + a_7 + c_0) \bmod 2 \\ &= (0 + 0 + 0 + 1 + 1 + 1) \bmod 2 \\ &= 1 \end{aligned}$$

$$b_1 = 0$$

$$\begin{aligned} (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0) \\ = (11101101) \end{aligned}$$

$$\text{Subbytes } (0101 \underline{00} \underline{11}) = (1110 \underline{11} \underline{01})$$

5 3 E D

$$\text{Subbytes } (53) = ED$$

$$\text{Input} = (XY)$$

$\text{Subbyte (Input)} = \text{element present in the}$
 $\text{row number } X \text{ and column}$
 $\text{number } Y$

Table is available in the
Stinson book pp - 112

Shift rows

Shift rows : $\{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

$$\begin{array}{l}
 \text{0} \quad \left[\begin{matrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{matrix} \right] \\
 \text{1} \\
 \text{2} \\
 \text{3}
 \end{array} \longrightarrow \left[\begin{matrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{matrix} \right]$$

Mix Column

Mix column : $\{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

$$(s_{ij})_{4 \times 4} \longrightarrow (\overset{\circ}{s}_{ij})_{4 \times 4}$$

Consider the column $c \in \{0, 1, 2, 3\}$

$$\underline{\text{Column}} = \begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix}$$

$$\begin{aligned}
 s_{ic} &= (a_7 a_6 \dots a_0) \\
 \text{Poly}^n &= a_0 + a_1 x + \dots + a_7 x^7
 \end{aligned}$$

For $i = 0 \text{ to } 3$

$$t_i = \text{Binary to poly } (s_{ic})$$

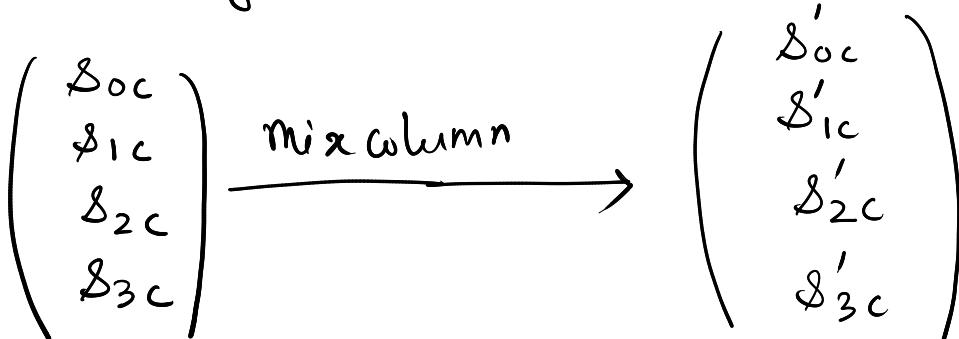
$$u_0 = [(x * t_0) + (x+1) * t_1 + t_2 + t_3] \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$u_1 = [(x * t_1) + (x+1) * t_2 + t_3 + t_0] \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$U_2 = [(x*t_2) + (x+1)*t_3 + t_0 + t_1] \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$U_3 = [(x*t_3) + (x+1)*t_0 + t_1 + t_2] \bmod (x^8 + x^4 + x^3 + x + 1)$$

• S'_{ic} = polynomial to binary (U_i)



Mix Column

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} * \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix}$$

$$\bmod (x^8 + x^4 + x^3 + x + 1) \\ = (S'_{ij})_{4 \times 4}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * (S_{ij}) \bmod (\cdot) \\ = (S'_{ij})_{4 \times 4}$$

$$\text{A } x \rightarrow (0\ 0\ 0\ 0\ 0\ 1\ 0) = 2$$

$$x+1 \rightarrow (0\ 0\ 0\ 0\ 0\ 1\ 1) = 3$$

Find $\begin{bmatrix} \delta'_{00} \\ \delta'_{10} \\ \delta'_{20} \\ \delta'_{30} \end{bmatrix}$ after doing operation on mixcolumn

where $\delta_{00} = 95$, $\delta_{10} = 65$, $\delta_{20} = FD$
 $\delta_{30} = F3$

$$\Rightarrow \delta_{00} = 95 = 10010101 = x^7 + x^4 + x^2 + 1$$

$$\delta_{10} = 65 = 01100101 = x^6 + x^5 + x^2 + 1$$

$$\delta_{20} = FD = 11111101 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$$

$$\delta_{30} = F3 = 11110011 = x^7 + x^6 + x^5 + x^4 + x + 1$$

$$\delta'_{00} = (x \times \delta_{00}) + ((x+1) \times \delta_{10}) + \delta_{20} + \delta_{30}$$

$$x \times \delta_{00} = x \times (x^7 + x^4 + x^2 + 1)$$

$$= x^8 + x^5 + x^3 + x \quad \text{mod } (x^8 + x^4 + x^3 + x + 1)$$

$$(x \times \delta_{00}) \text{ mod } (x^8 + x^4 + x^3 + x + 1)$$

$$= (x^8 + x^5 + x^3 + x) \text{ mod } (x^8 + x^4 + x^3 + x + 1)$$

$$\frac{x^8 + x^4 + x^3 + x + 1}{x^8 + x^4 + x^3 + x + 1} \overline{\underline{x^8 + x^5 + x^3 + x}} \quad |$$

$$\overline{\underline{x^5 + x^4 + 1}}$$

$$x^8 + x^5 + x^3 + x \equiv (x^4 + x^3 + x + 1) + x^5 + x^3 - x \\ \equiv x^5 + x^4 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}$$

$$x * s_{00} = x^5 + x^4 + 1$$

$$(x+1) * s_{10} = (x+1) * (x^6 + x^5 + x^2 + 1) \\ = x^7 + x^6 + x^3 + x + x^6 + x^5 + x^2 + 1 \\ = x^7 + x^5 + x^3 + x^2 + x + 1$$

$$s'_{00} = (x * s_{00}) + (x+1) * s_{10} + s_{20} + s_{30} \\ = (x^5 + x^4 + 1) + (x^7 + x^5 + x^3 + x^2 + x + 1) \\ + (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) \\ + (x^7 + x^6 + x^5 + x^4 + x + 1)$$

$$= x^7 + x^4$$

$$s'_{00} = x^7 + x^4 = (10010000) \\ = 90$$

$$s'_{10} = ?$$

$$s'_{20} = ? \quad \text{H.T}$$

$$s'_{30} = ?$$

$$s'_{10} = ((x * s_{10}) + (x+1) * s_{20} \\ + s_{30} + s_{00}) \pmod{x^8 + x^4 + x^3 + x + 1}$$

- i) Subbytes
- ii) Shiftrows
- iii) Mix Column

We are having clear idea on the round function

$f_1, f_2, \dots, f_9, f_{10}$

□ Key Scheduling

Input : 128 bit key

Output : 11 round keys

length of each round key is
128 bit

□ Key Scheduling Algo of AES - 128

Input: 128 bit key

Output: 11 round keys, each of length
128 bit.

$$\text{Key} = (\text{Key}[15], \dots, \text{Key}[0])$$

16 bytes

We will prepare 44 words which are denoted by $w[0], \dots, w[43]$

• ROTWORD (B_0, B_1, B_2, B_3)

$$= (B_1, B_2, B_3, B_0)$$

• SUBWORD (B_0, B_1, B_2, B_3)

$$= (B'_0, B'_1, B'_2, B'_3)$$

Where $B'_i = \text{SUBBYTES}(B_i) \quad \forall i=0, \dots, 3$

• 10 round constants (word)

$$R_{\text{Con}}[1] = 01\ 000\ 000$$

$$R_{\text{Con}}[2] = 02\ 00\ 000\ 0$$

$$R_{\text{Con}}[3] = 04\ 00\ 000\ 0$$

$$R_{\text{Con}}[4] = 08\ 00\ 000\ 0$$

$$R_{\text{Con}}[5] = 10\ 00\ 000\ 0$$

$$R_{\text{Con}}[6] = 20\ 00\ 000\ 0$$

$$Rcon[7] = 40000000$$

$$Rcon[8] = 80000000$$

$$Rcon[9] = 1B000000$$

$$Rcon[10] = 36000000$$

for $i = 0$ to 3

$$w[i] = (key[4i], key[4i+1], key[4i+2], \\ key[4i+3])$$

for $i = 4$ to 43

$$\text{temp} = w[i-1]$$

$$\text{if } i \equiv 0 \pmod{4}$$

$$\text{temp} = \text{SUBWORD}(\text{ROTWORD}(\text{temp})) \\ \oplus Rcon[i/4]$$

$$w[i] = w[i-4] \oplus \text{temp}$$

$$\text{return } (w[0], \dots, w[43])$$

② Round keys K_1, K_2, \dots, K_{11}

$$K_1 = w[0] \parallel w[1] \parallel w[2] \parallel w[3]$$

$$K_2 = w[4] \parallel w[5] \parallel w[6] \parallel w[7]$$

:

:

:

$$K_{11} = w[40] \parallel w[41] \parallel w[42] \parallel w[43]$$

Modes of operation

- i) ECB (Electronic Codebook mode)
- ii) CFB (Cipher feedback mode)
- iii) CBC (Cipher block chaining mode)
- iv) OFB (output feedback mode)
- v) Counter mode
- vi) CCM (Counter with cipher block chaining mode)

ECB

$$M = m_0 \parallel m_1 \parallel \dots \parallel m_t$$

Enc → It can encrypt ℓ bit plaintext block

$$\text{len}(m_i) = \ell \text{ bit}$$

Encryption

$$C = c_0 \parallel c_1 \parallel \dots \parallel c_t$$

$$c_i = \text{Enc}(m_i, K) \quad \forall i=0, \dots, t$$

Decryption

$$M = m_0 \parallel m_1 \parallel \dots \parallel m_t$$

$$m_i = \text{Dec}(c_i, K) \quad \forall i=0, \dots, t$$

Adv. Can be implemented parallelly

Dis Adv: if $m_i = m_j$
then $c_i = c_j$

CBC mode

$$M = m_1 \parallel m_2 \parallel \dots \parallel m_t$$

Initialization vector = IV (Public variable)

$\text{Enc} \rightarrow$ block size ℓ

$$\text{len}(m_i) = \ell$$

$$\text{len}(IV) = \ell$$

i) $c_0 = IV$

Encryption

$$c_i = \text{Enc}(c_{i-1} \oplus m_i, K) \quad \forall i=1, \dots, t$$

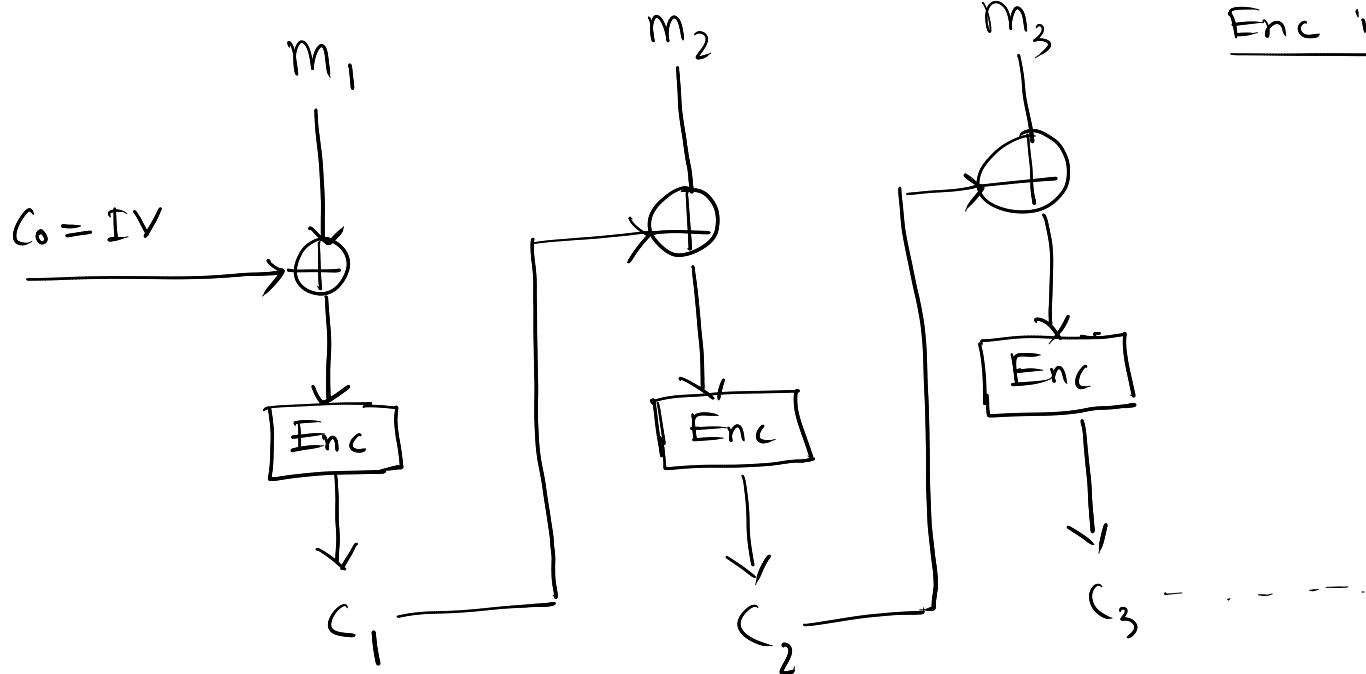
Ciphertext

$$C = c_0 \parallel c_1 \parallel c_2 \parallel \dots \parallel c_t$$

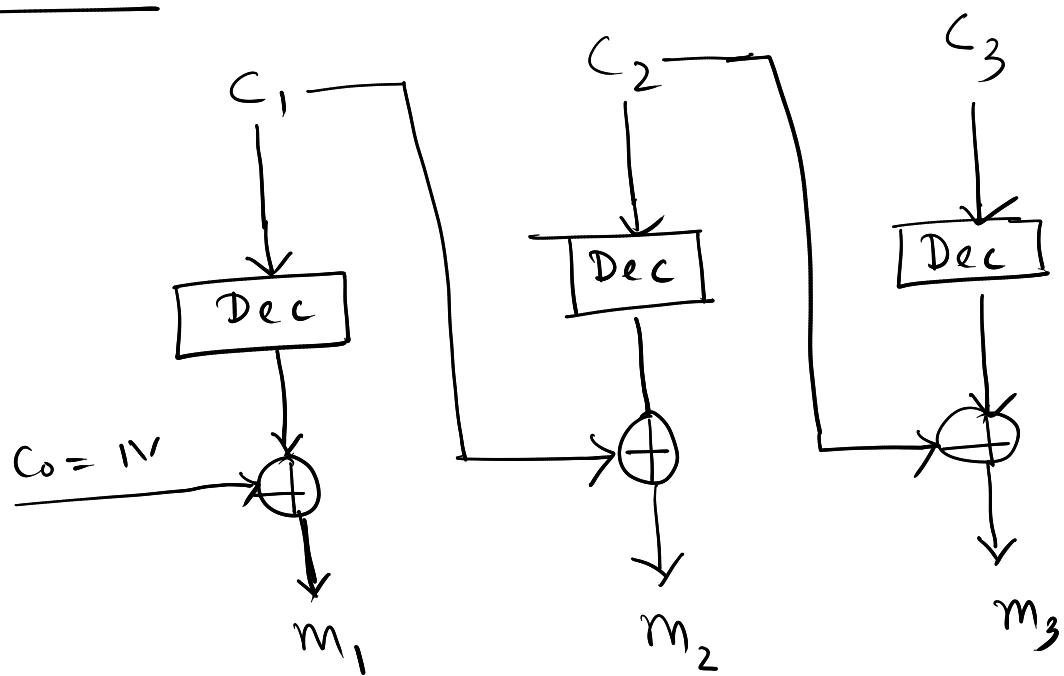
ii) $m_i = \text{Dec}(c_i, K) \oplus c_{i-1} \quad \forall i=1, \dots, t$

Where $c_0 = IV$

Enc in CBC



Dec in CBC



- Other modes of operation can be found in Stinson's book

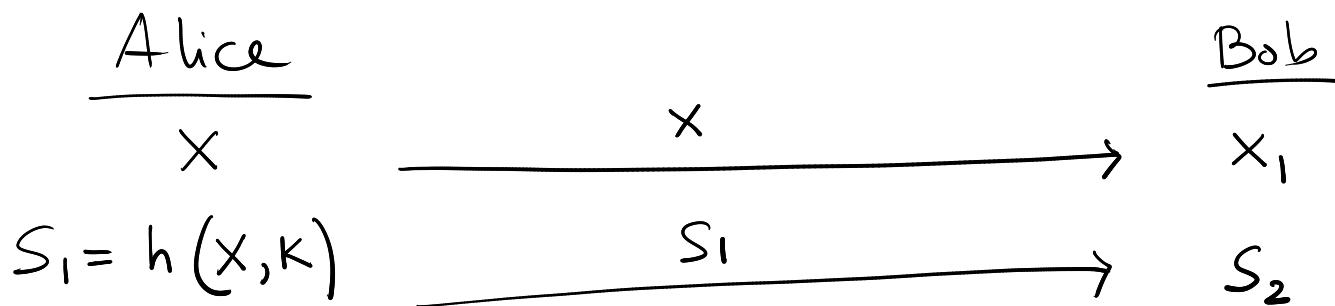
- Hash function

Hash Function

$$h : A \longrightarrow B$$

$$h(x) = Y$$

- I) If x is altered to x' then $h(x')$ will be completely different from $h(x)$
- II) Given Y it is practically infeasible to find X s.t. $h(x) = Y$
- III) Given X and $Y = h(x)$ it is practically infeasible to find X' s.t. $h(x) = h(x')$



If $h(x_1, K) = S_2$

then Bob accept x_1

- * We are able to check
 - I) whether x is altered during communication
 - II) whether S_1 is - - -

Defⁿ

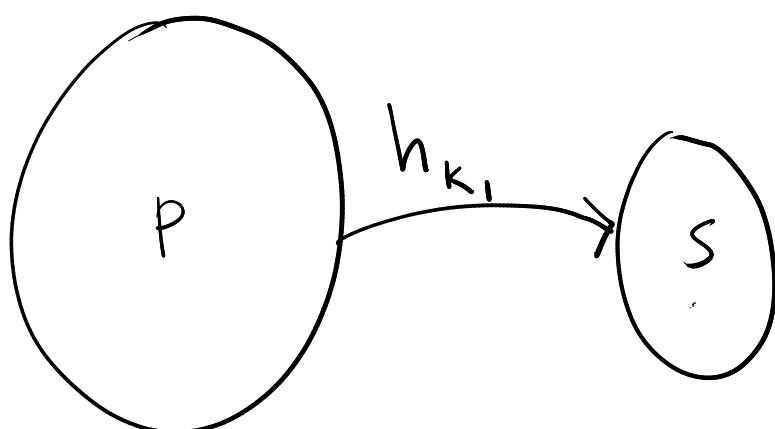
A hash family is a four tuple (P, S, K, H) where the following conditions are satisfied

- i) P is the set of all possible messages
- ii) S is the set of all possible message digests or authentication tags
- iii) K is the key space
- iv) For each $K_1 \in K$ there is a hash function $h_{K_1} \in H$ s.t.

$$h_{K_1} : P \longrightarrow S$$

Here $|P| \geq |S|$

More interestingly $\underline{|P| \geq 2 \times |S|}$



H : set of all hash functions

h_{K_1} : hash function

◻ If key is involved in the computation of hashed value then that hash function is known as Keyed hash function

If key is not required to compute the hashed value then that hash function is known as Unkeyed hash function.

◻ Problem 1

$$h: P \longrightarrow S$$

① Given $y \in S$ Find $x \in P$

such that $h(x) = y$

This problem is known as preimage finding problem.

For an hash function h if you can not find preimage in a feasible time then h is known as preimage resistant hash function.

* Finding preimage is computationally hard for preimage resistant hash function.

Problem 2

$$h : P \rightarrow S$$

Given $x \in P$ and $h(x)$ find $x' \in P$

$$\text{s.t. } x' \neq x \text{ and } h(x') = h(x)$$

This problem is known as Second pre image finding problem.

If finding second preimage is computationally hard for h then h is known as second preimage resistant hash function.

Problem 3

$$h : P \rightarrow S$$

Find $x, x' \in P$ s.t. $x \neq x'$
and $h(x) = h(x')$

This problem is known as Collision finding problem.

For an hash function h if finding collision is computationally hard then h is known as collision resistant hash function.

Ideal Hash function

Let $h : P \rightarrow S$ be an hash function.

h will be called ideal hash function if given $x \in P$ to find $h(x)$ either you have to apply h on x or you have to look into the table corresponding to h (hash table).

Pre image finding Algorithm

$$h : X \rightarrow Y$$

Choose any $X_0 \subseteq X$ s.t. $|X_0| = Q$

for each $x \in X_0$

Compute $y_x = h(x)$

if $y_x = y$

return x

\Pr [the above algorithm returns correct preimage] \Rightarrow give you the complexity.

Pre image finding Algo

Given $y \in Y$
 find $x \in X$
 s.t. $h(x) = y$

$$h: X \rightarrow Y ; |Y| = M$$

Choose any $X_0 \subseteq X$ s.t. $|X_0| = Q$

for each $x \in X_0$

compute $y_x = h(x)$

if $y_x = y$

return x

$$X_0 = \{x_1, x_2, \dots, x_Q\}$$

E_i : event $h(x_i) = y$; $1 \leq i \leq Q$

$$\Pr[E_i] = \frac{1}{M}$$

$$\Pr[E_i^c] = 1 - \frac{1}{M}$$

$$\Pr[E_1 \cup E_2 \cup E_3 \cup \dots \cup E_Q]$$

$$= 1 - \Pr[E_1^c \cap E_2^c \cap E_3^c \cap \dots \cap E_Q^c]$$

$$= 1 - \prod_{i=1}^Q \Pr[E_i^c]$$

$$= 1 - \left(1 - \frac{1}{M}\right)^Q$$

$$\begin{aligned}
 &= 1 - \left[1 - \binom{Q}{M} \frac{1}{M} + \binom{Q}{2} \frac{1}{M^2} \dots \right] \\
 &\approx 1 - \left[1 - \binom{Q}{M} \frac{1}{M} \right] \\
 &= \frac{Q}{M}
 \end{aligned}$$

$$\Pr[\text{Pre image finding}] \approx \frac{Q}{M}$$

Complexity of finding Preimage = $O(M)$

Collision finding Algo

$$h : X \rightarrow Y$$

$$|Y| = M$$

Find $x, x' \in X$ s.t. $x \neq x'$
and $h(x) = h(x')$

$X_0 \subseteq X$, $|X_0| = Q$
 $X_0 = \{x_1, \dots, x_Q\}$
for each $x \in X_0$

compute $y_x = h(x)$

if $y_x = y_{x'}$ for some $x \neq x'$

then return (x, x')

else return failure

E_i : event $h(x_i) \notin \{h(x_1), h(x_2), \dots, h(x_{i-1})\}$

$$X_o = \{x_1, \dots, x_{i-1}\}$$

$$\Pr[E_1] = 1$$

$E_2: h(x_2) \notin \{h(x_1)\}$

$$h(x_2) = z$$

$$z \in Y \setminus \{h(x_1)\}$$

$$\Pr[E_2 | E_1] = \frac{M-1}{M}$$

$$\Rightarrow \frac{\Pr[E_1 \cap E_2]}{\Pr[E_1]} = \frac{M-1}{M}$$

$$\Rightarrow \Pr[E_1 \cap E_2] = \frac{M-1}{M} \times \Pr[E_1]$$
$$= \frac{M-1}{M}$$

$$\Pr[E_3 | E_1 \cap E_2] = \frac{M-2}{M}$$

$$\Rightarrow \frac{\Pr[E_1 \cap E_2 \cap E_3]}{\Pr[E_1 \cap E_2]} = \frac{M-2}{M}$$

$$\Rightarrow \Pr[E_1 \cap E_2 \cap E_3] = \frac{M-2}{M} \times \Pr[E_1 \cap E_2]$$
$$= \frac{M-2}{M} \times \frac{M-1}{M}$$

$$\Pr[E_4 \mid E_1 \cap E_2 \cap E_3] = \frac{M-3}{M}$$

$$\Rightarrow \Pr[E_1 \cap E_2 \cap E_3 \cap E_4] = \frac{M-1}{M} \times \frac{M-2}{M} \times \frac{M-3}{M}$$

Continuing this process

$$\Pr[E_1 \cap E_2 \cap E_3 \dots \cap E_q] = \frac{M-1}{M} \times \frac{M-2}{M} \times \frac{M-3}{M} \dots \times \frac{M-(q-1)}{M}$$

$$\begin{aligned} & \Pr[\text{Collision finding Algo return success}] \\ &= 1 - \Pr[E_1 \cap E_2 \cap E_3 \dots \cap E_q] \\ &= 1 - \left[\frac{M-1}{M} \times \frac{M-2}{M} \times \dots \times \frac{M-(q-1)}{M} \right] \end{aligned}$$

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$$

$$\approx 1 - x$$

$$\frac{M-i}{M} = 1 - \frac{i}{M}$$

$$\approx e^{-\frac{i}{M}}$$

$$\begin{aligned}
 & \frac{M-1}{M} \times \frac{M-2}{M} \times \dots \times \frac{M-(Q-1)}{M} \\
 & \approx \prod_{i=1}^{Q-1} e^{-\frac{i}{M}} \\
 & = e^{-\sum_{i=1}^{Q-1} \frac{i}{M}} \\
 & = e^{-\frac{1}{M} \sum_{i=1}^{Q-1} i} \\
 & = e^{-\frac{1}{M} \frac{(Q-1) \cdot Q}{2}} \\
 & = e^{-\frac{1}{M} \frac{Q(Q-1)}{2}}
 \end{aligned}$$

$$\Pr[\text{Collision}] \approx 1 - e^{-\frac{1}{M} \frac{Q(Q-1)}{2}}$$

$$\begin{aligned}
 \epsilon & \approx 1 - e^{-\frac{1}{M} \frac{Q(Q-1)}{2}} \\
 \Rightarrow e^{-\frac{1}{M} \cdot \frac{Q(Q-1)}{2}} & \approx 1 - \epsilon
 \end{aligned}$$

$$\Rightarrow -\frac{Q(Q-1)}{2M} \approx \ln(1 - \epsilon)$$

$$\Rightarrow Q^2 - Q \approx -2M \ln(1 - \epsilon)$$

$$\Rightarrow Q^2 - Q \approx 2M \ln\left(\frac{1}{1-\epsilon}\right)$$

$$\Rightarrow Q^2 \approx 2M \ln\left(\frac{1}{1-\varepsilon}\right)$$

$$\Rightarrow Q \approx \sqrt{2M \ln\left(\frac{1}{1-\varepsilon}\right)}$$

$$= \sqrt{2 \ln\left(\frac{1}{1-\varepsilon}\right)} \sqrt{M}$$

$$\varepsilon = \frac{1}{2}$$

$$Q \approx \sqrt{2 \ln\left(\frac{1}{1-1/2}\right)} \sqrt{M}$$

$$= \sqrt{2 \times \ln 2} \sqrt{M}$$

$$\approx 1.177 \sqrt{M}$$

$$\varepsilon = 0.9$$

$$Q \approx \sqrt{2 \times \ln \frac{1}{1-0.9}} \sqrt{M}$$

$$\approx \sqrt{2 \times \ln 10} \sqrt{M}$$

$$\approx 2.19 \sqrt{M}$$

$$Q = O(\sqrt{M})$$

Complexity of Collision finding
= $O(\sqrt{M})$

□ $h : X \rightarrow Y \quad |Y| \leq 2^{|X|}$

Preimage $\rightarrow O(|Y|)$

Collision $\rightarrow O(\sqrt{|Y|})$

Second preimage $\rightarrow O(|Y|)$

□ $h : \{0,1\}^* \rightarrow \{0,1\}^m$

h is secure hash function

\rightarrow Preimage $\rightarrow O(2^m)$

Collision $\rightarrow O(2^{m/2})$

□ Compression function

$$h : \{0,1\}^{m+t} \rightarrow \{0,1\}^m$$

Preimage $\rightarrow O(2^m)$

Collision $\rightarrow O(2^{m/2})$

Target Construct $H : \{0,1\}^* \rightarrow \{0,1\}^m$
from h

Security of H will completely depend
on security of h .



Given $x \in \{0, 1\}^*$

$|x|$: length of x

$|x| \geq m+t+1$

From x construct y by using a public function. s.t

$$|y| \equiv o \pmod{t}$$

$$y = \begin{cases} x & \text{if } |x| \equiv o \pmod{t} \\ x \| 0^d & \text{if } |x| + d \equiv o \pmod{t} \end{cases}$$

Select $IV \in \{0, 1\}^m$ (IV is public)

$$y = y_1 \| y_2 \| \dots \| y_r$$

$$\text{s.t. } |y_i| = t, 1 \leq i \leq r$$

$$H \left\{ \begin{array}{l} z_0 = IV \\ z_1 = h(z_0 \| y_1) \\ z_2 = h(z_1 \| y_2) \\ \vdots \\ z_r = h(z_{r-1} \| y_r) \end{array} \right.$$

$z_r = H(x)$

This is known as iterative hash function

$$x' = z_{r-1} \parallel y_r$$

$$|x'| = m+t$$

$$\text{IV} = z_{r-1}, \quad x^* = y_r, \quad |x^*| \equiv 0 \pmod{t}$$

$$|x^*| = t$$

$$H\left\{ h\left(\underline{z_{r-1} \parallel y_r}\right) = z_r \right.$$

$$x'_1 = z'_{r-1} \parallel y'_r$$

$$x'_2 = z''_{r-1} \parallel y''_r$$

$$h(x'_1) = h(x'_2)$$

$$H(x'_1) = H(x'_2)$$

$$\textcircled{2} \quad M = y_1 \parallel y_2 \parallel \dots \parallel y_r$$

$$z_r = h(z_{r-1} \parallel y_r)$$

$$\text{where } z_i = h(z_{i-1} \parallel y_i) \quad i=1, \dots, r-1$$

$$z_0 = \text{IV}$$

Given (M, Z_r) is it possible to find (M_2, Z) without computing H on (M_2, Z)

$$\Rightarrow M_2 = M \parallel y_{r+1} \quad |y_{r+1}| = t$$

$$h(Z_r \parallel y_{r+1}) = Z \quad H(M) = Z_r$$

length extension Attack

Merkle - Damgard $h : \{0,1\}^* \rightarrow \{0,1\}$

$$\text{Compress} : \{0,1\}^{m+t} \rightarrow \{0,1\}^m \quad t \geq 2$$

$$n = |\chi|$$

$$K = \lceil n / (t-1) \rceil$$

$$d = K \cdot (t-1) - n$$

$$\chi = \chi_1 \parallel \chi_2 \parallel \dots \parallel \chi_K$$

$$|\chi_i| = t-1$$

for $i = 1$ to $K-1$

$$y_i = \chi_i$$

$$y_K = \chi_K \parallel 0^d$$

$$y_{K+1} = \text{binary}(d)$$

$$z_1 = o^{m+1} \parallel y_1$$

$$g_1 = \text{compress}(z_1)$$

for $i = 1$ to K

$$z_{i+1} = g_i \parallel 1 \parallel y_{i+1}$$

$$g_{i+1} = \text{compress}(z_{i+1})$$

$$h(x) = g_{K+1}$$

$$\text{return } (h(x))$$

D

SHA - I

MAC

SHA

Secure Hash Algorithm

- i) SHA-160
- ii) SHA-256
- iii) SHA-512

$$\text{SHA}: \{0,1\}^* \rightarrow \{0,1\}^n$$

SHA-1 PAD (x)

$$|x| \leq 2^{64} - 1$$

$$d = (447 - |x|) \bmod 512$$

$$l = \text{binary } (|x|)$$

$$y = x \parallel 1 \parallel 0^d \parallel l$$

$$\begin{aligned} |x| + d \\ \equiv 447 \pmod{512} \end{aligned}$$

$$\begin{aligned} |y| &= |x| + 1 + d + |l| & 447 + 1 + 64 \\ &\equiv 0 \pmod{512} & \equiv 0 \end{aligned}$$

X \wedge Y : bitwise and operation

X \vee Y : bitwise or operation

X \oplus Y : bitwise xor operation

$\neg X$: bitwise complement

X + Y : addition mod 2^{32}

$\text{ROTL}^S(x)$: Circular left shift on x by S position.

$$f_t(B, C, D) = \begin{cases} (B \wedge C) \vee (\neg B) \wedge D & 0 \leq t \leq 19 \\ B \oplus C \oplus D & 20 \leq t \leq 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & 40 \leq t \leq 59 \\ B \oplus C \oplus D & 60 \leq t \leq 79 \end{cases}$$

⊕ $\text{SHA-1}(x)$

$$y = \text{SHA-1-PAD}(x)$$

$$y = M_1 \parallel M_2 \parallel \dots \parallel M_n \quad |M_i| = 512$$

$$H_0 = 67952301$$

$$H_1 = EFCDAB89$$

$$H_2 = 98BA DC FE$$

$$H_3 = 10325476$$

$$H_4 = C3D2E1F0$$

$$K_t = \begin{cases} 5A827999 & 0 \leq t \leq 19 \\ 6ED9EBAA & 20 \leq t \leq 39 \\ 8F1BBCDC & 40 \leq t \leq 59 \\ CA62C1D6 & 60 \leq t \leq 79 \end{cases}$$

for $i = 1 \text{ to } n$

$$M_i = \omega_0 \parallel \omega_1 \parallel \omega_2 \parallel \dots \parallel \omega_{15}; |\omega_i| = 32$$

for $t = 16 \text{ to } 79$

$$\omega_t = \text{ROTL}^1 \left(\omega_{t-3} \oplus \omega_{t-8} \oplus \omega_{t-14} \oplus \omega_{t-16} \right)$$

$$A = H_0$$

$$B = H_1$$

$$C = H_2$$

$$D = H_3$$

$$E = H_4$$

for $t = 0 \text{ to } 79$

$$\begin{aligned} \text{temp} = & \text{ROTL}^5(A) + f_t(B, C, D) \\ & + E + \omega_t + K_t \end{aligned}$$

$$E = D$$

$$D = C$$

$$C = \text{ROTL}^{30}(B)$$

$$B = A$$

$$A = \text{temp}$$

$$H_0 = H_0 + A$$

$$H_1 = H_1 + B$$

$$H_2 = H_2 + C$$

$$H_3 = H_3 + D$$

$$H_4 = H_4 + E$$

Return $(H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4)$

MAC

Message authentication code

Alice
K

Bob
K

$$C = \text{Enc}(M, K) \xrightarrow{C} \tilde{C}$$

$$\text{MAC} = \text{Hash}(M, K) \xrightarrow{\text{MAC}} \tilde{\text{MAC}}$$

$$\text{Dec}(\tilde{C}, K) = \tilde{M}$$

$$\begin{aligned} & \text{Hash}(\tilde{M}, K) = \text{MAC}, \\ & \text{if } \text{MAC}_1 = \tilde{\text{MAC}} \\ & \text{accept } \tilde{M} \\ & \text{as } \tilde{M} = M \end{aligned}$$

□ HMAC

$$\text{ipad} = 36\ 36\ \dots\ 36 \rightarrow 512 \text{ bits}$$

$$\text{opad} = 5C\ 5C\ \dots\ 5C \rightarrow 512 \text{ bits}$$

K → Secret key

$$\text{HMAC}_K(x) = \text{SHA-1}\left(\left(K \oplus \text{opad}\right) \parallel \text{SHA-1}\left(\left(K \oplus \text{ipad}\right) \parallel x\right)\right)$$

□ CBC-MAC (x, K)

$$x = x_1 \parallel \dots \parallel x_n$$

$$\text{IV} = 00 \dots 0$$

$$y_0 = \text{IV}$$

for $i = 1$ to n

$$y_i = \text{Enc}\left((y_{i-1} \oplus x_i), K\right)$$

return (y_n)



Elliptic Curve Cryptography

P+Q, 2P

$$y^2 = x^3 - x$$

$$y^2 = x^3 + ax + b$$

$E_{23}(1,1)$ $y^2 = x^3 + x + 1 \pmod{23}$
(0 ... 22)

36

- i) $P = (13, 7)$; $-P = (x, -y) = (13, -7) = (13, 16)$
- ii) $R = P + Q$ $P = (3, 10)$ $Q = (9, 7)$

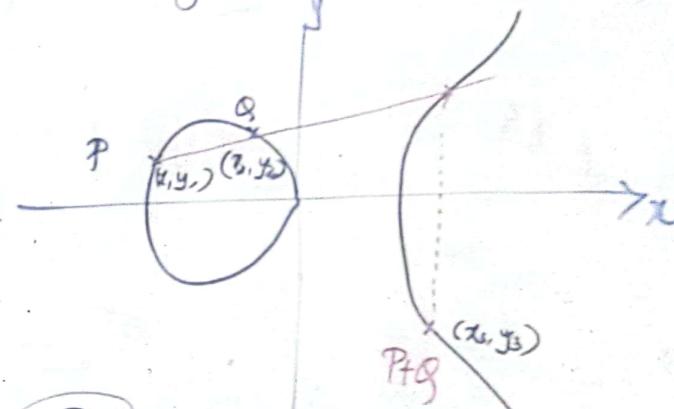
To find $2P$ $x_3 = \frac{(3 \cdot 9 + 1)^2 - 6}{2 \cdot 10} = \left(\frac{28}{20}\right)^2 + 17$

$$\left(\frac{5}{26}\right)^2 + 17 = \left(\frac{1}{4}\right)^2 + 17 = (1 \cdot 4)^2 + 17$$

$$6^2 + 17 = \underline{\underline{36 + 17}} = \underline{\underline{7}}$$

$$y_3 = -10 + \left(\frac{3 \cdot 9 + 1}{2 \cdot 10} \right) (3 - 7) = 13 + \left(\frac{28}{20} \right) \cdot -4$$

$$= 13 + \left(\frac{1}{4} \right) \cdot -4 = 13$$



$P+Q$, $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3)$$

$2P$, $P = Q$

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3)$$





LECTURES BY
SHREELAL DARSHAN

Elliptic Curve Cryptography

$P+Q, 2P$

$$y^2 = x^3 - z$$

$$\# E_{23}(1,1) \quad y^2 = x^3 + x + 1 \pmod{23}$$

$(0 \dots 22) \quad 36$

$P = (13, 7); \quad -P = (x, -y) = (13, -7) = (13, 16)$

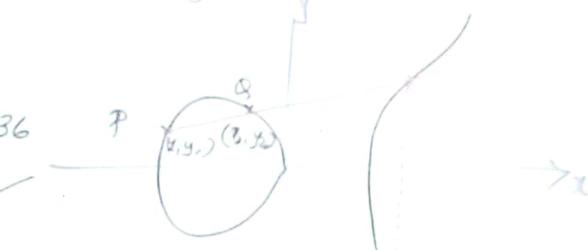
$R = P+Q \quad P = (3, 10) \quad Q = (9, 7)$

To find $2P \quad x_3 = \left(\frac{3x_1 + 1}{2x_1} \right)^2 - 6 = \left(\frac{28}{20} \right)^2 + 17$

$$\left(\frac{5}{4} \right)^2 + 17 = \left(\frac{1}{4} \right)^2 + 17 = (1.4)^2 + 17$$

$$6^2 + 17 = 36 + 17 = 53$$

$$y_3 = -10 + \left(\frac{3x_1 + 1}{2x_1} \right) (3 - 7) = 13 + \left(\frac{28}{20} \right) \cdot -4$$



$$P+Q, \quad x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3)$$

2P (P+Q)

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3)$$



Elliptic Curve Cryptography | Find points P+Q and 2P | ECC in Cryptography & Security

ES BY
RSHAN

Elliptic Curve Cryptography

P+Q, 2P

$$y^2 = x^3 - z$$

$$y^2 = x^3 + ax + b$$

$y^2 = x^3 - 36x$, $P = (-3, 9)$, $Q = (-2, 8)$; $a = -36$
 $P+Q$, & $2P$ $P+Q = (6, 0)$

$$x_3 = \left(\frac{8-9}{-2+3} \right)^2 - (-3) - (-2) = 1^2 + 3 + 2 = 6$$

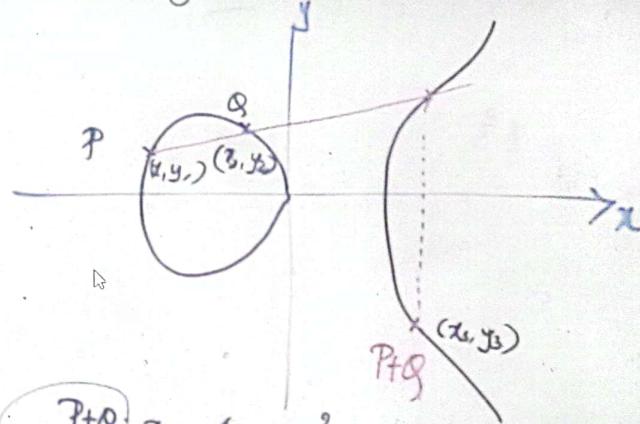
$$y_3 = -9 + \left(\frac{8-9}{-2+3} \right) (-3 - 6) = -9 - 1(-9) = 0$$

$$\underline{\underline{2P}} \quad x_3 = \left(\frac{3(-3)^2 + (-36)}{2 \cdot 9} \right)^2 - 2(-3) = \left(\frac{27-36}{18} \right)^2 + 6$$

$$x_3 = \frac{1}{4} + 6 = \frac{25}{4}$$

$$y_3 = -9 + \left(\frac{3 \cdot 9 - 36}{18} \right) (-3 - \frac{25}{4}) = -\frac{35}{8}$$

$$2P = \left(\frac{25}{4}, -\frac{35}{8} \right)$$



$$P+Q; x_3 = \left(\frac{y_2-y_1}{x_2-x_1} \right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1} \right) (x_1 - x_3)$$

(2P) P=Q

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3)$$



Elliptic Curve Cryptography - Encryption & Decryption

Calculation secret key User A $K = n_A, P_B$
 User B $K = n_B, P_A$

ECC	RSA/DSA
(n)	
112	512
256	3072

ECC Encryption :- $M \rightarrow$ message

Encode $M \rightarrow$ point on the EC, point P_M

For Encryption choose a +ve random int k

Cipher point $C_M = \{ \underline{kG}, P_M + kP_B \}$ Public key User B

ECC Decryption Multiply 1st pt Rx's private key

kG, n_B

$$\begin{aligned} \text{2nd pt } & P_M + k \underline{P_B} - k G n_B \\ & P_M + k, \underline{n_B}, G - k \underline{n_B} G \\ & = \underline{P_M} \end{aligned}$$

512 15360
 $y^2 = x^3 + ax + b$

$$P_A = n_A G$$

$$P_B = \underline{\underline{n_B}}, G$$

Elliptic Curve Cryptography - Encryption & Decryption

Calculation secret key User A $K = n_A, P_B$
 User B $K = n_B, P_A$

ECC (n)	RSA/DSA
112	512
256	3072

ECC Encryption :- $M \rightarrow$ message

Encode $M \rightarrow$ point on the EC, point P_M

For Encryption choose a +ve random int k'

Cipher point $C_M = \{ \underline{k'G}, P_M + k'P_B \}^{Public\ key}_{User\ B}$

ECC Decryption Multiply 1st pt Rx's private key

kG, n_B

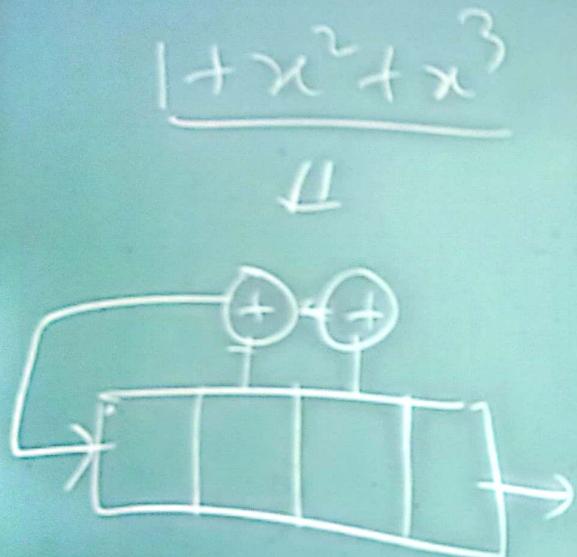
$$\begin{aligned} 2^{\text{nd pt}} \quad & P_M + k \underline{P_B} - k G n_B \\ & P_M + k, \underline{n_B}, G - k \underline{n_B} G \\ & = \underline{P_M} \end{aligned}$$

512 15360
 $y^2 = x^3 + ax + b$

$$P_A = n_A G$$

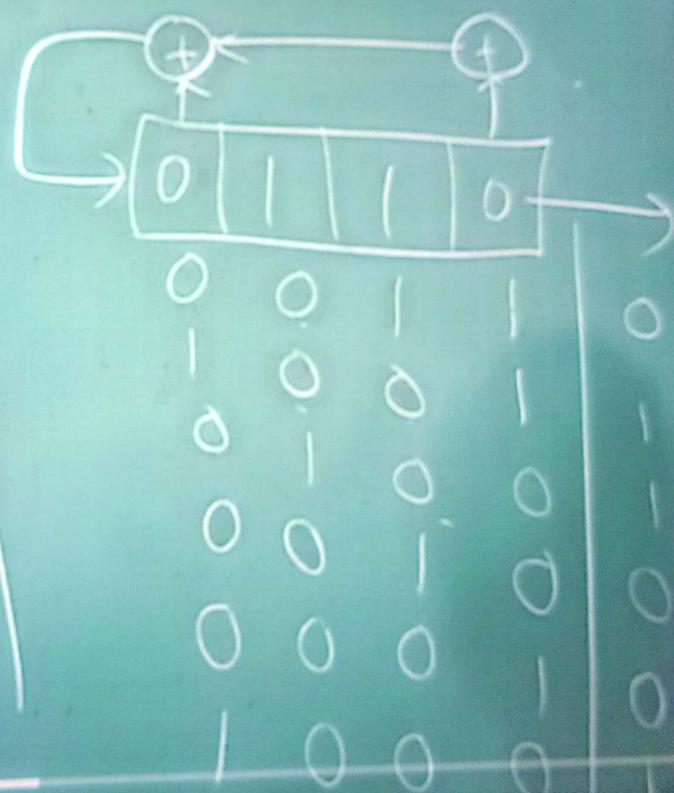
$$P_B = \underline{n_B}, G$$

LFSR BASED STREAM CIPHER



LFSR based Stream Cipher

0110



Subtitles/closed c

▶ ▶ ⏪ 7:17 / 30:22

OPPO Reno2 F

LFSR based Stream Cipher

$$1+x^2+x^3$$

↓↓

$$+ +$$



01100100011

0
0
0
0
1
0
1
1
1
0
1
1
1
0
0
0
1

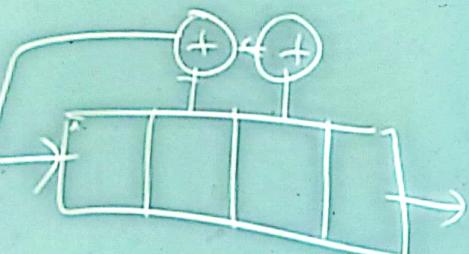
OPPO Reno2 F

ideapad GAMING

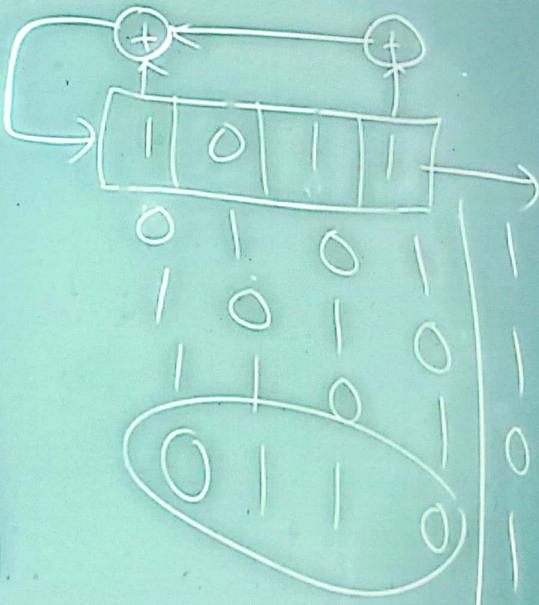
LFSR based Stream Cipher

$$1 + x^2 + x^3$$

↓↓

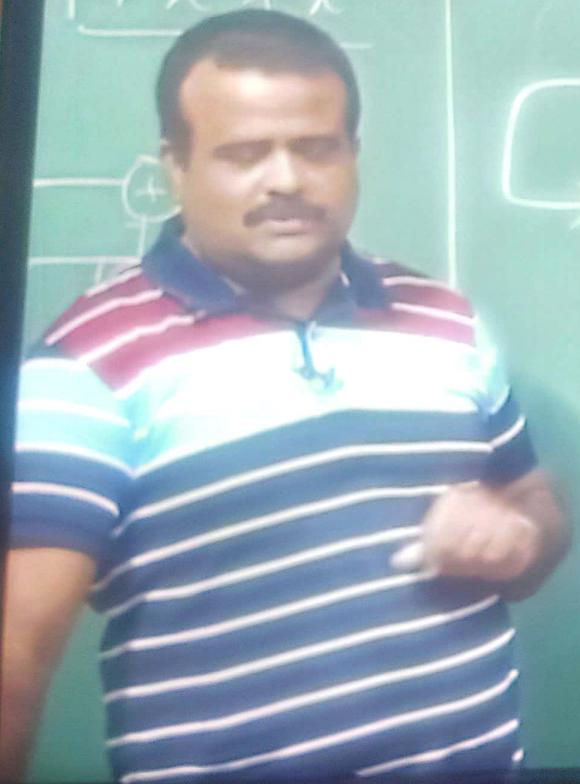


011001000111101



LFSR based Stream Cipher

$$1+x^2+x^3$$



011001000111101

↓
Period & length is

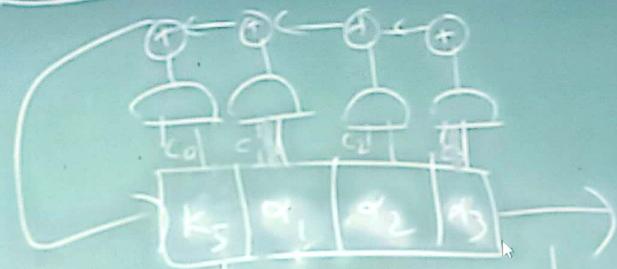
$1+x+x^4 \rightarrow$ primitive
Polynomial



LFSR BASED STREAM CIPHER

LFSR based Stream Cipher

$\alpha_1 \alpha_2 \alpha_3 \alpha_4$



linear function in $\alpha_1, \alpha_2, \alpha_3, \alpha_4$

$$\alpha_4 = k_1$$

$$\alpha_3 = k_2$$

$$\alpha_2 = k_3$$

$$\alpha_1 = k_4$$

$$k_5 = c_0\alpha_1 + c_1\alpha_2 + c_2\alpha_3 + c_3\alpha_4$$

$$\begin{aligned} k_6 &= c_0k_5 + c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 \\ &= d_0\alpha_1 + d_1\alpha_2 + d_2\alpha_3 + d_3\alpha_4 \\ k_7 &= w_0\alpha_1 + w_1\alpha_2 + w_2\alpha_3 \\ &\quad + w_3\alpha_4 \end{aligned}$$



RSA



Multiplicative inverse
 $x \neq 0 \pmod n$ (n is prime number)

$y = 1 \pmod n$ [y is multiplicative inverse of x]
 $y = x^{-1} \pmod n$

$$\begin{aligned} &x \neq 0 \pmod 5 \\ &3 \times 2 \equiv 1 \pmod 5 \\ &2 = 3^{-1} \pmod 5 \end{aligned}$$

$$\begin{aligned} &x \neq 0 \pmod 5 \\ &2 \times 3 \equiv 1 \pmod 5 \end{aligned}$$

'2' is MI of '3'

'2' or
'2' is MI of $3 \pmod 5$

$$\begin{aligned} &5 \neq 0 \pmod 9 \\ &5 \times 2 \equiv 1 \pmod 9 \quad \text{gcd}(5, 9) = 1 \end{aligned}$$

Explained with Examples in Hindi

OPPO Reno2F 1.1K

DISLIKE

SHARE

THANKS

CLIP

SAVE

...

Information And Cyber Security

5 Minutes Engineering - 32 / 66

RSA

X Q

Multiplicative inverse
(n is prime number)

- $x \neq 0 \pmod{n}$
- $x \cdot y \equiv 1 \pmod{n}$ [y is multiplicative inverse of x]
- $y = x^{-1} \pmod{n}$

eg

$$3 \neq 0 \pmod{5}$$

$$3 \times 2 \equiv 1 \pmod{5}$$

$$2 = 3^{-1} \pmod{5}$$

$$2 \neq 0 \pmod{5}$$

$$2 \times 3 \equiv 1 \pmod{5}$$

'2' is MI of '3'

OR

'2' is MI of $3 \pmod{5}$

$$5 \neq 0 \pmod{9}$$

$$5 \times 2 \equiv 1 \pmod{9}$$

$$\gcd(5,9)=1$$

RSA

Euler's Theorem:

$$\Rightarrow x^{\phi(n)} \equiv 1 \pmod{n}$$

Ex: $x = 4, n = 165$

$$\gcd(4, 165) = 1$$
$$\phi(165) = \phi(15) \times \phi(11)$$
$$= \phi(3) \times \phi(5) \times \phi(11)$$
$$= 2 \times 4 \times 10$$
$$= 80$$
$$\Rightarrow 4^{80} \equiv 1 \pmod{165}$$

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

Theorem Explained with Examples in Hindi

Mar 6, 2019

2.5K DISLIKE SHARE THANKS CLIP SAVE ...

Information And Cyber Security
5 Minutes Engineering - 33 / 66

40°C Smoke ENG 20:37 27-04-2022

OPPO Reno2 F

Fermat's Theorem:

$$\Rightarrow x^{n-1} \equiv 1 \pmod{n}$$

n : prime no.

x is not divisible by n

$$(x \not\equiv 0 \pmod{n})$$

$$\phi(n) = n-1$$

$$x=3 \quad n=5$$

$$3^{n-1} = 3^4 = 81$$

$$\therefore 81 \equiv 1 \pmod{5}$$

$$x \cdot x^{n-1} = x^n$$

$$\begin{aligned} & x \cdot x^{\phi(n)} \equiv 1 \pmod{n} \\ & x^{\phi(n)+1} = x^{n-1} \equiv 1 \pmod{n} \end{aligned}$$

$$\Rightarrow x^{\phi(n)+1} \equiv x \pmod{n}$$

$$\Rightarrow x^{(n-1)+1} \equiv x \pmod{n}$$

$$x^n \equiv x \pmod{n}$$

$$(\gcd(x, n) = 1)$$

$$3 \pmod{5}$$



RSA algorithm (Rivest, Shamir, Adleman)

Choose 2 Prime nos, p & q

$$p = 61 \quad q = 53$$

note : $n = p \times q = 61 \times 53 = 3233$

$$\boxed{n = 3233}$$

$$\begin{aligned}n) &= \phi(p \times q) = \phi(p) \times \phi(q) \\&= (p-1) \times (q-1) = 60 \times 52 \\&\quad \boxed{= 3120}\end{aligned}$$

$$\phi(n)$$

choose 'e' ; $1 \leq e < \phi(n)$, Coprime to $\phi(n)$

$$e = 17$$

$$\circ (e, n) = \text{public key } (17, 3233) \quad \boxed{\gcd(17, 3120) = 1}$$

Determine 'd' as

$$\boxed{ed \equiv 1 \pmod{\phi(n)}}$$

$$d = e^{-1} \pmod{\phi(n)} \quad (\text{d is MI of e})$$

$$2753$$

$$\circ (d, n) = \text{private key } (2753, 3233)$$

RSA Algorithm (Rivest, Shamir, Adleman)

Choose 2 Prime nos, p & q:

$$p = 61 \quad q = 53$$

Compute : $n = p \times q = 61 \times 53 = 3233$

$$\begin{aligned}\phi(n) &= \phi(p \times q) = \phi(p) \times \phi(q) \\ &= (p-1) \times (q-1) = 60 \times 52 \\ &\quad \boxed{= 3120} \end{aligned}$$

$$\boxed{n = 3233}$$

$$\phi(n)$$

④ choose 'e'; $1 \leq e < \phi(n)$, Coprime to $\phi(n)$

$$\circ (e, n) = \text{public key } (17, 3233) \quad \boxed{\gcd(17, 3120) = 1}$$

Determine 'd' as

$$ed \equiv 1 \pmod{\phi(n)}$$

$$17^{-1} \pmod{3120} \quad (d \text{ is MI of } e)$$

$$17 \times d = 1$$

$$\circ (d, n) = \text{private key } (2753, 3233)$$

RSA algorithm

◦ Finding 'd'

$$ed = 1 \bmod \phi(n)$$

$$d = \frac{(\phi(n) \times i) + 1}{e}$$

$$d = \frac{(3120 \times 4) + 1}{17} = 734.17$$

$$d = \frac{(3120 \times 12) + 1}{17} = 2,202.411$$

$$d = \frac{(3120 \times 15) + 1}{17} = 2753$$

$$d = \frac{(3120 \times 1) + 1}{17} = 183.58$$

$$d = \frac{(3120 \times 2) + 1}{17} = 367.11$$

$$d = \frac{(3120 \times 3) + 1}{17} = 550.647$$

RSA algorithm

Encryption (13, 143)

$$C = P^e \pmod{n}; P < n$$

$$C = 13^{13} \pmod{143}$$

$$\circ 13 \pmod{143} = 13$$

$$\circ 13^4 \pmod{143} = 104$$

$$\circ 13^8 \pmod{143} = 91$$

$$\left[(13^8 \pmod{143})(13^4 \pmod{143}) \right. \\ \left. (13 \pmod{143}) \right] \pmod{143}$$

$$(109 \times 13) \pmod{143}$$

decryption (37, 143)

$$P = C^d \pmod{n} \\ = 52^{37} \pmod{143}$$

$$\circ 52 \pmod{143} = 52$$

$$\circ 52^4 \pmod{143} = 26$$

$$\circ 52^{32} \pmod{143} = 130$$

$$P = \left[(52^{32} \pmod{143})(52^4 \pmod{143}) \right. \\ \left. (52 \pmod{143}) \right] \pmod{143}$$

$$P = [130 \times 26 \times 52] \pmod{143}$$

$$\boxed{P = 13}$$



RSA algorithm

Encryption $(13, 143)$

$$C = P^e \text{ mod } n ; P < n$$

$$C = 13^{13} \text{ mod } 143$$

$$\circ 13 \text{ mod } 13 = 13$$

$$\circ 13^2 \text{ mod } 143 = 104$$

$$8$$

$$91$$

$$\circ (13^4 \text{ mod } 143)$$

$$\text{mod } 143$$

$$\text{mod } 143$$

$$= 52$$

decryption $(37, 143)$

$$P = C^d \text{ mod } n$$

$$= 52^{37} \text{ mod } 143$$

$$\circ 52 \text{ mod } 143 = 52$$

$$\circ 52^2 \text{ mod } 143 = 26$$

$$\circ 52^{32} \text{ mod } 143 = 130$$

$$P = [(52^{32} \text{ mod } 143)(52^4 \text{ mod } 143) \\ (52 \text{ mod } 143)] \text{ mod } 143$$

$$P = [130 \times 26 \times 52] \text{ mod } 143$$

$$\boxed{P = 13}$$

RSA algorithm

Encryption (13, 143)

$$C = P^e \text{ mod } n ; P \in \mathbb{Z}_n$$

$$C = 13^{13} \text{ mod } 143$$

$$\circ 13 \text{ mod } 143 = 13$$

$$\circ 13^4 \text{ mod } 143 = 101$$

$$\circ 13^8 \text{ mod } 143 =$$

$$\quad \quad \quad (13^4 \text{ mod } 143)$$

$$\quad \quad \quad [143)] \text{ mod } 143$$

$$= (91 \times 109 \times 13) \text{ mod } 143$$

$$= 52$$

decryption (37, 143)

$$P = C^d \text{ mod } n$$

$$= 52^{37} \text{ mod } 143$$

$$\circ 52 \text{ mod } 143 = 52$$

$$\circ 52^4 \text{ mod } 143 = 26$$

$$\circ 52^{32} \text{ mod } 143 = 130$$

$$P = [(52^{32} \text{ mod } 143)(52^4 \text{ mod } 143) \\ (52 \text{ mod } 143)] \text{ mod } 143$$

$$P = [130 \times 26 \times 52] \text{ mod } 143$$

$$\boxed{P = 13}$$

RSA algorithm
Encryption $(13, 143)$

$$C \mod n ; P < n$$
$$13^{13} \mod 143$$

$$\mod 143 = 13$$

$$\mod 143 = 104$$

$$13^8 \mod 143 = 91$$

$$C = [(13^8 \mod 143)(13^4 \mod 143) \\ (13 \mod 143)] \mod 143$$
$$= (91 \times 104 \times 13) \mod 143$$

$$C = 52$$

decryption $(37, 143)$

$$P = C^d \mod n$$
$$= 52^{37} \mod 143$$

$$52 \mod 143 = 52$$

$$52^4 \mod 143 = 26$$

$$52^{32} \mod 143 = 130$$

$$P = [(52^{32} \mod 143)(52^4 \mod 143) \\ (52 \mod 143)] \mod 143$$

$$P = [130 \times 26 \times 52] \mod 143$$

$$P = 13$$

Inbox (3,627) - goyaljatin3

Inbox (315) - goyaljatin110

Classes

Assignment-II.pdf - Google

Euler's Totient Function

GitHub

cryptography and network security

Euler's Totient function

- It is represented using phi as $\phi(n)$ and may also be called Euler's phi function.
- Euler's totient fn is defined as the no. of +ve integers less than n that are coprime to n.
 $n \geq 1$

$$\phi(1) = 1$$

$$\phi(5) = \{1, 2, 3, 4\} \quad \{4\}$$

$$\phi(6) = \{1, 5\}$$

① $\begin{matrix} 2 & 3 & 4 & 5 \\ \times & \times & \times & \checkmark \end{matrix}$

no. of elements in these sets
is the totient fⁿ.

Note → Two integers a, b are said to be
• relatively prime, mutually prime or
• coprime

bhishesh011

Totient Function in Cryptography

Oct 31, 2019

OPPO Reno2 F Cryptography and Network Security

1.4K

DISLIKE

SHARE

THANKS

CLIP

Cryptography and network security
Abhishek Sharma · 24 / 20

YouTube IN

Inbox (3,627) - goyaljatin3 Inbox (315) - goyaljatin110 Classes Assignment-II.pdf - Google Docs Euler's Totient Function GitHub

youtube.com/watch?v=ZBkpYKGPHUs&list=PL9FuOtXibFjV77w2eyll4Xzp8eo0qsPp8&t=34

cryptography and network security

Now, when $n \rightarrow \text{prime}$
eg $\phi(5) = 4$ // we have seen the eg. above
 $\phi(23) = 23 - 1$
 $= 22$

Also, $\phi(a * b) = \phi(a) * \phi(b)$ / a and b should be coprime
eg $\phi(35) = \phi(7) * \phi(5)$
 $= 6 * 4 =$
eg $\phi(12) = \phi(3) * \phi(4) = 2 * 2 = 4$
 $\phi(15) = \phi(3) * \phi(5) = 2 * 4 = 8$
8, 11, 13, 14

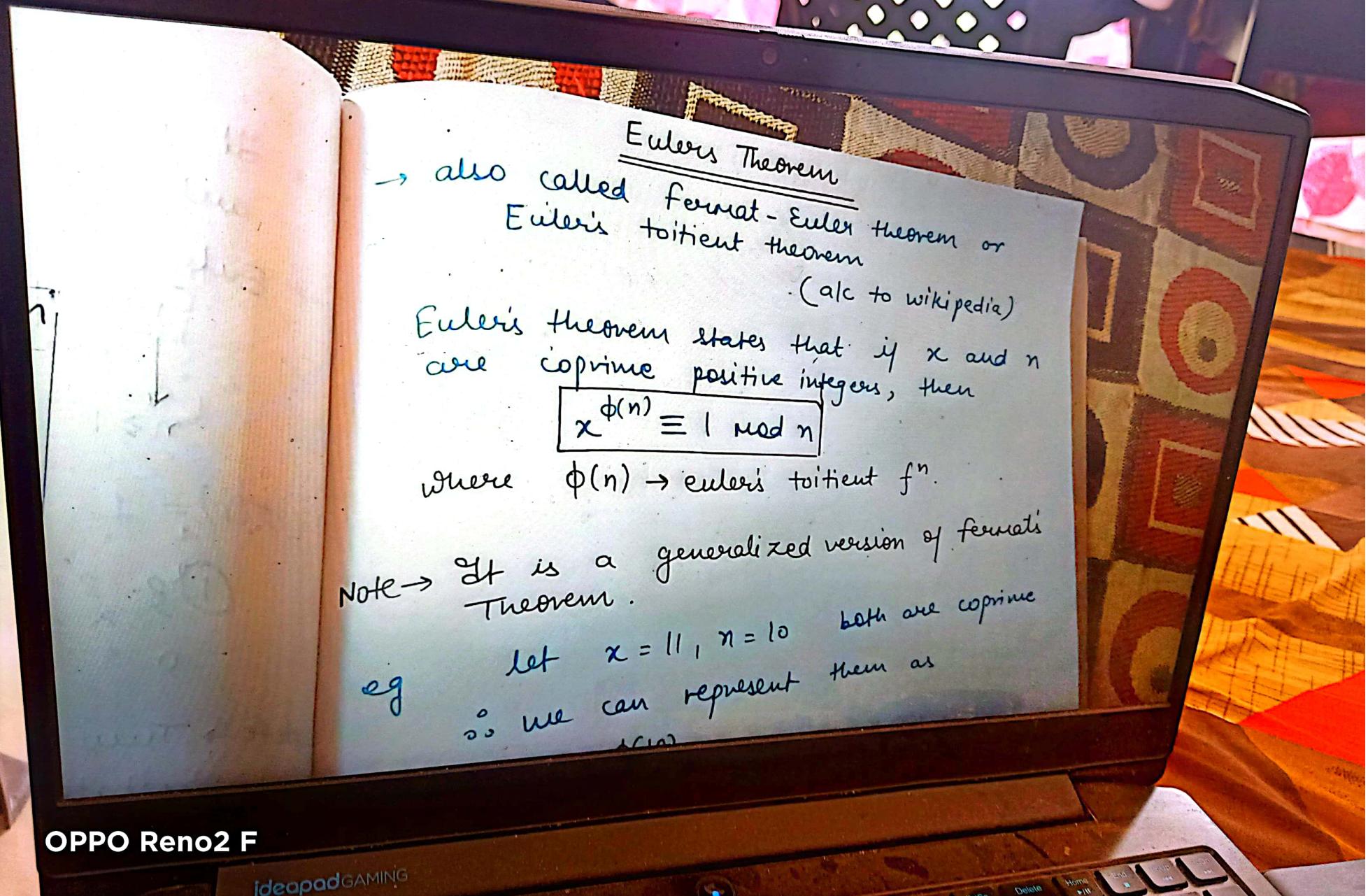
789 #AbhishekDIT
Euler's Totient Function In Cryptography and Network Security
3 views · Oct 31, 2019 · OPPO Reno2 F

Cryptography and network security
Abhishek Sharma · 34:10

1.4K DISLIKE SHARE THANKS CLIP SAVE

59% 37°C Smoke 11:31 08:00 06.01.2022

Be here to search



OPPO Reno2 F

ideapad GAMING

$\phi(n) \rightarrow$ Euler's totient function $x^{\phi(n)} \bmod n = 1$

Note \rightarrow It is a generalized version of fermat's theorem.

eg

let

$$\therefore x = 11, n = 10$$

\therefore we can represent them as
both are coprime

$$11^{\phi(10)} \equiv 1 \pmod{10}$$

$$11^4 \equiv 1 \pmod{10}$$

$$\boxed{14641} \equiv 1 \pmod{10}$$

which is true

$$\phi(10) = \phi(2) \cdot \phi(5)$$

$$1 \cdot 4$$

$$\phi(a+b) = \phi(a) \cdot \phi(b)$$

$$\phi(13) = 12$$

$$11^8 = 214,358,881$$

Note \rightarrow

$$\frac{1}{d_n}$$

OPPO Reno2 F

ideapad GAMING

$$4^{99} \mod 35$$

$$x = 4, n = 35$$

by euler theorem,

$$4^{\phi(35)} \equiv 1 \pmod{35}$$

$$4^{24} \equiv 1 \pmod{35} \quad (1)$$

$$1.99 - 1.24(4) \cdot 4^3$$

$$\equiv 1 \pmod{n}$$

$$\equiv 1 \pmod{n}$$

euler theorem
 $x^{\phi(n)} \equiv 1 \pmod{n}$

$x, n \rightarrow$ coprime +ive integers

$$\phi(n) = n-1$$

$$\begin{aligned}\phi(35) &= \phi(7) \cdot \phi(5) \\ &= 6 \cdot 4\end{aligned}$$

$$\phi(35) = 24$$

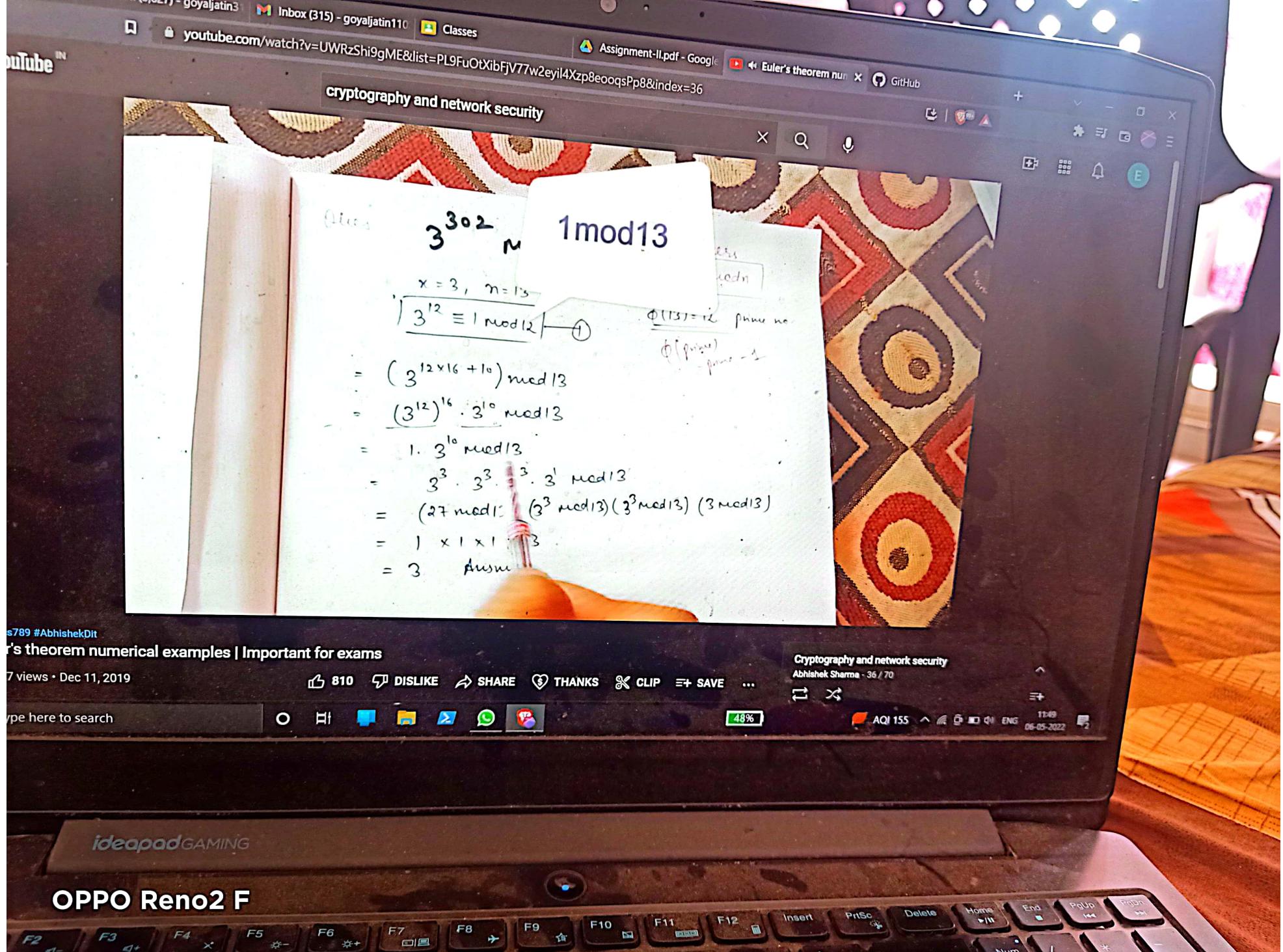
$$4^{24} \equiv 1 \pmod{35}$$

$$\begin{aligned}4^{35} &= 4^{24 \times 4 + 3} \pmod{35} \\ &= (4^{24})^4 \cdot 4^3 \pmod{35} \\ &= (4^4)^4 \pmod{35} \cdot 4^3 \pmod{35}\end{aligned}$$

$$\pmod{n} \equiv (a \pmod{n})(b \pmod{n})$$

$$\begin{aligned}&= 1 \times 4^3 \pmod{35} \\ &= 64 \pmod{35} \\ &= 29\end{aligned}$$

$$99 \pmod{25} = 24$$



OPPO Reno2 F

cryptography and network security

X Q

Fermat's Theorem / Fermat's Little Theorem
→ special case of Euler's theorem
If n is prime and x is a non-integer not divisible by n then
$$x^{n-1} \equiv 1 \pmod{n}$$

$n \rightarrow$ prime no.

x is not divisible by n

$$\phi(n)=n-1$$

Also,

$x, n \rightarrow$ coprime

eg $x = 3, n = 5$
 $3^{5-1} = 3^4$
 $\therefore 81 \equiv 1 \pmod{5}$

Euler theorem

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

$$x^{n-1} \equiv 1 \pmod{n}$$

Inbox (315) - goyaljatin110 Classes Assignment-II.pdf - Google Docs Fermat's Theorem GitHub

cryptography and network security

SOLVE BY FERMAT's Theorem

Ques

$a^{n-1} \equiv 1 \pmod{n}$ if n is a prime number.

or $a^{p-1} \equiv 1 \pmod{p}$.

eg $2^{16} \pmod{17}$

By Fermat's theorem

$$x^n \equiv 1 \pmod{n}$$
$$2^{16} \equiv 1 \pmod{17}$$
$$2^{16} \pmod{17} = 1 \quad \text{Ans}$$

eg

ics789 #AbhishekDit
mat's Theorem Numerical examples | Important for exams
66 views • Dec 11, 2019

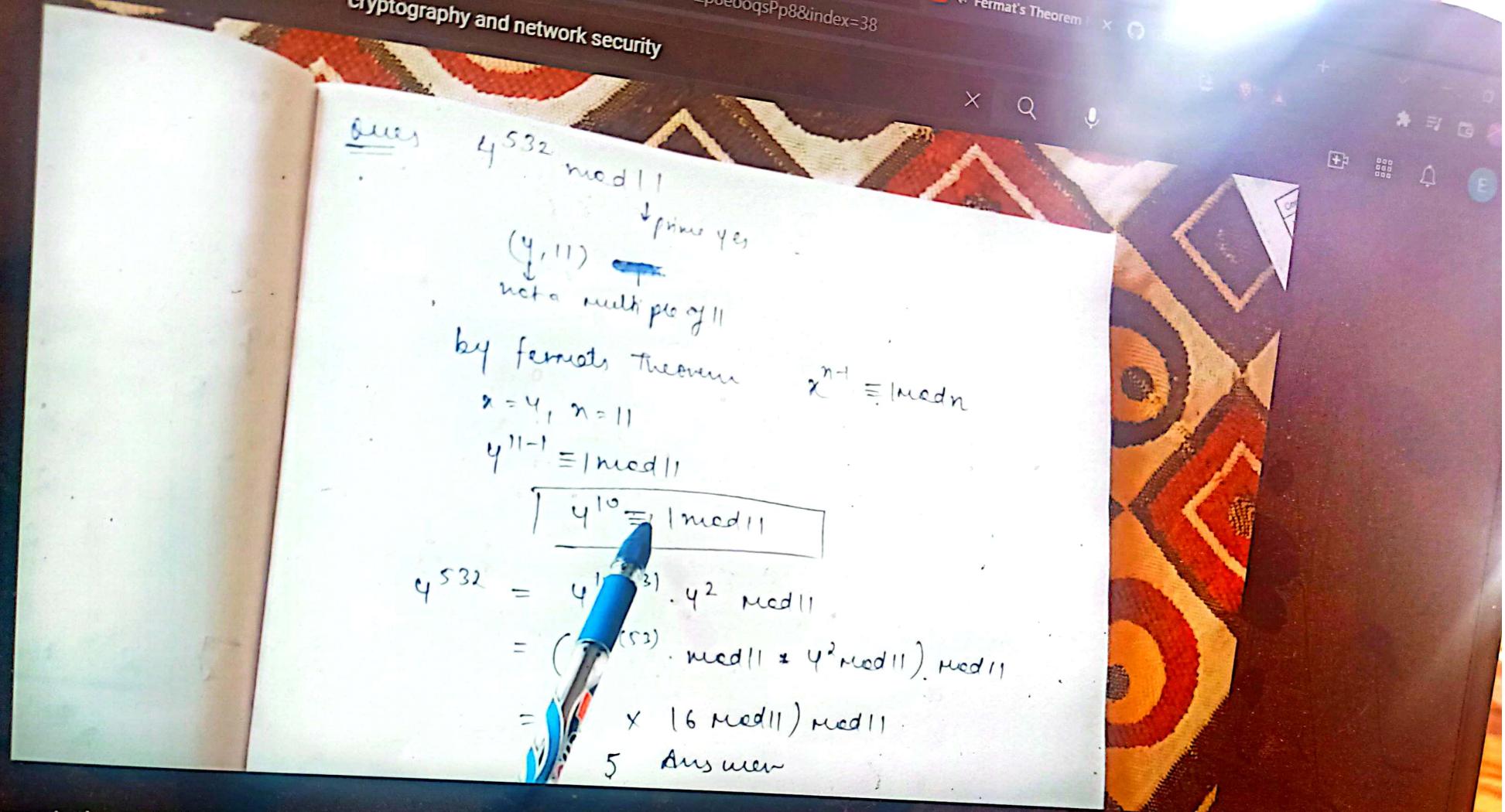
1.2K DISLIKE SHARE THANKS CLIP SAVE ...

Cryptography and network security
Abhishek Sharma - 38 / 70

41% 38°C Smoke 12:03 ENG 06-05-2022

OPPO Reno2 F

ideapad GAMING



Numerical examples | Important for exams

019

1.2K

DISLIKE

SHARE

THANKS

CLIP

SAVE

Cryptography and network security

Abhishek Sharma - 38 / 70



38°C Smoke ENG 06-05-2022

OPPO Reno2 F

apadGAMING

Scanned with CamScanner



OPPO Reno2 F

CHINESE REMAINDER THEOREM

Chinese Remainder theorem states that there always exists an "x" that satisfies the given congruence.

$$x \equiv \text{rem}[0] \pmod{\text{num}[0]}$$

$$x \equiv \text{rem}[1] \pmod{\text{num}[1]}$$

and $(\text{num}[0], \text{num}[1], \dots, \text{num}[m-1])$ must be coprime to one another.

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned} \quad \rightarrow \quad 5 \text{ and } 7 \text{ are coprime}$$

Theorem

with NUMERICAL in Cryptography | Abhishek Sharma

OPPO Reno2 F

3.7K DISLIKE

SHARE

THANKS



CLIP

SAVE

...

Cryptography and network security

Abhishek Sharma - 40 / 70



cryptography and network security

X Q



$$x = \text{rem}[1] \pmod{\text{num}[1]}$$

and $(\text{num}[0], \text{num}[1], \dots, \text{num}[m-1])$ must be coprime to each other.
one another.

eg.

$$x \equiv 1 \pmod{5}$$

$$x \equiv 3 \pmod{7} \rightarrow 5 \text{ and } 7 \text{ are coprime}$$

we have to find this $x = 31$

eg

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 1 \pmod{5}$$

$$\begin{aligned} \gcd(3, 4) &= \gcd(4, 1) \\ &= \gcd(3, 1) = 1 \end{aligned}$$

Then only x exists.

$$\text{here } x = 11$$

to find such

OPPO Reno2 F

eorem

NUMERICAL in Cryptography and Network Security



find no. of ~~books~~/books

if. Explain Chinese Remainder Theorem

$$\textcircled{x} \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

$$(i) \quad \gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$$

ie all coprime

$$(ii) \quad x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3 + \dots + M_n x_n a_n) \pmod{M}$$

$$M = m_1 * m_2 * m_3 * \dots * m_n$$

$$M_i^{\circ} = \frac{M}{m_i} \quad \text{eg} \quad M_1 = \frac{M}{m_1} = m$$

$$\therefore M_1 = m$$

4:56



@RemainderTheorem

orem with NUMERICAL in Cryptography | Abhishek Sharma

OPPO Reno2 F 7K

DISLIKE

SHARE

THANKS

CLIP

SAVE

...

Cryptography and network security

Abhishek Sharma - 40 / 70



74%

41°C Smoke

ENG

cryptography and network security

If $\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \end{aligned}$ Chinese Remainder Theorem

(i) $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1$
ie all coprime

(ii) $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3 + \dots + M_n x_n a_n) \pmod{M}$

$$M = m_1 * m_2 * m_3 * \dots * m_n$$

$$M_i = \frac{M}{m_i} \quad \text{eg} \quad M_1 = \frac{M}{m_1} = \frac{m_1 * m_2 * m_3}{m_1} = m_2 * m_3$$

$$\therefore M_1 = m_2 * m_3$$

Similarly $M_2 = m_1 * m_3$

" $M_3 = m_1 * m_2$

Multiplicative inverse of M_i

Theorem

OPPO Reno2 Fphy | Abhishek Sharma

3.7K

DISLIKE

SHARE

THANKS

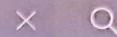
CLIP

SAVE

...

Cryptography and network security

Abhishek Sharma - 40 / 70



$$\boxed{M_i = \frac{M}{m_i}} \quad \text{eg} \quad M_1 = \frac{M}{m_1} = \frac{m_1 m_2 m_3}{m_1} = m_2 m_3$$

$$\therefore \boxed{M_1 = m_2 m_3}$$

Similarly $\rightarrow M_2 = m_1 m_3 = \frac{M}{m_2} = m_1 \cancel{m_2} m_3 = m_1 m_3$

" $M_3 = m_1 m_2$

To calculate $\boxed{X_i^o}$ \rightarrow multiplicative inverse of $\boxed{M_i}$

$$\boxed{M_i^o (X_i^o)} \equiv 1 \pmod{m_i}$$

$$\text{eg} \quad M_1 X_1^o \equiv 1 \pmod{m_1}$$



cryptography and network security



17

another. So, we can find x
 i.e. $\text{gcd}(5, 7) = \text{gcd}(7, 11) = \text{gcd}(11, 5) = 1$

$$\underline{M} = m_1 * m_2 * m_3 = 5 * 7 * 11 = 385$$

$$\boxed{M = 385}$$

$$M_1 = \frac{M}{m_1} = m_2 * m_3 = 7 * 11 = 77$$

$$M_2 = m_1 * m_3 = 5 * 11 = 55$$

$$M_3 = m_1 * m_2 = 5 * 7 = 35$$

$$\left. \begin{array}{l} M_1 = 77 \\ M_2 = 55 \\ M_3 = 35 \end{array} \right\}$$

Now we will calculate x_i value

$$M_1 x_1 = 1 \pmod{m_1} \quad \text{i.e. } M_1 x_1 \pmod{m_1} = 1$$

$$77 \cdot x_1 \pmod{m_1} = 1$$

$$\pmod{m_2}$$

OPPO Reno2 F

theorem

NUMERICAL in Cryptography | Abhishek Sharma

3.7K DISLIKE

SHARE

THANKS

CLIP

SAVE

...

Cryptography and network security

Abhishek Sharma - 40 / 70

14:37
06-05-2022

74%

41°C Smoke





cryptography and network security



$$M_1 = \frac{M}{m_1} = m_2 m_3 = 7 * 11 = 77$$

$$M_2 = m_1 m_3 = 5 * 11 = 55$$

$$M_3 = m_1 m_2 = 5 * 7 = 35$$

$$M_1 = 77$$

$$M_2 = 55$$

$$M_3 = 35$$

$$+ M_n x_n \text{ mod } M$$

Now we will calculate x_i value

$$M_1 x_1 \equiv 1 \pmod{m_1} \text{ ie } M_1 x_1 \pmod{m_1} = 1$$

$$77 \cdot x_1 \pmod{5} = 1$$

$$2 \cdot x_1 \pmod{5} = 1$$

$$\therefore x_1 = 3$$

$$= m_2 m_3$$

$$\frac{M_1 M_2 M_3}{m_2} = M_1 M_3$$

$$n \text{ of } M_i$$

$$\text{Similarly } M_2 x_2 \equiv 1 \pmod{m_2}$$

$$55 \cdot x_2 \pmod{7} = 1$$

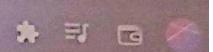
$$6 \cdot x_2 \pmod{7} = 1$$

$$\therefore x_2 = 6$$

we have to find
value such
that
value

multiple + 1) ho





cryptography and network security



Now we will calculate x_1 value.

$$M_1 x_1 \equiv 1 \pmod{m_1} \text{ ie } M_1 x_1 \pmod{m_1} = 1$$

$$\begin{aligned} 7 &\quad x_1 \pmod{5} = 1 \\ 2 &\quad x_1 \pmod{5} = 1 \end{aligned}$$

$$\therefore x_1 = 3$$

$$n \pmod{M}$$

$$n_2 m_3$$

$$n_3 = M_1 a_3$$

$$M_i$$

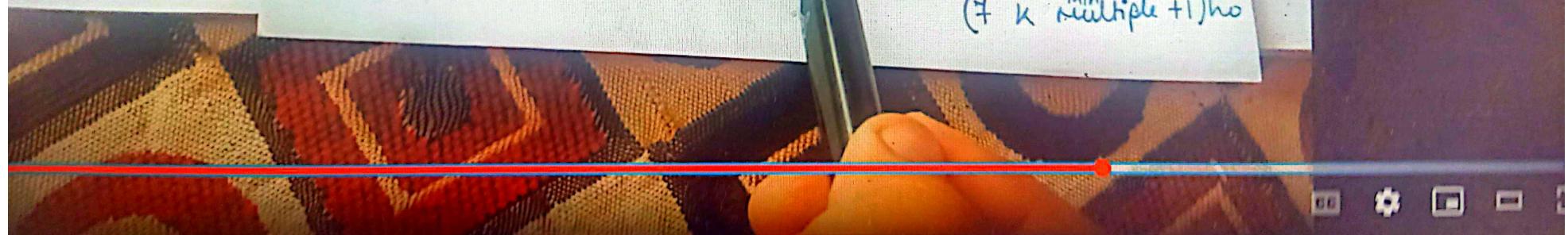
Similarly $M_2 x_2 \equiv 1 \pmod{m_2}$

$$55 x_2 \pmod{7} = 1$$

$$6 x_2 \pmod{7} = 1$$

$$\boxed{x_2 = 6}$$

} we have to find
a value such
that
 $6 * x_2$ at value
(7 k multiple + 1) no



Theorem

NUMERICAL in Cryptography | Abhishek Sharma

OPPO Reno2 F

DISLIKE

SHARE

THANKS

CLIP

SAVE

...

Cryptography and network security

Abhishek Sharma • 40 / 70



73%

14:37 41°C Smoke ENG 06-05-2021

cryptography and network security



$$35 x_3 \equiv 1 \pmod{11}$$

$$2 x_3 \equiv 1 \pmod{11}$$

$$2 x_3 \pmod{11} = 1$$

$$\therefore x_3 = 6$$

Now,

$$a_1 = a_2 = 1, a_3 = 3$$

$$m_1 = 5, m_2 = 7$$

$$M_1 = 77, M_2 = 55$$

$$x_1 = 3, x_2 = 6$$

$$m_3 = 11$$

$$M_3 = 35$$

$$M = 385$$

$$x = 6$$

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod{M}$$

$$x = (77(3)(1) + 55(6)(1) + 35(6)(3)) \pmod{385}$$

$$x = (231 + 330 + 630) \pmod{385}$$

$$x = 1191 \pmod{385}$$

LIGHT
56

CC G

$$\therefore \boxed{x_3 = 6}$$

Now,

$$a_1 = a_2 = 1$$

$$m_1 = 5 \quad a_3 = 3$$

$$M_1 = 77 \quad M_2 = 55$$

$$x_1 = 3 \quad x_2 = 6$$

$$m_3 = 11$$

$$M_3 = 35 \quad M = 385$$

$$x_3 = 6$$

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \text{ mod } M$$

$$x = (77(3)(1) + 55(6)(1) + 35(6)(3)) \text{ mod } 385$$

$$x = (231 + 330 + 630) \text{ mod } 385$$

$$x = 1191 \text{ mod } 385$$

$$\boxed{x = 6}$$

calculator

cryptography and network security

X Q

$$\begin{aligned}x &= (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \text{ mod } M \\x &= (77(3)x_1 + 55(6)x_2 + 35(1)x_3) \text{ mod } M \\x &= (231 + 330 + 630) \text{ mod } 385 \\x &= 1191 \text{ mod } 385\end{aligned}$$

$$\boxed{x = 36}$$

If u dont have calculator

$$1191 - 385 = 806$$

$$806 - 385 = 421$$

and

\because we can verify any

$$36 \text{ mod } 5 = 1$$

$$36 \text{ mod } 7 = 1$$

$$36 \text{ mod } 3 = 0$$

$$421 - 385 = 36 \text{ ans}$$



cryptography and network security

NUMerical Chinese Remainder
Theorem

$$\pmod{5}$$

$$x \equiv a_1 \pmod{m_1}$$

$$\pmod{7}$$

$$\rightarrow \text{so } a_1 = 1, a_2 = 1, a_3 = 2$$

$$\pmod{11}$$

$$m_1 = 5, m_2 = 7, m_3 = 11$$

5, 7 and 11 all are relatively prime to one
another, so, we can find x

$$\gcd(5, 7) = \gcd(7, 11) = \gcd(11, 5) = 1$$

$$m_2 + m_3 = 5 * 7 + 11 = 385$$

$$\rightarrow M = 385$$

$$= m_2 m_3 = 7 * 11 = 77$$

$$m_3 = 5 * 11 = 55$$

$$l_1 = 5 * 7 = 35$$

will calculate x_1 value.

$$x_1 \equiv 1 \pmod{m_1} \text{ ie } M_1 x_1 \pmod{m_1} = 1$$

$$\pmod{5} = 1$$

$$\pmod{5} = 1$$

$$\equiv 1 \pmod{m_2}$$

F

OPPO Reno2 F

Theorem with NUMERICAL in Cryptography | Abhishek Sharma

CHINESE REMAINDER THEOREM

Chinese Remainder theorem states that there always exists an "x" that satisfies the given congruence.

$$x \equiv \text{rem}[0] \pmod{\text{num}[0]}$$

$$x \equiv \text{rem}[1] \pmod{\text{num}[1]}$$

and $(\text{num}[0], \text{num}[1])$ must be coprime to
~~etc etc~~
all one another.

eg:

$$x \equiv 1 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

5 and 7 are coprime

we have to find this $x = 31$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 2 \pmod{4}$$

$$x \equiv 1 \pmod{5}$$

$$\gcd(3, 4) = \gcd(4, 5)$$

$$= \gcd(3, 5) = 1$$

cryptography and network security

X Q

We will use asymmetric encryption to exchange secret keys between 2 users. We need two secret keys for two users.

(public & private key concept)

Why this algo?

bcz when we are sending a key to receiver, it can be attacked in b/w.

ALGORITHM

- consider a prime number 'q'
- select α such that it must be the primitive root of q and $\alpha < q$

' α ' is a primitive root of q if

$$\alpha^1 \pmod{q}$$

$$\alpha^2 \pmod{q}$$

$$\alpha^3 \pmod{q}$$

$$\dots \alpha^{q-1} \pmod{q}$$

gives results {

{ }
 $q-1$

i.e. Value

no

repeated & we should
in the off set

Internship | SIP 2

Inbox (3,627) - goyaljatin13

Inbox (315) - goyaljatin110

Classes

Assignment-II.pdf - Google

GitHub

YouTube IN

youtube.com/watch?v=zLNug0LrFiU&list=PL9FuOtXibFjV77w2eyiI4Xzp8eoqsPp8&index=41

Diffi Hellman Key

cryptography and network security

to ex

x_2

x_7

x_1

x_2

x_7

x_8

x_9

x_{10}

x_{11}

x_{12}

x_{13}

x_{14}

x_{15}

x_{16}

x_{17}

x_{18}

x_{19}

x_{20}

x_{21}

x_{22}

x_{23}

x_{24}

x_{25}

x_{26}

x_{27}

x_{28}

x_{29}

x_{30}

x_{31}

x_{32}

x_{33}

x_{34}

x_{35}

x_{36}

x_{37}

x_{38}

x_{39}

x_{40}

x_{41}

x_{42}

x_{43}

x_{44}

x_{45}

x_{46}

x_{47}

x_{48}

x_{49}

x_{50}

x_{51}

x_{52}

x_{53}

x_{54}

x_{55}

x_{56}

x_{57}

x_{58}

x_{59}

x_{60}

x_{61}

x_{62}

x_{63}

x_{64}

x_{65}

x_{66}

x_{67}

x_{68}

x_{69}

x_{70}

x_{71}

x_{72}

x_{73}

x_{74}

x_{75}

x_{76}

x_{77}

x_{78}

x_{79}

x_{80}

x_{81}

x_{82}

x_{83}

x_{84}

x_{85}

x_{86}

x_{87}

x_{88}

x_{89}

x_{90}

x_{91}

x_{92}

x_{93}

x_{94}

x_{95}

x_{96}

x_{97}

x_{98}

x_{99}

x_{100}

x_{101}

x_{102}

x_{103}

x_{104}

x_{105}

x_{106}

x_{107}

x_{108}

x_{109}

x_{110}

x_{111}

x_{112}

x_{113}

x_{114}

x_{115}

x_{116}

x_{117}

x_{118}

x_{119}

x_{120}

x_{121}

x_{122}

x_{123}

x_{124}

x_{125}

x_{126}

x_{127}

x_{128}

x_{129}

x_{130}

x_{131}

x_{132}

x_{133}

x_{134}

x_{135}

x_{136}

x_{137}

x_{138}

x_{139}

x_{140}

x_{141}

x_{142}

x_{143}

x_{144}

x_{145}

x_{146}

x_{147}

x_{148}

x_{149}

x_{150}

x_{151}

x_{152}

x_{153}

x_{154}

x_{155}

x_{156}

x_{157}

x_{158}

x_{159}

x_{160}

x_{161}

x_{162}

x_{163}

x_{164}

x_{165}

x_{166}

x_{167}

x_{168}

x_{169}

x_{170}

x_{171}

x_{172}

x_{173}

x_{174}

x_{175}

x_{176}

x_{177}

x_{178}

x_{179}

x_{180}

x_{181}

x_{182}

x_{183}

x_{184}

x_{185}

x_{186}

x_{187}

x_{188}

x_{189}

x_{190}

x_{191}

x_{192}

x_{193}

x_{194}

x_{195}

x_{196}

x_{197}

x_{198}

x_{199}

x_{200}

x_{201}

x_{202}

x_{203}

x_{204}

x_{205}

x_{206}

x_{207}

x_{208}

x_{209}

x_{210}

x_{211}

x_{212}

x_{213}

x_{214}

x_{215}

x_{216}

x_{217}

x_{218}

x_{219}

x_{220}

x_{221}

x_{222}

x_{223}

x_{224}

x_{225}

x_{226}

x_{227}

x_{228}

x_{229}

x_{230}

x_{231}

x_{232}

x_{233}

x_{234}

x_{235}

x_{236}

x_{237}

x_{238}

x_{239}

x_{240}

x_{241}

x_{242}

x_{243}

x_{244}

x_{245}

x_{246}

x_{247}

x_{248}

x_{249}

x_{250}

x_{251}

x_{252}

x_{253}

x_{254}

x_{255}

x_{256}

x_{257}

x_{258}

x_{259}

x_{260}

x_{261}

x_{262}

x_{263}

x_{264}

x_{265}

x_{266}

x_{267}

x_{268}

x_{269}

x_{270}

x_{271}

x_{272}

x_{273}

x_{274}

x_{275}

x_{276}

x_{277}

x_{278}

x_{279}

x_{280}

x_{281}

x_{282}

x_{283}

x_{284}

x_{285}

x_{286}

x_{287}

x_{288}

x_{289}

x_{290}

x_{291}

x_{292}

x_{293}

x_{294}

x_{295}

x_{296}

x_{297}

x_{298}

x_{299}

x_{300}

x_{301}

x_{302}

x_{303}

x_{304}

x_{305}

x_{306}

x_{307}

x_{308}

x_{309}

x_{310}

x_{311}

x_{312}

x_{313}

x_{314}

x_{315}

x_{316}

x_{317}

x_{318}

x_{319}

x_{320}

x_{321}

x_{322}

x_{323}

x_{324}

x_{325}

x_{326}

x_{327}

x_{328}

x_{329}

x_{330}

x_{331}

x_{332}

x_{333}

x_{334}

x_{335}

x_{336}

x_{337}

x_{338}

x_{339}

x_{340}

x_{341}

x_{342}

x_{343}

x_{344}

x_{345}

x_{346}

x_{347}

x_{348}

x_{349}

x_{350}

x_{351}

x_{352}

x_{353}

x_{354}

x_{355}

x_{356}

x_{357}

x_{358}

x_{359}

x_{360}

x_{361}

x_{362}

x_{363}

x_{364}

x_{365}

x_{366}

x_{367}

x_{368}

x_{369}

x_{370}

x_{371}

x_{372}

x_{373}

x_{374}

x_{375}

x_{376}

x_{377}

x_{378}

x_{379}

x_{380}

x_{381}

x_{382}

x_{383}

x_{384}

x_{385}

x_{386}

x_{387}

x_{388}

x_{389}

x_{390}

x_{391}

x_{392}

x_{393}

x_{394}

x_{395}

x_{396}

x_{397}

x_{398}

x_{399}

x_{400}

x_{401}

x_{402}

x_{403}

x_{404}

x_{405}

x_{406}

x_{407}

x_{408}

x_{409}

x_{410}

x_{411}

x_{412}

x_{413}

x_{414}

x_{415}

x_{416}

x_{417}

x_{418}

x_{419}

x_{420}

x_{421}

x_{422}

x_{423}

x_{424}

x_{425}

x_{426}

x_{427}

x_{428}

x_{429}

x_{430}

x_{431}

x_{432}

x_{433}

x_{434}

x_{435}

x_{436}

x_{437}

x_{438}

x_{439}

x_{440}

x_{441}

x_{442}

x_{443}

x_{444}

x_{445}

x_{446}

x_{447}

x_{448}

x_{449}

x_{450}

x_{451}

x_{452}

x_{453}

x_{454}

x_{455}

x_{456}

x_{457}

x_{458}

x_{459}

x_{460}

x_{461}

x_{462}

x_{463}

x_{464}

x_{465}

x_{466}

x_{467}

x_{468}

x_{469}

x_{470}

x_{471}

x_{472}

x_{473}

x_{474}

x_{475}

x_{476}

x_{477}

x_{478}

x_{479}

x_{480}

x_{481}

x_{482}

x_{483}

x_{484}

x_{485}

x_{486}

x_{487}

x_{488}

x_{489}

x_{490}

x_{491}

x_{492}

x_{493}

x_{494}

x_{495}

x_{496}

x_{497}

x_{498}

x_{499}

x_{500}

x_{501}

x_{502}

x_{503}

x_{504}

x_{505}

x_{506}

x_{507}

x_{508}

x_{509}

x_{510}

x_{511}

x_{512}

x_{513}

x_{514}

x_{515}

x_{516}

x_{517}

x_{518}

x_{519}

x_{520}

x_{521}

x_{522}

x_{523}

x_{524}

x_{525}

x_{526}

x_{527}

x_{528}

x_{529}

x_{530}

x_{531}

x_{532}

x_{533}

x_{534}

x_{535}

x_{536}

x_{537}

x_{538}

x_{539}

x_{540}

x_{541}

x_{542}

x_{543}

x_{544}

x_{545}

x_{546}

x_{547}

x_{548}

x_{549}

x_{550}

x_{551}

x_{552}

x_{553}

x_{554}

x_{555}

x_{556}

x_{557}

x_{558}

x_{559}

x_{560}

x_{561}

x_{562}

x_{563}

x_{564}

x_{565}

x_{566}

x_{567}

x_{568}

x_{569}

x_{570}

x_{571}

x_{572}

x_{573}

x_{574}

x_{575}

x_{576}

x_{577}

x_{578}

x_{579}

x_{580}

x_{581}

x_{582}

x_{583}

x_{584}

x_{585}

x_{586}

x_{587}

x_{588}

x_{589}

x_{590}

x_{591}

x_{592}

x_{593}

x_{594}

x_{595}

x_{596}

x_{597}

x_{598}

x_{599}

x_{600}

x_{601}

x_{602}

x_{603}

x_{604}

x_{605}

x_{606}

x_{607}

x_{608}

x_{609}

x_{610}

x_{611}

x_{612}

x_{613}

x_{614}

x_{615}

x_{616}

x_{617}

x_{618}

x_{619}

x_{620}

x_{621}

x_{622}

x_{623}

x_{624}

x_{625}

x_{626}

x_{627}

x_{628}

x_{629}

x_{630}

x_{631}

x_{632}

x_{633}

x_{634}

x_{635}

x_{636}

x_{637}

x_{638}

x_{639}

x_{640}

x_{641}

x_{642}

x_{643}

x_{644}

x_{645}

x_{646}

x_{647}

x_{648}

x_{649}

x_{650}

x_{651}

x_{652}

x_{653}

x_{654}

x_{655}

x_{656}

x_{657}

x_{658}

x_{659}

x_{660}

x_{661}

x_{662}

x_{663}

x_{664}

x_{665}

x_{666}

x_{667}

x_{668}

x_{669}

x_{670}

x_{671}

x_{672}

x_{673}

x_{674}

x_{675}

x_{676}

x_{677}

x_{678}

x_{679}

x_{680}

x_{681}

x_{682}

x_{683}

x_{684}

x_{685}

x_{686}

x_{687}

x_{688}

x_{689}

x_{690}

x_{691}

x_{692}

x_{693}

x_{694}

x_{695}

x_{696}

x_{697}

x_{698}

x_{699}

x_{700}

x_{701}

x_{702}

x_{703}

x_{704}

x_{705}

x_{706}

x_{707}

x_{708}

x_{709}

x_{710}

x_{711}

x_{712}

x_{713}

x_{714}

x_{715}

x_{716}

x_{717}

x_{718}

x_{719}

x_{720}

x_{721}

x_{722}

x_{723}

x_{724}

x_{725}

x_{726}

x_{727}

x_{728}

x_{729}

x_{730}

x_{731}

x_{732}

x_{733}

x_{734}

x_{735}

x_{736}

x_{737}

x_{738}

x_{739}

x_{740}

x_{741}

x_{742}

x_{743}

x_{744}

x_{745}

x_{746}

x_{747}

x_{748}

x_{749}

x_{750}

x_{751}

x_{752}

x_{753}

x_{754}

x_{755}

x_{756}

x_{757}

x_{758}

x_{759}

x_{760}

x_{761}

x_{762}

x_{763}

x_{764}

x_{765}

x_{766}

x_{767}

x_{768}

x_{769}

x_{770}

x_{771}

x_{772}

x_{773}

x_{774}

x_{775}

x_{776}

x_{777}

x_{778}

x_{779}

x_{780}

x_{781}

x_{782}

x_{783}

x_{784}

x_{785}

x_{786}

x_{787}

x_{788}

x_{789}

x_{790}

x_{791}

x_{792}

x_{793}

x_{794}

x_{795}

x_{796}

x_{797}

x_{798}

x_{799}

x_{800}

x_{801}

x_{802}

x_{803}

x_{804}

x_{805}

x_{806}

x_{807}

x_{808}

x_{809}

x_{810}

x_{811}

x_{812}

x_{813}

x_{814}

x_{815}

x_{816}

x_{817}

x_{818}

x_{819}

x_{820}

x_{821}

x_{822}

x_{823}

x_{824}

x_{825}

x_{826}

x_{827}

x_{828}

x_{829}

x_{830}

x_{831}

x_{832}

x_{833}

x_{834}

x_{835}

x_{836}

x_{837}

x_{838}

x_{839}

x_{840}

x_{841}

x_{842}

x_{843}

x_{844}

x_{845}

x_{846}

x_{847}

x_{848}

x_{849}

x_{850}

x_{851}

x_{852}

x_{853}

x_{854}

x_{855}

x_{856}

<

to calculate $Y_A = \alpha^{x_A} \text{ mod } q$
 public key of A

(ii) assume x_B (private of B)

calculate $Y_B = \alpha^{x_B} \text{ mod } q$
 public key of B

$x_B < q$

Now we will calculate secret key

To calculate the secret keys, both the sender & receiver will use public keys.

$$K_A = (Y_B)^{x_A} \text{ mod } q$$

public keys known to all

$$K_B = (Y_A)^{x_B} \text{ mod } q$$

$K_1 = K_2$ then we say exchange is successful.

o/o

goyaljatin3 Gmail Inbox (315) - goyaljatin110 Classes Assignment-II.pdf - Google Docs GitHub

ube.com/watch?v=zLNug0LrFiU&list=PL9FuOtXibFjV77w2eyil4Xzp8eo0qsPp8&index=41 Diffie Hellman Key Exchange

cryptography and network security

Diffie - Hellman key exchange algorithm

- (i) not an encryption algo.
- (ii) used to exchange secret keys between 2 users
- (iii) we will use asymmetric encryption to exchange the secret key b/w users.
(public & private key concept)

yo this algo?
b/c when we are sending a key to receiver, it can be attacked in b/w.

ALGORITHM

- (i) consider a prime number ' q '
- (ii) select α such that it must be the primitive root of q and $\alpha < q$

a is a primitive root of q if

$a \text{ mod } q$
 $a^2 \text{ mod } q$

9/1/2020

CC

OPPO Reno2 F

cryptography and network security



es)

algorithm

st



How secure?

Why this algo?

bc when we are sending a key to receiver, it can be attacked in b/w.

↓ exchange
(public & private key concept)

ALGORITHM

- (i) consider a prime number ' q '
- (ii) select α such that it must be the primitive root of q and $\alpha < q$

→ α is a primitive root of q if

$$\alpha \text{ mod } q$$

$$\alpha^2 \text{ mod } q$$

$$\alpha^3 \text{ mod } q$$

$$\dots$$

$$\dots \text{ mod } q$$

gives results $\{1, 2, 3, \dots, q-1\}$

i.e. values shouldn't be repeated & we should have all the off set (see example).



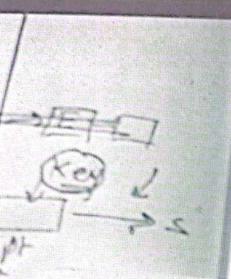
cryptography and network security

X Q

3 < 7 yes)

17

Both of them
don't need any info from
anyone. They
just use
 α and q ,
which are
known.



other key
two users

why this algo?

H/C When we are sending a key to receiver, it
can be attacked in b/w.

key exchange

(public & private
key concept)

Deffie Hellman key exchange algorithm

calculating primitive root

$$\begin{aligned} 3^1 \bmod 7 &= 3 \\ 3^2 \bmod 7 &= 2 \\ 3^3 \bmod 7 &= 6 \\ 3^4 \bmod 7 &= 4 \\ 3^5 \bmod 7 &= 5 \\ 3^6 \bmod 7 &= 1 \end{aligned} \quad \left. \right\} \quad \alpha = 3$$

'q'
must be the primitive

1

2 4

mod q

1 }

repeated & we should
in the off set

(show example).

15:24

OPPO Reno2 F

workSecurity

cryptography and network security

X Q

algorithm

of

$$\underline{q = 7}$$

Let $q = 7$ (prime) $\alpha < q$ i.e. it is a primitive root

$$\boxed{\alpha = 5}$$

we can take any of the two
primitive root 3 or 5. α and $q \rightarrow$ global public elements (known to everyone)

will sh - Diffie

 \rightarrow private key of us
 \rightarrow public key of us
(y) and $X_A < q$ Key generation of person 1Assume private key $\boxed{X_A = 3}$
 $(X_A < q$
 $3 < 7$ yes)
calculating public key $Y_A = \alpha^{X_A} \bmod q$

$$Y_A = 5^3 \bmod 7 = 125 \bmod 7$$

$$\boxed{Y_A = 1}$$

key generation of person 2let private key $X_B = 4$ $(X_B < q)$

Both of them
don't need any
info from
anyone. They
just
use
 α and q .

secret key

secret keys, both

will use public

calculating public key $Y_B = \alpha^{X_B} \bmod q$

$$Y_B = 5^4 \bmod 7 = 625 \bmod 7$$

$$\boxed{Y_B = 1}$$

(show current
scenario
diagram?)

$$K_2 = (Y_A)^{X_B} \bmod q$$

OPPO Reno2 F

key calculation by person 2

cryptography and network security

Diffi Hellman Key Exchange

X
Y(3) assume X_A (private key of A)

calculate $Y_A = \alpha^{X_A} \text{ mod } q$
 \downarrow
 public key of A

(4) assume X_B (private key of B)

calculate $Y_B = \alpha^{X_B} \text{ mod } q$
 \downarrow
 public key of B

Now we will calculateTo calculate the secret key between two persons

3/15:24

OPPO Reno2 F

#NetworkSecurity

Change Algorithm | Cryptography and Network Security

$\alpha < q$ i.e. it is a primitive root
 let $\alpha = 5$

we can take any of the two
 primitive root 3 or 5.

α and $q \rightarrow$ global public elements (known to everyone)

Key generation of person 1

Assume private key $X_A = 3$ $\therefore (X_A < q, 3 \neq 1 \text{ or } q)$

calculating public key $Y_A = \alpha^{X_A} \text{ mod } q$

$Y_A = 5^3 \text{ mod } 7 = 125 \text{ mod } 7$

$Y_A = 1$

Both of them
 don't need any
 info from
 anyone. They
 $(X_B < q)$ just
 use
 α and q ,
 which are
 known to
 all.

key generation of person 2

Let private key $X_B = 4$

calculating public key $Y_B = \alpha^{X_B} \text{ mod } q$

$Y_B = 5^4 \text{ mod } 7 = 625 \text{ mod } 7 = 1$

$Y_B = 1$

(show current
 scenario
 diagram)

Secret key calculation
 by person 1

by person 2.



cryptography and network security

let $\alpha = 5$

\rightarrow a primitive root
we can take any of the two
primitive root 3 or 5.

α and $q \rightarrow$ global public elements (known to everyone)

Key generation of persons

Assume private key $X_A = 3$ $\therefore X_A < q$

So current scenario

private key
 $X_A = 3$

global elements
 $q = 7$
 $\alpha = 5$

public keys
 $y_A = 6$
 $y_B = 2$

private key
 $X_B = 4$

(A)

person 1

(B)

person 2

$x \rightarrow$ public keys
 $y \rightarrow$ private keys

cryptography and network security

X Q

(4) a

calculating public key $Y_A = \alpha^{x_A} \text{ mod } q$ ($x_A < q$
 $3 < 7$ yes)

$$Y_A = 5^3 \text{ mod } 7 = 125 \text{ mod } 7$$

$$\boxed{Y_A = 6}$$

No. key generation of person 2
 Let private key $x_B = 4$

calculating public key $Y_B = \alpha^{x_B} \text{ mod } q$

$$Y_B = 5^4 \text{ mod } 7 = 625 \text{ mod } 7$$

$$\boxed{Y_B = 2}$$

Both of them don't need any info from anyone. They just use α and q , which are known to all.

(show current scenario diagram)

Secret key calculation by Alice/person 1

$$K_A = (Y_B)^{x_A} \text{ mod } q$$

$$= 2^3 \text{ mod } 7$$

$$= 8 \text{ mod } 7$$

$$\boxed{K = 1}$$

$$K_B = (Y_A)^{x_B} \text{ mod } q$$

$$K = 6^4 \text{ mod } 7$$

$$K = (1296 \text{ mod } 7) \text{ mod } 7$$

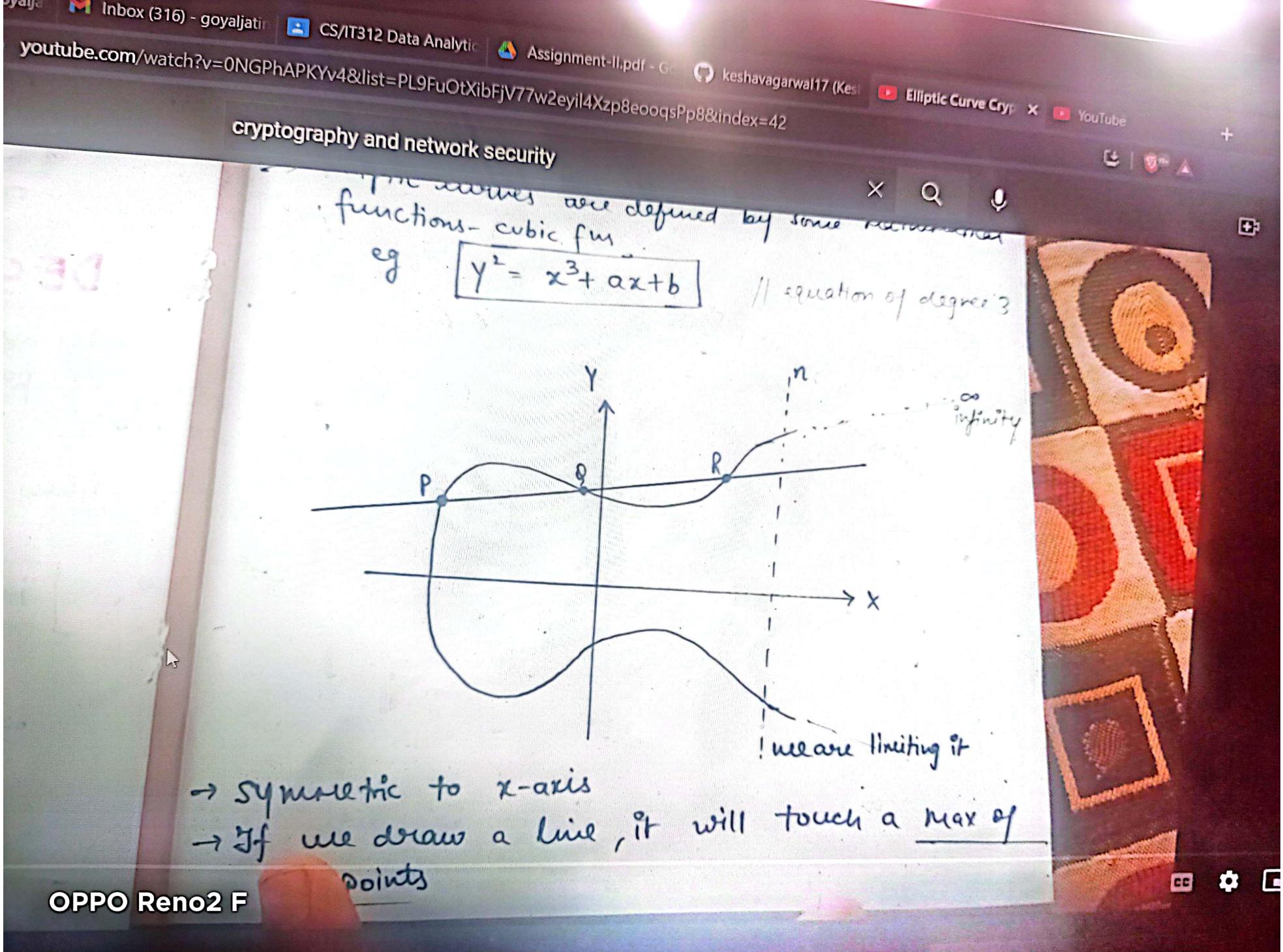
$$\boxed{K = 1}$$

Thus, the key is changed 😊

Elliptic Curve Cryptography

ECC

- It is asymmetric / public key cryptosystem.
- It provides equal security with smaller key size (eg: compared to RSA) as compared to non-ECC algos.
ie small key size and high security
- It makes use of Elliptic curves.
- Elliptic curves are defined by some mathematical functions - cubic fm.
eg $y^2 = x^3 + ax + b$ // equation of degree 3

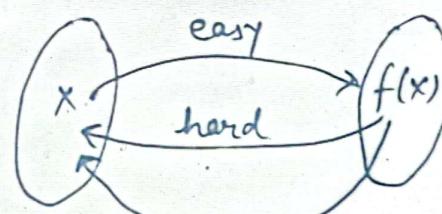


A Trapdoor function is a fn that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the trapdoor

a, b

the

se



easy if given "t" → trapdoor value.

$A \rightarrow B$

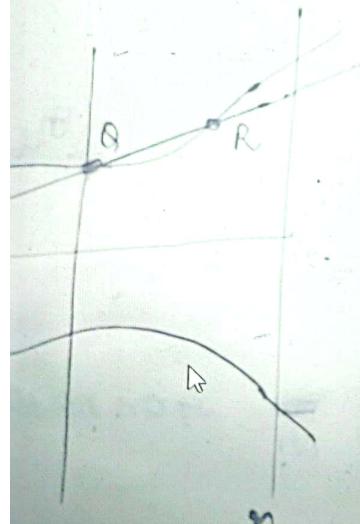
refer wikipedia for more details.

Let $E_p(a, b)$ be the elliptic curve
Consider the equation $Q = kP$
where $Q, P \rightarrow$ points on curve and $k \in \mathbb{N}$

If k and $P \rightarrow$ given, it should be easy to find Q
but if we know Q and P , it should be extremely difficult to find k .
ie. It is a one way fun. \rightarrow Trap door fun
This is called the discrete logarithm problem for elliptic curves

It is easy
 $B \rightarrow A$
difficult..

Algo is somewhat similar to



ECC - ALGORITHM

ECC - Key Exchange

Global Public Elements

$E_q(a, b)$: elliptic curve with parameters a, b and q

prime no. or an integer of the form 2^m .

G_1 : Point on the curve/elliptic curve whose order is large value of n

User A key generation

Select private key

$$\eta_A < n$$

calculate pub'

$$P_A$$

$$P_A = \eta_A \times G$$

$E_q(a, b)$

: elliptic curve with parameters a, b
and \boxed{q}

↓
prime no. or an integer of the
form 2^m .

G_1 : Point on the curve/elliptic curve whose
order is large value of n

User A key generation

Select private key n_A
calculate public key P_A

$$n_A < n$$
$$P_A = n_A \times G$$

User B key generation

Select private key n_B
calculate public key P_B

$$B < n$$
$$P_B = n_B \times G$$

Calculation of secret key K

$$K = n_A \times P_B$$

elliptic curve with parameters a, b
and q

prime no. or an integer of the
form 2^m .

G_1 : Point on the curve/elliptic curve whose
order is large value of n

User A key generation

Select private key n_A
calculate public key P_A

$$n_A < n$$
$$P_A = n_A \times G_1$$

User B key generation

Select private key n_B
calculate public key P_B

$$n_B < n$$
$$P_B = n_B \times G_1$$

Calculation of secret key by A:

$$K = n_A \times P_B$$

G₁: Point on the curve/elliptic curve whose order is large value of n

prime no. or an integer of the form 2^m .

User A key generation

Select private key n_A
calculate public key P_A

$$n_A < n$$
$$P_A = n_A \times G$$

User B key generation

Select private key n_B
calculate public key P_B

$$n_B < n$$
$$P_B = n_B \times G$$

Calculation of secret key by user A

$$K_A = K = n_A \times P_B$$

calculation of secret key by user B

$$K = n_B \times P_A$$

ECC ENCRYPTION

- Let the message be M .
- first encode this message M into a point on elliptic curve.
- Let this point be P_m .

Now this point is encrypted.

for encryption, chose a random positive integer k

The cipher point will be

$$C_m = \{ kG_1, P_m + kP_B \}$$

This point will be sent to the receiver

DECRIPTION

for decryption, multiply 1st point in the

YouTube

The cipher point will be

$$C_m = \{ kG_1, P_m + kP_B \}$$

This point will be sent to the receiver

DECRYPTION

for decryption, multiply 1st point in the pair with receiver's secret key

$$\text{i.e. } kG_1 * n_B \quad \text{[for decryption private key of } B \text{ used]}$$

Then subtract it from 2nd point/coordinate in the pair

$$\text{i.e. } P_m + kP_B - (kG_1 * n_B)$$

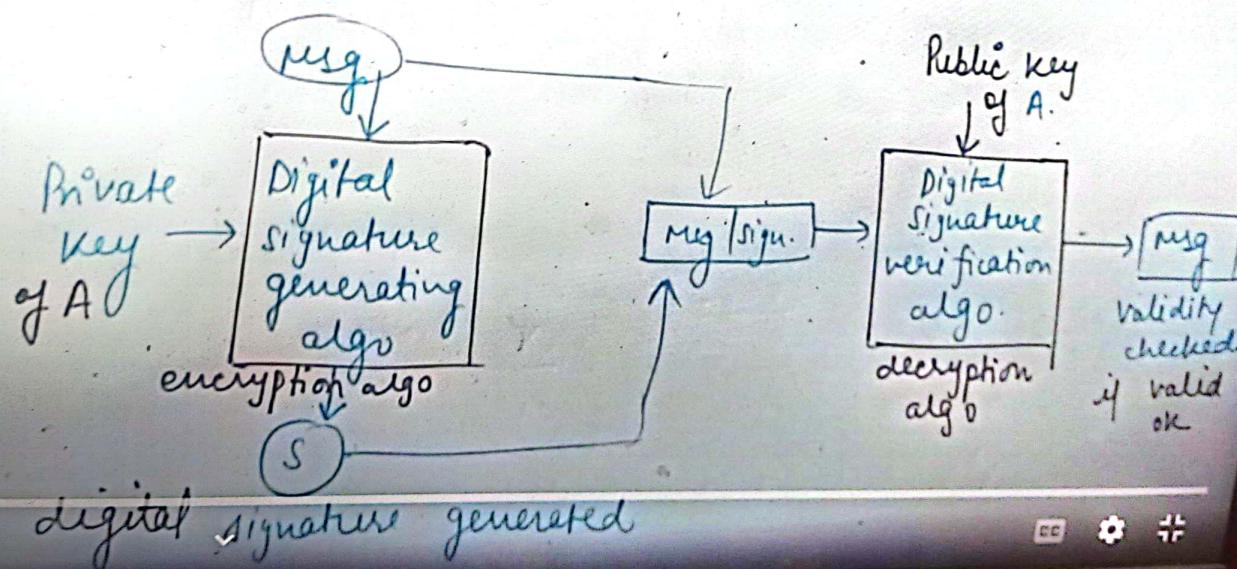
$$\text{but we know } P_B = n_B * G_1$$

$$\text{so } P_m + kP_B - kP_B$$

$$= P_m \quad \text{(original)}$$

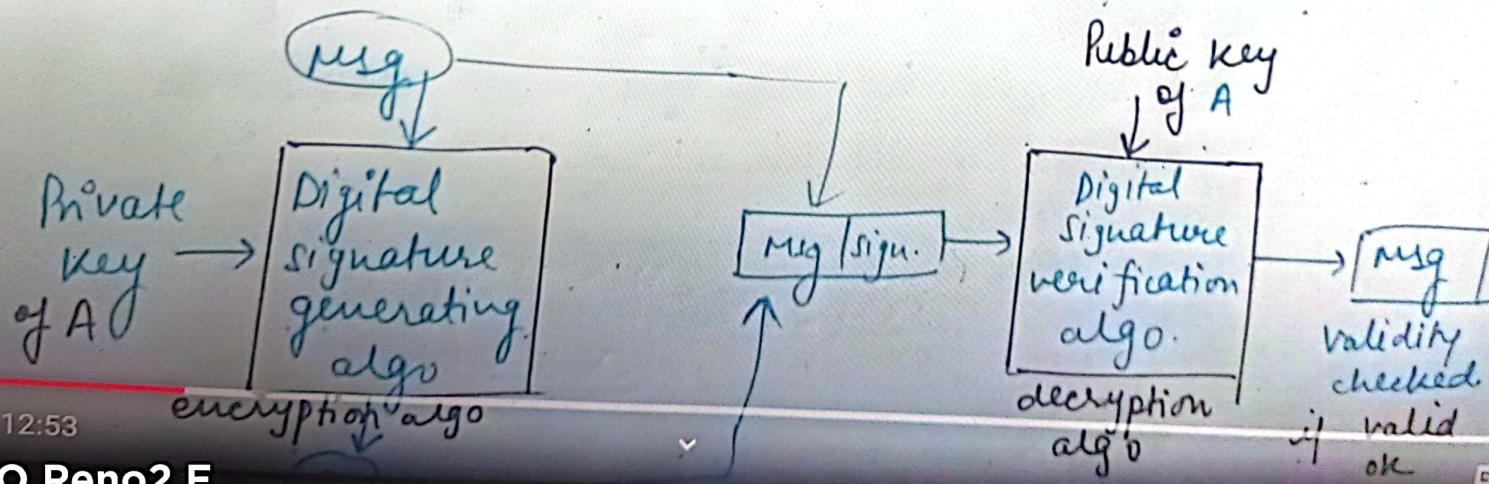
Digital signature

- rising role in e-commerce, online transaction, etc.
- based on asymmetric key cryptography
- encryption → private key
- decryption → public key
- used for msg authentication & non repudiation & msg integrity
- not used for confidentiality

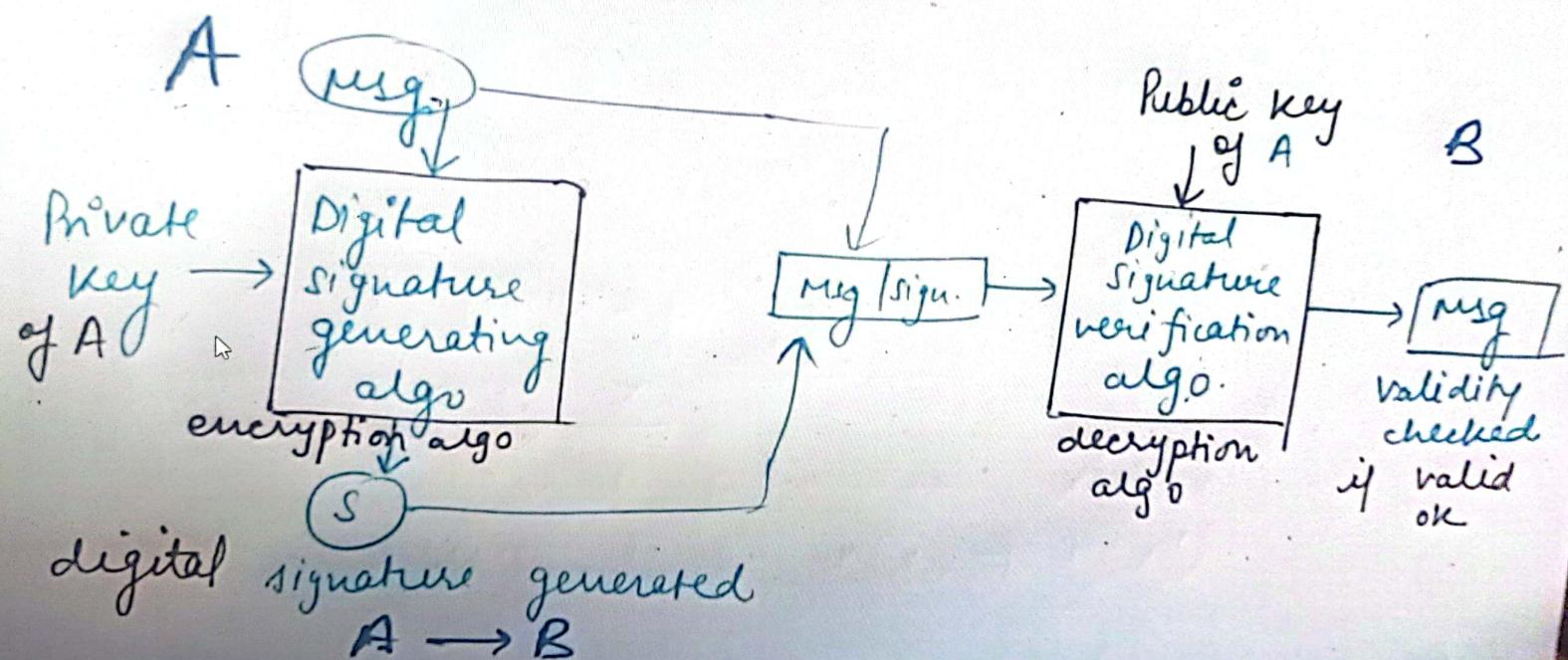


Digital signature

- very use in e-commerce, online transaction, etc.
- based on asymmetric key cryptography
 - decryption → private key
 - encryption → public key
- used for msg authentication & non repudiation & msg integrity
- not used for confidentiality



decryption → private key
 decryption → public key
 → used for msg authentication & non repudiation & msg integrity
 → not used for confidentiality



→ also provides msg integrity

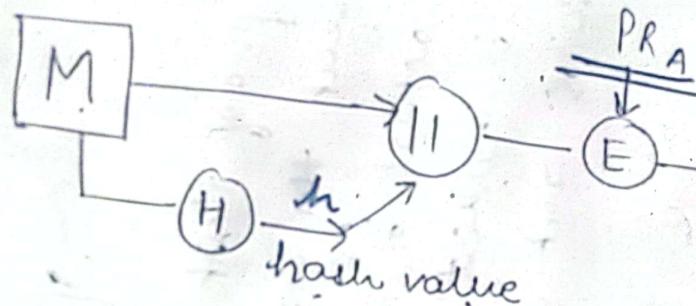
OPPO Reno2 F

b/c if msg changed then at receiver

Digital signature

Digital signature

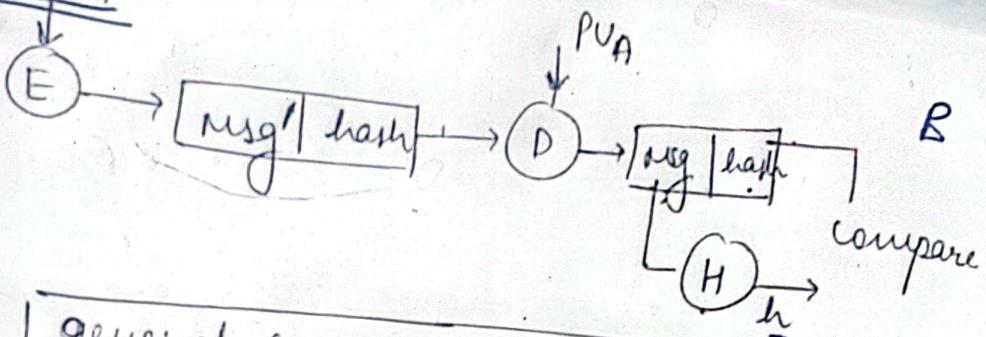
A



$H \rightarrow$ hash fn
 $h \rightarrow$ hash code
 $II \rightarrow$ append

private key of Alice is used.
authenticity achieved.

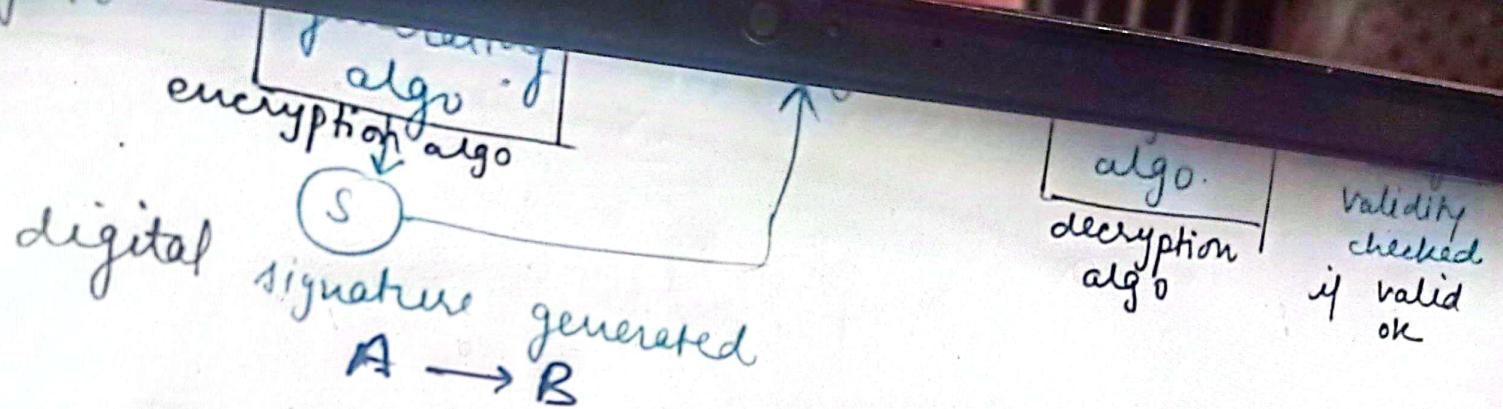
B



general concept of digital
signature

Note → The signature must use some info. unique to the sender to prevent both forgery & denial.

nature



→ also provides msg integrity
blk if msg changed then at receiver side, we will not get the exact msg.

achieved using Hashing
concept using msg digest/
hash values

Note → When we sign a document digitally,
= we send the signature as a separate
document.

OPPO Reno2 F
owner sends 2 docs → msg & signature.

Digital signature

Non repudiation

achieved by using a trusted 3rd party

Digital Signature

pg 351

pg 352

confidentiality

- signature must use some info unique to the sender, to prevent forgery & denial.
- It must be easy to produce digital signatures.
- " " " " to verify & recognize " " .
- we need (i) key generation algo → to generate private key
(ii) Signing Algo if P → M and Private key , o/p → Digital sign
(iii) verifying algo → using public key & sig

We are getting msg authentication?
Bob can verify that msg is sent by Alice b/c
Alice's public key is used in verification.
and we can get the same msg digest/hash value
only if ~~the~~ private key of Alice is used.
 \therefore authenticity achieved.

message Integrity

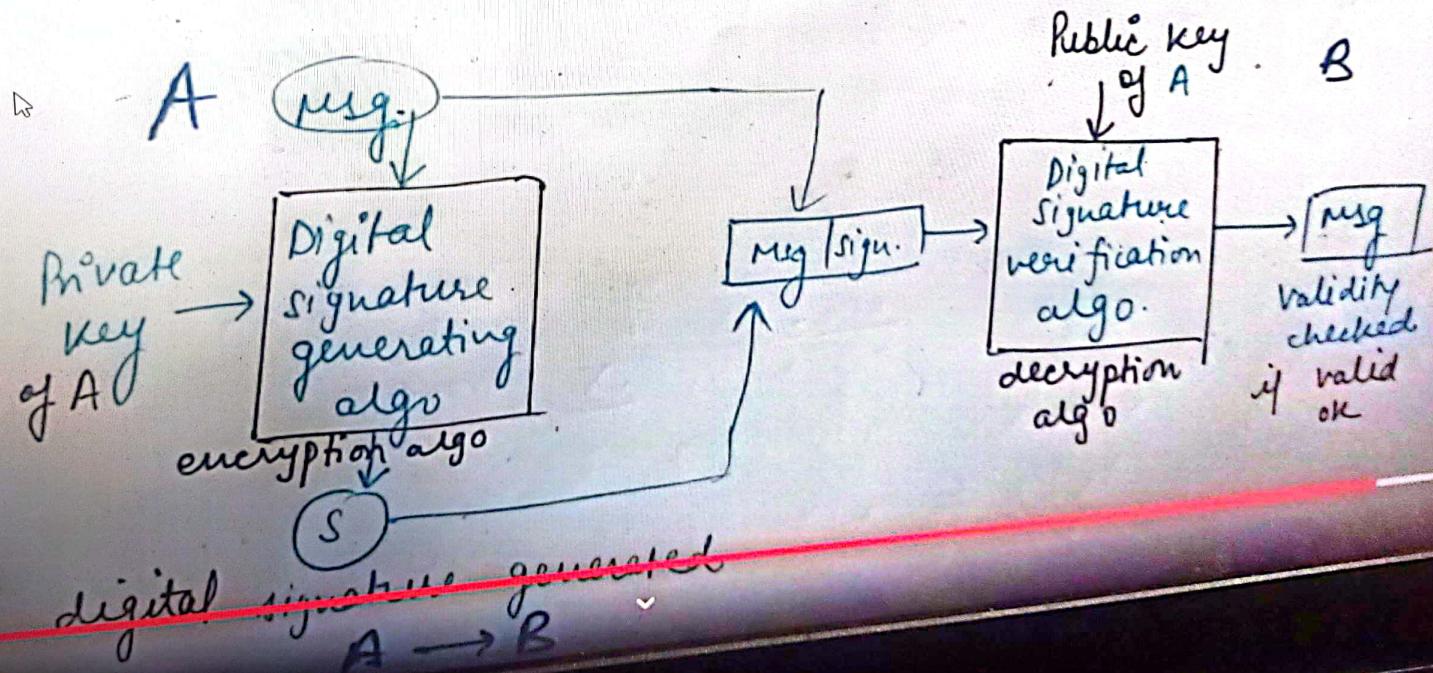
If msg is changed in b/w anyhow then,
receiver will not get the same hash value/
msg digest.

so if hash value/digest not same then ~~the~~
msg changed.

Hash for helps in preserving the integrity of msg.

Digital signature

- plays role in e-commerce, online transaction, etc.
- based on asymmetric key cryptography
- encryption → private key
- decryption → public key
- used for authentication & non repudiation & msg integrity
- not used for confidentiality



3.4 Confidentiality

A digital signature does not provide confidential communication. If confidentiality is required, the message and the signature must be encrypted using either a secret-key or public-key cryptosystem. Figure 13.5 shows how this extra level can be added to a simple digital signature scheme.

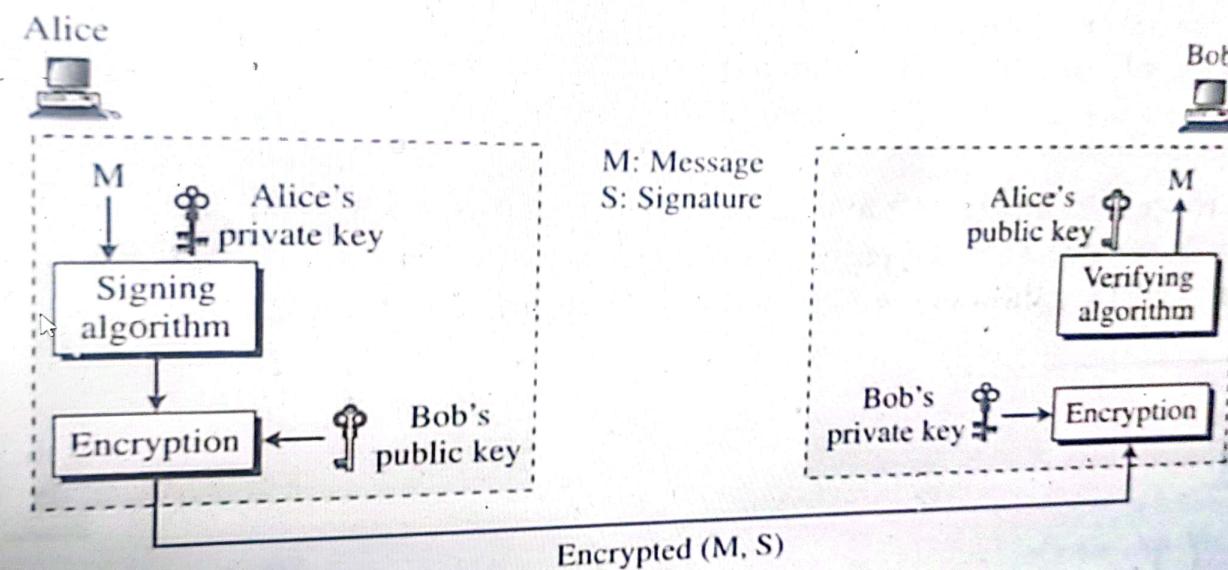


Fig. 13.5 Adding confidentiality to a digital signature scheme

We have shown asymmetric-key encryption/decryption just to emphasize the type of keys used at each end. Encryption/decryption can also be done with a symmetric key.

RSA DIGITAL SIGNATURE SCHEME

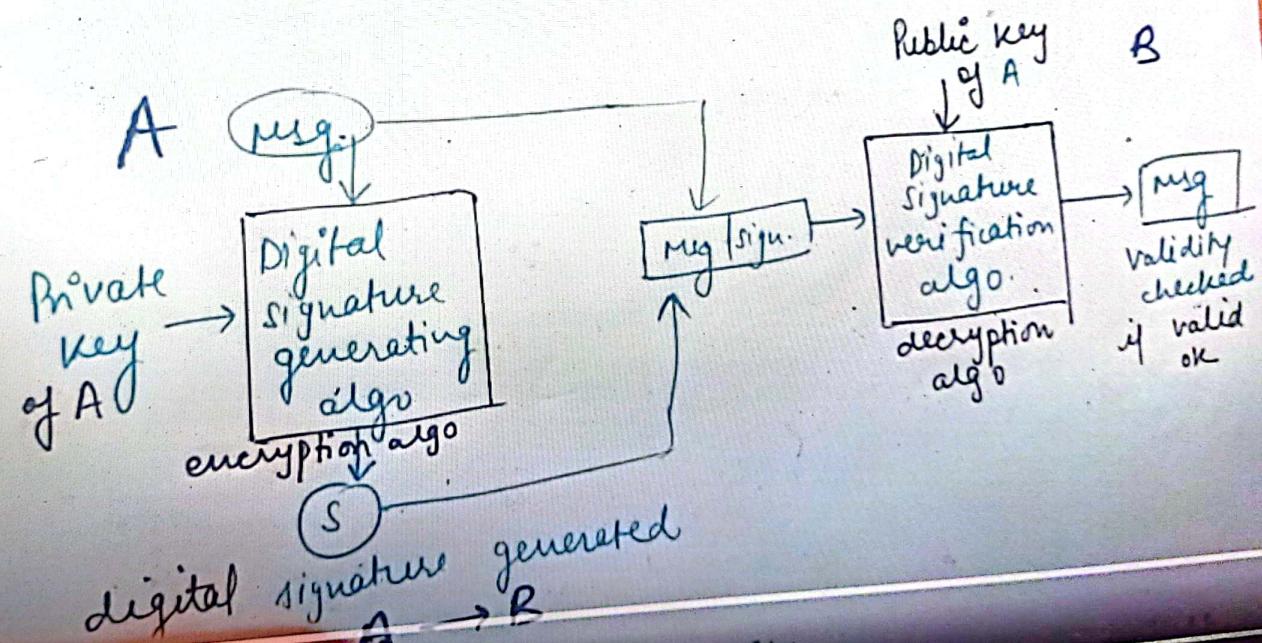
- The RSA idea can also be used to sign and verify a msg. In this case, it is called the RSA digital signature scheme.
- The digital signature scheme changes the roles of the private and public keys.

Note → 1stly, the private & public keys of the sender are used (not of the receiver).

2nd → the sender uses his/her own private key to sign the document and receiver uses the sender's public key to verify it.

Digital signature

- vinyl role in e-commerce, online transaction, etc.
- based on asymmetric key cryptography
 - encryption → private key
 - decryption → public key
- used for authentication & non repudiation & msg integrity
- not used for confidentiality



Cryptographic Scheme using RSA concept

the sender uses his/her own private key to sign the document and receiver uses the sender's public key to verify it.

key Generation

(same as RSA algo).

e.g. Alice sends a msg to Bob.

Alice chooses 2 prime nos. "p" and "q"

$$\underline{n = p * q}$$

$$\underline{\phi(n) = (p-1) * (q-1)}$$

she then chooses e (the public exponent)

and calculates d (the private exponent)

$$\text{such that } ed \equiv 1 \pmod{\phi(n)}$$

eps d and publicly announces n & e.

A2A scheme using RSA concept

A2A

In normal RSA,

Encryption

$$C = M^e \text{ mod } n$$

$M \in \mathbb{N}$

e in \rightarrow public key

Here,

for signing

$$S = M^d \text{ mod } n$$

uses her private key
or we can say

she uses her private exponent "d" to
create her signature.

Now, this signature S &
message M is sent to Bob.

verifying \rightarrow Bob receives M and S

Bob applies Alice's public exponent (e),
to the signature to create a copy of
message $|M'| = S^e \text{ mod } n$

Digital Signature Scheme using RSA concept

354

Cryptography and Network Security

In the RSA digital signature scheme, d is private; e and n are public.

□ Signing and Verifying

Figure 13.7 shows the RSA digital signature scheme.

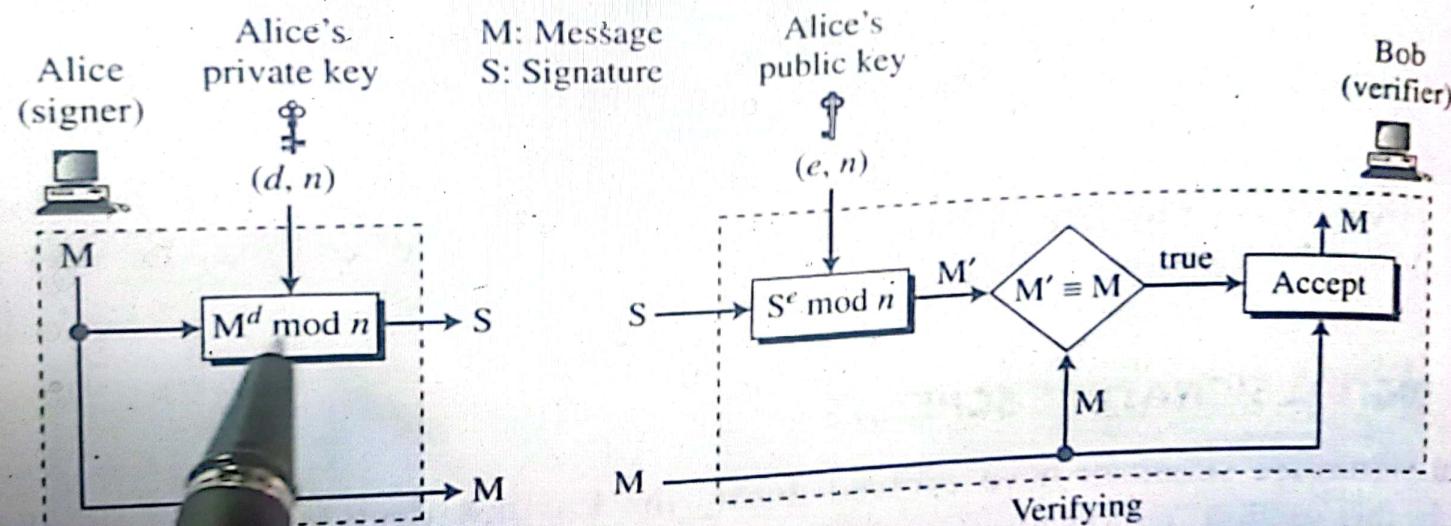


Fig. 13.7 RSA digital signature scheme

OPPO Reno2 F

Alice takes a signature out of the message using her private exponent, $S = M^d \bmod n$ and sends the signature to Bob.

Bob applies Alice's public exponent to the signature to create a message M' .

Digital Signature Scheme using RSA concept

Cryptography and Network Security

digital signature scheme, d is private; e and n are public.

Verifying

is the RSA digital signature scheme.

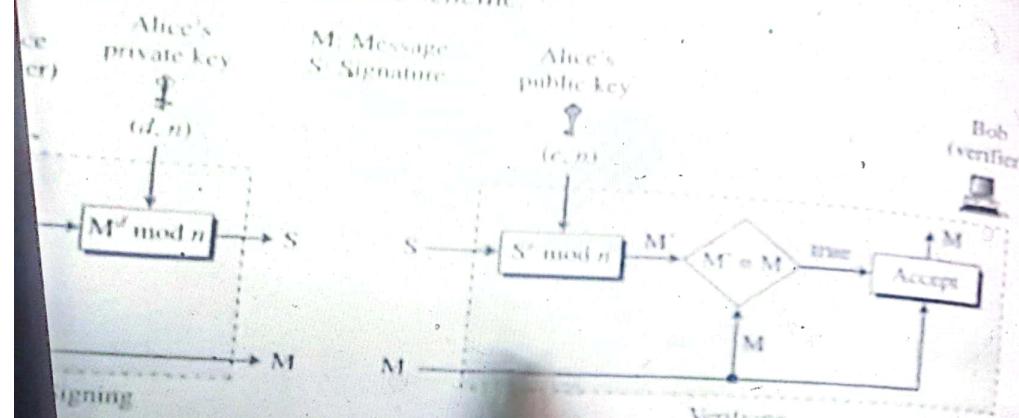


Fig. 13.7 RSA digital signature scheme

uses a signature out of the message using her private exponent, $S = M^d \text{ mod } n$ and sends the signature to Bob.

Bob receives M and S . Bob applies Alice's public exponent to the signature to create a copy of the message M' using his own private key (e, n) . Bob compares the value of M' with the value of M . If the two values are congruent, then he accepts the message. To prove this, we start with the verification criteria:

$$M \pmod{n} \rightarrow S \pmod{n} \rightarrow M^{d \times e} \equiv M \pmod{n}$$

Here,

for signing

$$S = M^d \text{ mod } n$$

\leftarrow public key

uses her private key or we can say she uses her private exponent d to create her signature.

" S " & " M' " is sent to Bob.

→ Bob receives " M " and " S "

Bob applies Alice's public exponent (e), to the signature to create a copy of message $M' = S^e \text{ mod } n$

compares the value of M' with M

both values [congruent] Bob [accepts] the message else NOT.

Signature Scheme using RSA concept

$$S = M^d \text{ mod } n$$

Now, this signature "S" & message "M" is sent to Bob.

uses her private key
or we can say
she uses her private exponent "d" to
create her signature.

Verifying → Bob receives "M" and "S"

Bob applies Alice's public exponent (e),
to the signature to create a copy of
message $M' = S^e \text{ mod } n$

Bob compares the value of M' with M

if both values match then Bob has the
mess else NOT.

In RSA Decryption
 $M = C^d \text{ mod } n$

Digital Signature Scheme using RSA concept

X

Cryptography and Network Security

In the RSA digital signature scheme, d is private; e and n are public.

□ Signing and Verifying

Figure 13.7 shows the RSA digital signature scheme.

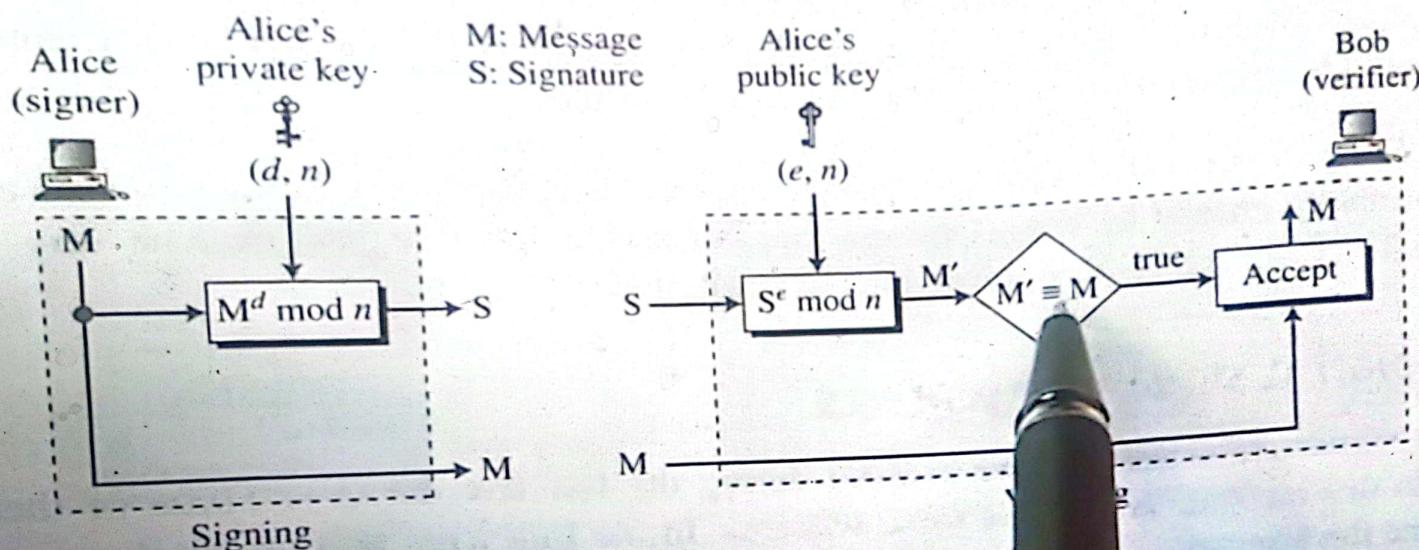


Fig. 13.7 RSA digital signature sc

Signing Alice creates a signature out of the message us
message and the signature to Bob.

OPPO Reno2 F

8:53 / 9:09 M and S. Bob apply

Elliptical Curve Cryptography

$$y^2 = x^3 + ax + b \pmod{11}$$

$$y^2 = x^3 + x + 6 \pmod{11}$$

$$E \text{ } (1, 6)$$

$a=1, b=6$

Φ^{-1}

0 --- 10

$$x | x^3 + x + 6 \pmod{11}$$

x	$x^3 + x + 6 \pmod{11}$
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	4
10	1

$$y | y^2 \pmod{11}$$

y	$y^2 \pmod{11}$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

(2, 4) (2, 7)
 (3, 5) (3, 6)
 (5, 2) (5, 9)

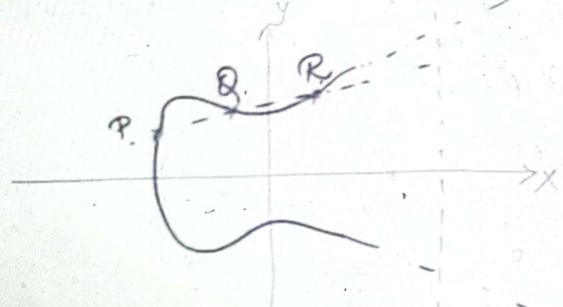


Elliptic Curve Cryptography | Encryption and Decryption | ECC in Cryptography & Security

LECTURES BY
ELLEDARSIAN



Elliptic Curve Cryptography - Encryption & Decryption



$$y^2 = x^3 + ax + b$$

asymmetric, PKC.

ECC
(n)

112

256

512

RSA/DSA

512

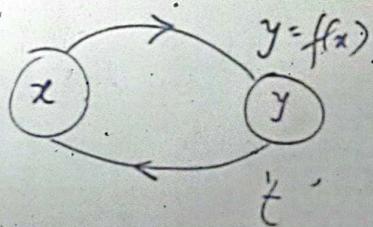
3072

15360

$E_p(a, b)$

$$\underline{Q} = \underline{kP}$$

$k < n$ (limit)



Elliptic Curve Cryptography - Encryption & Decryption

ECC Key Exchange - Global Public elements (n)

Eq. (a, b) : Elliptic curve with parameters a, b.

q : prime no., int of form 2^m

G : pt. of the EC whose order is a large value q.

ECC (n) RSA/DSA

112 512

256 3072

512 15360

$$y^2 = x^3 + ax + b$$

User A Key Generation

Select private key n_A ; $n_A < n$

Calculate public " P_A ; $P_A = n_A \cdot G$

User B: Key Generation

Select private key n_B ; $n_B < n$

Calculate public " P_B ; $P_B = n_B \cdot G$

COURSE INSTRUCTOR: Dr. Dibyendu Roy

DUE: Feb 27, 2022, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be written clearly. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks.

Problem 1

Consider the plaintext (i.e., message) CRYPTOGRAPHY and the permutation π on 12 numbers as defined below.

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$$

- (a) Using the encryption technique of Transposition cipher encrypt the above plaintext.
- (b) Check whether decryption is possible or not (provide justification). If decryption is possible write down the decryption technique.

Problem 2

Consider the plaintext (i.e., message) WEAREINDIAN and generate the ciphertext using the Shift cipher encryption algorithm with the secret key 4. Perform decryption on the ciphertext to check the correctness of your encryption.

Problem 3

Encrypt the plaintext WEAREINDIAN using Playfair cipher, where the secret key is CRICKET. Perform decryption on your generated ciphertext to validate your encryption.

Problem 4

In case of Affine cipher the key is $K = (a, b)$, where $0 \leq a, b \leq 25$ and the encryption algorithm is $y = Enc_K(x) = (a \cdot x + b) \bmod 26$. Find out the case when the decryption is not possible. Write down the decryption algorithm when we can have successful decryption. Find out the exact number of different keys for which we will have the same plaintext-ciphertext pair (x, y) .

Problem 5

If Enc is the encryption function of DES then find out the relation between the ciphertexts $C_1 = \text{Enc}(M, K)$ and $C_2 = \text{ENC}(\overline{M}, \overline{K})$. Here \overline{X} denotes the bitwise complement of X i.e., if $X = (x_1, \dots, x_n)$ then $\overline{X} = (1 \oplus \overline{x_1}, \dots, 1 \oplus \overline{x_n})$.

Problem 6

One unknown plaintext is encrypted using shift cipher encryption algorithm. The ciphertext is AFITIFWF. Find the plaintext and the secret key.

Problem 7

We use the following correspondence $A \rightarrow 0, B \rightarrow 1, \dots, Z \rightarrow 25$ to map english letters (A to Z) to numbers from 0 to 25. Let the message HILL is encrypted to XIYJ by using Hill cipher. Find atleast one possible key.

Problem 8

Using Euclidean algorithm solve the following problems.

- (a) Find the $\gcd(222, 18)$.
- (b) Find x_0, y_0 such that $1 = 33x_0 + 13y_0$.
- (c) If b is the multiplicative inverse of a under modulo n i.e., $a \cdot b \equiv 1 \pmod{n}$. Find the multiplicative inverse of 5 under modulo 26.

Problem 9

Prove that if we apply AES Subbytes function on D_3 you will get 66 as output.

Problem 10

Find the AES-Mixcolumn($33, 42, 66, 24$). Here inputs and outputs are given in integer.

Jatin Goyal
2019-10-72

Cipher

classmate

Date

Page

Q=1 message = CRYPTOGRAPHY

Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 \\ 8 & 9 & 10 & 11 & 12 \\ 2 & 10 & 4 & 12 & 7 \end{pmatrix}$

- Q) In the encryption technique of transposition cipher what we do is we replace position of words in message.
Let the plain text is :-

$P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12}$
we will replace it with :-

$P_3 P_5 P_6 P_9 P_{11} P_1 P_8 P_2 P_{10} P_4 P_{12} P_7$

So, the encryption of message CRYPTOGRAPHY
will be YTOAHCCRPPYH

- Q) To find the decryption of cipher text we will reverse permutation π .

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 8 & 1 & 10 & 2 & 3 & 12 & 7 & 4 & 9 & 5 & 11 \end{pmatrix}$$

So, the decryption of YTOAHCCRPPYH will be CRYPTOGRAPHY

2019/5/16 92

Tath Goyal

classmate

Date _____
Page _____

$\theta = 2$

In the encryption of shift cipher we shift the characters of plain text by K amount and if shift is more than 26 we take modulo.

$$\text{Encryption} = (\text{Plain text} + \text{shift}) \bmod 26$$

So, the encryption of message WE ARE INDIAN will be -

Message \rightarrow W E A R E I N D O I A N

Index \rightarrow 23 3 0 17 4 8 13 3 8 0 13

Shift \rightarrow 4 4 4 4 4 4 4 4 4 4 4 4

Adding \rightarrow 26 8 4 21 8 12 17 7 12 4 17

taking mod \rightarrow 8 4 21 8 12 17 7 12 4 17

W E A R E I N D O I A N

Encrypted text \rightarrow A I E V I M R H M E R

$$\text{Decryption} = (\text{Cipher} - \text{shift} + 26) \bmod 26$$

$$(A - 4 + 26) \bmod 26 = W \quad (M - 4 + 26) \bmod 26 = I$$

$$(I - 4 + 26) \bmod 26 = E \quad (R - 4 + 26) \bmod 26 = N$$

$$(E - 4 + 26) \bmod 26 = V \quad (H - 4 + 26) \bmod 26 = M$$

$$(H - 4 + 26) \bmod 26 = R \quad (M - 4 + 26) \bmod 26 = I$$

$$(M - 4 + 26) \bmod 26 = E \quad (E - 4 + 26) \bmod 26 = A$$

2019/10/22

Tathu Loyal

EFOLI CLASSMATE

Date _____
Page 71

$$(R-4+26) \bmod 26 = N$$

so, decryption of AIEVIMRHMER will
be WEAREINOTAN.

Forward writing shown above second row, fourth row

3 X 5 4 3

7 8 3 H T

4 M J H N

3 2 D 9 0

5 V X W Y

to bring column in second row, fourth

• best nicely

X 4 - H P U V I B Z R E S O

103 forward writing second row with 103 \rightarrow 350

H - S K S F W M N O P Q R

S C -

103 forward writing second row with 103 \rightarrow 350

H G F W M N O P Q R

H F K -

H H = M

103 forward writing second row with 103 \rightarrow 350

D E B 3 V A

A C T

2019/10/72

Tatin loyal

STORY CLASSMATE

Date _____
Page _____

$\alpha = 3$

Plain text = WE ARE INDIAN

Secret Key = CRICKET
Encryption :-

First, we have to make a key matrix

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

Second, we have to make pairs of plain text.

WE AR EI ND IA NX

WE :- As they are not in same row or same column so $W \rightarrow 2$ & $E \rightarrow R$
 $= 2R$

AR :- As they are in same column
so, $A \rightarrow H$

$R \rightarrow A$

AR = HA

EI :- They are in same row
so, $E \Rightarrow C$

$I \rightarrow K$

OPPO Reno2 F

2019SS10 72

Tatish Rayal

classmate

Date _____

Page _____

$$EI = CR$$

ND :- As they are not in same row
or same column.

$$\text{So, } N \rightarrow M$$

$$\therefore ND = MF$$

IA :- They are also not in same row
or same column.

$$\text{So, } I \rightarrow R$$

$$\therefore IA = RB$$

NX :- They are also not in same row
or same column

$$\text{So, } N \rightarrow L$$

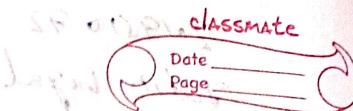
$$X \rightarrow 2$$

$$\therefore NX = L2$$

so, encryption of WE ARE INDIAN
is ZRHACKMERBL2

2019/1672

John royal



Decryption :-

In decryption we will use same key matrix as encryption.

2R :- They are in different row and col.
 $2R = WE$

HA :- They are in same column
 $HA = AR$

CR :- They are in same row
 $CR = EI$

MF :- They are in diff. row and col.
 $MF = NO$

RB :- They are in diff. row & col.
 $RB = IA$

L2 :- They are in diff. row & col.
 $L2 = NX$

So, decryption of 2RHACKMFRB12
will be WEARE INDIANX

2019/5/10/72

Tath Boyal

Topic: classmate

Date _____

Page _____

Q:4 Decryption of affine cipher is not possible if a^{-1} does not exist. So, if $(a, 26)$ are not coprime or $\text{gcd}(a, 26)$ is not equal to 1 then a^{-1} does not exist.

Decryption Algorithm :-

$$\text{Decryption} = ((C - b) * \text{inv}(a)) \bmod 26.$$

Let k be the inverse of a .

$$\text{So, } k * a \bmod 26 \equiv 1$$

$$k = \text{inv}(a) \bmod 26$$

So, both (a, b) & $(\text{inv}(a), b)$ will have the same ciphertext of a plaintext.

201951072

Tath Loyal

SPOLIATED CLASSMATE

Date _____
Page _____

$C = S$

$C_1 = ENC(m, k)$

$C_2 = ENC(\bar{m}, \bar{k})$

\bar{x} = bitwise complement of x

$x = (x_1, x_2, \dots, x_n)$

So by using the complement property of P.E.S.

$ENC(m, k) = C$

also $ENC(\bar{m}, \bar{k}) = \bar{C}$

$C_2 = ENC(\bar{m}, \bar{k})$

$\bar{C}_2 = ENC(\bar{\bar{m}}, \bar{\bar{k}}) \quad (\because \bar{\bar{x}} = x)$

$\bar{C}_2 = ENC(m, k) \equiv C_1$

$\therefore C_1 = \bar{C}_2$

Let $M = L_0 : R_0$

$L_1 = R_0$

$M = (R_0 \text{ XOR } R_1) \quad (\text{round function})$

$M = Sbox(m)$

$R_0 = L_0 \text{ XOR } (M)$

$C_1 = L_1 : R_1$

Now $C_2 = ENC(\bar{m}, \bar{k})$

let $\bar{m} = L_0 : R_0$

$L_1 = R_0 = \bar{R}_0$

2019/16/72

Tathri Gayal

16/01/2021 CLASSMATE

Date _____

Page _____

$$M = \overline{R_0} \text{ XOR } \overline{K}$$

$$M = (R_0 \text{ XOR } K) \quad (\text{XOR causal complement})$$

$$M = (\overline{R_0} \text{ XOR } K) \quad (\text{Same as round function})$$

$$M = \overline{\text{box}}(m)$$

$$R_1 = \overline{I_0} \text{ XOR } (m)$$

$$(R_1)_2 = \overline{R_1} + 1 \quad (\text{do both } R_1 \text{ and } \overline{R_1})$$

$$(I_1)_2 = \overline{I_1} + 1 \quad (\text{do both } I_1 \text{ and } \overline{I_1})$$

$$(C_1)_2 = (I_1)_2 (R_1)_2 = \overline{I_1} \overline{R_1} = \overline{C_1}$$

$$(C_1)_2 = \overline{C_1} \quad (\text{do both } C_1 \text{ and } \overline{C_1})$$

(do both I_1 and $\overline{I_1}$)

Thus after a single round the ciphertext achieves $(\overline{m}, \overline{R})$, i.e. the complement of ciphertext (m, R) . Since, K is always complementary, this trend will happen in all rounds.

so, $C_2 = \text{ENC}(\overline{m}, \overline{K}) = \overline{m} = \text{ENC}(m, K)$

Hence proved.

10/9/10/92
Tahn royal

ST 211A classmate

Date _____
Page _____

$$Q = 6$$

ciphertext = AFITIFWF

(Known)

chaypt $\rightarrow (X + K) \bmod 26 = Y$
decrypt $\rightarrow (Y - K) \bmod 26 = X$

F repeated 3 times.

$$(S - K) \bmod 26 = L$$

$$\begin{aligned} (L + K) \bmod 26 &= S \\ (S - K) \bmod 26 &= L \end{aligned}$$

$$(L + S)(K + L - S) = 0$$

Now we will try for $K = 0, 1, 2, 3, 4, 5$
As most common word in english
is 'A'. So, we will first try
 $K = 5$.

$$\text{FOR } K = 5$$

$$\begin{aligned} A &\rightarrow V, F \rightarrow A, I \rightarrow O, T \rightarrow O \\ S &\rightarrow R \end{aligned}$$

so plaintext will be VADODARA.

2019/10/2

Tutor: royal

classmate

Date _____

Page _____

a = 7

message = HILL

Cipher = XI XJ

HILL = [7, 8, 11, 11]

XIXJ = [23, 8, 23, 9]

Let key = $\begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$

Enc = $XK \pmod{26}$

Dec = $XK^{-1} \pmod{26}$

$$[7, 8][11, 11] \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} = \begin{bmatrix} 23 & 8 \\ 24 & 9 \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} k_1 + k_2 \\ k_3 + k_4 \end{bmatrix} = \begin{bmatrix} 23 & 8 \\ 24 & 9 \end{bmatrix}$$

$$7k_1 + 8k_2 = 23$$

$$7k_3 + 8k_4 = 24$$

$$11k_1 + 11k_2 = 24$$

$$11k_3 + 11k_4 = 9$$

on solving above equation:

$$k_1 = 11, k_2 = 8, k_3 = 3, k_4 = 7$$

$$(11 - 8) + 11 \cdot (3 - 7) = 1$$

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

$$\text{Q} = 8 \quad (9) \quad \gcd(222, 18)$$

Euclidean theorem $\Rightarrow a = b \times q + r$

If $A = 0$ then $\gcd(A, B) = B$

$$\gcd(0, B) = B$$

If $B = 0$ then $\gcd(A, B) = A$

$$\gcd(A, 0) = A$$

$$222 = (18 \times 12) + 6$$

$$\text{Here } r_1 = 6$$

$$18 = 6 \times 3 + 0$$

$$\text{Here } r_2 = 0$$

$$\gcd(222, 18) = 6$$

(6)

$$1 = 33x_0 + 13y_0$$

$$33 = 13 \times 2 + 7 \quad (r_1 = 7)$$

$$13 = 7 \times 1 + 6 \quad (33 \div (r_1 = 6))$$

$$7 = 6 \times 1 + 1 \quad (33 \div (r_1 = 1))$$

$$6 = 1 \times 6 + 0 \quad (33 \div (r_1 = 0))$$

$$1 = 7 \times 6 - 1 \times 33$$

$$1 = (33 - 13 \times 2) - (13 - 7 \times 1)$$

$$1 = (33 - 13 \times 2) - 13 + (33 - 13 \times 2)$$

$$1 = 2 \times 33 - 5 \times 13$$

261951672

Tathbi Koyal

classmate

Date _____

Page _____

after Comparing

$$1 = 23 \times 33 - 5 * 13$$

$$1 = 33x_0 + 13y_0$$

$$x_0 = 2$$

$$y_0 = -5$$

① $a \cdot b = 1 \pmod{n}$ (b is mul-inv. of a)

$$x = s^{-1} \pmod{26}$$

$$sx = 1 \pmod{26}$$

$$sx = 10s \pmod{26}$$

$$sx = 26(8) \pmod{26}$$

$$x = 21 \pmod{26}$$

$$x = 21$$

21/9/2022

Tahn Loyel

classmate

Date _____

Page _____

Q = 9

~~Off 00 03 06 Happy 2013 2014
Duration we will get 66 nos
about~~

2019 S10 72
Tatin Loyal

classmate

Date _____

Page _____

(2/10) AES Mix column $(33, 42, 66, 24)$

$$\begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix} = \begin{bmatrix} 33 \\ 42 \\ 66 \\ 24 \end{bmatrix}$$

$$K_1 = 33 = 110011 = x^5 + x^4 + x + 1$$

$$K_2 = 42 = 1000010 = x^5 + x$$

$$K_3 = 66 = 1100110 = x^6 + x^5 + x^2 + x$$

$$K_4 = 24 = 100100 = x^5 + x^2$$

$$\begin{aligned} K_1' &= x(K_1) + (x+1)K_2 + K_3 + K_4 \\ &= x^7 + x^6 + x^5 + x \\ &= 1100010 = 52 \end{aligned}$$

$$\begin{aligned} K_2' &= x(K_2) + (x+1)K_3 + K_4 + K_1 \\ &= x^2 + x^2 + x^7 + x^5 + x^3 + x + x^5 + x^2 \\ &\quad + x^5 + x^4 + x + 1 \\ &= x^5 + x^4 + x^3 + 1 \\ &= 00111001 = 39 \end{aligned}$$

$$\begin{aligned} K_3' &= xK_3 + (x+1)K_4 + K_1 + K_2 \\ &= x^6 + x^6 + x^4 + 1 \\ &= 11010001 \\ &= 08 \end{aligned}$$

20/9/2022

Jatin Goyal

classmate

Date _____
Page _____

$$\begin{aligned}K_4' &= \alpha K_4 + (\alpha+1) K_1 + R_2 + K_3 \\&= \alpha^5 + \alpha^4 + 1 \\&= 60110001 \\&= 31\end{aligned}$$

$$\begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^9 \\ D_1 \\ 0110001 \end{bmatrix}$$

$$\begin{aligned}\alpha^2 + \alpha^9 + \alpha(1+\alpha) + (1+\alpha)\alpha &= 1 \\ \alpha^2 + 2\alpha^9 + 2\alpha + \alpha^2 + \alpha^9 + \alpha &= 1 \\ 2\alpha^9 + 3\alpha^2 + 3\alpha &= 1 \\ 2\alpha^9 &= 01000011\end{aligned}$$

$$\begin{aligned}\alpha^2 + \alpha^9 + \alpha(1+\alpha) + \alpha^2 &= 1 \\ \alpha^2 + 2\alpha^9 + 2\alpha + \alpha^2 &= 1 \\ 2\alpha^9 + 3\alpha^2 + 2\alpha &= 1 \\ 2\alpha^9 &= 10011100\end{aligned}$$

$$\begin{aligned}\alpha^2 + \alpha^9 + \alpha(1+\alpha) + \alpha^2 &= 1 \\ \alpha^2 + 2\alpha^9 + 2\alpha + \alpha^2 &= 1 \\ 2\alpha^9 + 3\alpha^2 + 2\alpha &= 1 \\ 2\alpha^9 &= 10011100\end{aligned}$$

CS304: INTRODUCTION TO CRYPTOGRAPHY & NETWORK SECURITY
ASSIGNMENT II

COURSE INSTRUCTOR: Dr. Dibyendu Roy

DUE: Apr 22, 2022, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be handwritten. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks. Your submission will not be considered if you submit late.

Problem 1

2 marks

The DES S-box S_4 has some unusual properties:

- (a) Prove that the second row of S_4 can be obtained from the first row by means of the following mapping:

$$(y_1, y_2, y_3, y_4) \rightarrow (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0)$$

where the entries are represented as binary strings.

- (b) Show that any row of S_4 can be transformed into any other row by a similar type of operation.

Problem 2

1 mark

Describe in detail how both encryption and decryption in CTR mode can be parallelized efficiently.

Problem 3

1 mark

Suppose that $X = (x_1, \dots, x_n)$ and $X' = (x'_1, \dots, x'_n)$ are two sequences of n plaintext blocks. Suppose X and X' are encrypted in OFB mode using the same key and the same IV. Show that it is easy for an adversary to compute $X \oplus X'$. Show that a similar result holds for CTR mode if ctr is reused.

Problem 4

1 mark

Construct two LFSRs using the following two connection polynomials and find their periods.

- (a) $f(x) = x^4 + x + 1$.
(b) $f(x) = x^5 + 1$.

Problem 5

1 mark

Define a toy hash function $h : (\mathbb{Z}_2)^7 \rightarrow (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and the matrix A is given below

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Find all preimages of $(0, 1, 0, 1)$.

Problem 6

1 mark

Suppose $h_1 : \{0, 1\}^{2m} \rightarrow \{0, 1\}^m$ is a collision resistant hash function. Define $h_2 : \{0, 1\}^{4m} \rightarrow \{0, 1\}^m$ as follows:

- (a) Write $x \in \{0, 1\}^{4m}$ as $x = x_1 \parallel x_2$, where $x_1, x_2 \in \{0, 1\}^{2m}$.
(b) Define $h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2))$.

Show that h_2 is collision resistant.

Problem 7**1 mark**

Suppose $\lambda : \mathbb{Z}_{105} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ is defined as

$$\lambda(x) = (x \pmod{3}, x \pmod{5}, x \pmod{7}).$$

Give an explicit formula for the function λ^{-1} and use it to compute $\lambda^{-1}(2, 2, 3)$.

Problem 8**1 mark**

Solve the following system of congruences:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}.$$

Problem 9**2 marks**

In RSA cryptosystem consider $n = 18923$ and the encryption key $e = 1261$. For the ciphertext $c = 6127$ find the corresponding plaintext. Explain each and every step.

Problem 10**2 marks**

Let EL be the elliptic curve $y^2 = x^3 + 5x + 3$ defined over \mathbb{Z}_{13} . Find out all the possible points on EL . Provide justification against your answer.

Tatin Loyal
201951072

classmate

Date _____
Page _____

Q=3 This problem can be solve easily by checking for every element in row 1 & apply operation and match with row 2.

row 1 Binary(most) shift Bits XOR Decimal
 $y_1 y_2 y_3 y_4 \quad (y_2 \cdot y_1 y_4 y_3) \quad (0, 1, 1, 0)$

7	0111	1011	1100	13
13	1101	1110	1000	8
14	1110	1101	1011	11
3	0011	0011	0101	5

0	0000	0000	0110	6
6	0110	1001	1111	15
9	1001	0110	0000	0
10	1010	0101	0011	3

1	0001	0010	0100	4
2	0010	0001	0111	7
8	1000	0100	0010	2
5	0101	1000	1100	12

11	1011	0111	0001	1
12	1100	1100	1010	10
4	0000	1000	1110	9
15	1111	1111	1001	9

2019/10/7 2

Jatin Voyal

classmate

Date _____
Page _____

as we can see now: 1 & row 2
are same.

⑥ By the above rule discussed we can
show that, 2nd row can be
transformed into forth row.

To transform, st row into 4th row.

(i) convert entry into binary format

$$(y_1, y_2, y_3, y_4) \text{ where } y_i \in \{0, 1\}$$

⑦ compute $(y_4 y_3 y_2 y_1) \oplus (0, 1, 1, 0)$

row y_3 can be transformed into y_4
using

$$(y_1, y_2, y_3, y_4) \rightarrow (y_2 y_1 y_4 y_3) \oplus (0, 1, 1, 0)$$

2019/10/7
Tatin royalCLASSMATE
Date _____
Page _____

Q2 let length of plain text is m . In CTR mode we choose a counter denoted "ctr" which is bit string of length m .

We construct a sequence of bit string of length m denoted T_1, T_2 etc defined as follows.

$$T_i = \text{ctr} + i - 1 \bmod 2^m$$

Encrypt to plain text block x_1, x_2, \dots, x_n

$$y_i = x_i \oplus \text{ctr}(T_i)$$

As we can see that we can encrypt plaintext blocks independently of any other element.

So, we can parallelly encrypt and decrypt blocks efficiently.

2019/5/6 72

Tatin Loyal

classmate

Date _____

Page _____

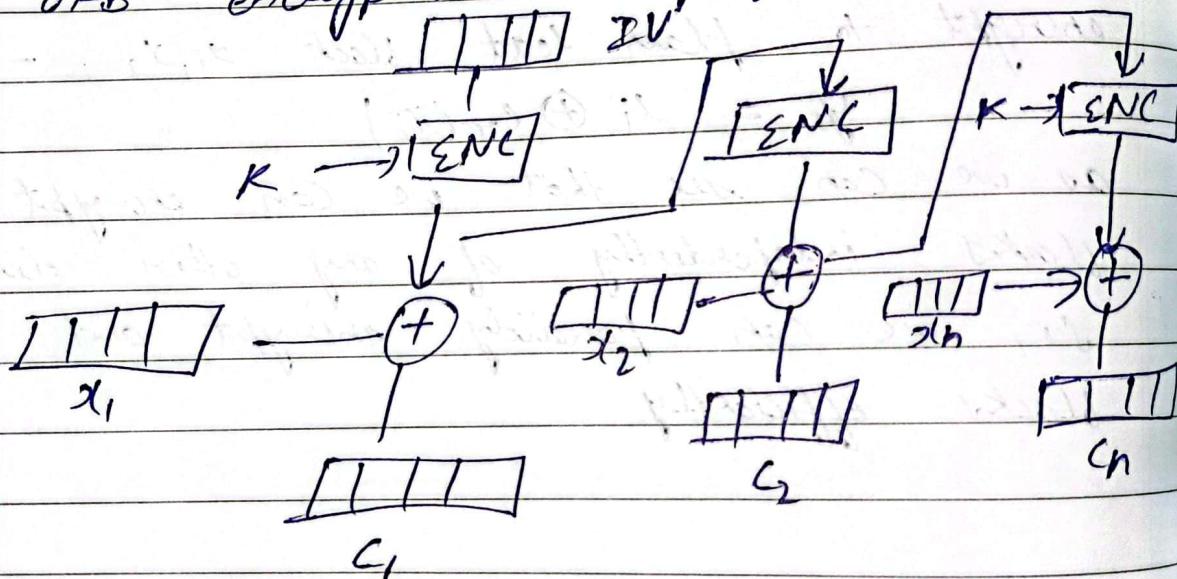
 $Q=3$

6 bit plaintext

$$x = (x_1, x_2, \dots, x_n)$$

$$x' = (x'_1, x'_2, \dots, x'_n)$$

x & x' are encrypted in OFB mode using same key and the same IV. OFB encryption is performed.



2019 S1672

Tatish Goyal

classmate

Date _____

Page _____

 $a=4$

$$F(x) = x^4 + x + 1$$

As we know from LFSR

$$L(t) = C_{t-1} \oplus C_{t-2} \oplus \dots \oplus C_0$$

↑
feedback function

$$F(x) = x^4 + x + 1$$

$$L = S_0 \oplus S_3$$

t	S_3	S_2	S_1	S_0
0	0	0	1	0
1	1	1	0	0
2	1	0	1	1
3	0	0	1	0
4	1	0	0	1
5	1	0	0	1
6	0	1	0	0
7	0	0	1	0
8	0	0	0	1
9	1	0	0	0
10	1	1	0	0
11	1	1	1	0
12	1	1	1	1
13	0	1	1	1
14	1	0	1	1
15	0	1	0	1

2019S1G72

Jafir Uygal

classmate

Date

Page

output sequence =

1010110010001111

Period = 15 AY

$$\textcircled{1} \quad F(x) = x^5 + 1$$

$$L = 50$$

T	S ₄	S ₃	S ₂	S ₁	S ₀
0	0	0	1	1	0
1	1	0	1	1	0
2	0	1	0	1	1
3	1	0	1	0	1
4	1	1	0	1	0
5	0	1	1	0	1

output sequence

10110

Period = 5 AY

2019/10/72

Tathik Goyal

classmate

Date _____

Page _____

$$h: (2^2)^7 \rightarrow (2^2)^4$$

$$h(x) = xA$$

where x is 7 bit length string

$$h(x) \rightarrow 4 \text{ bit output}$$

$$\text{Let } x = [x_1, x_2, x_3, x_4, x_5, x_6, x_7]$$

$$h(x) = xA$$

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \left[\begin{array}{r} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array} \right] = [y_1, y_2, y_3, y_4]$$

~~we need to find for~~

we need to find pre image of $[0\ 1\ 0\ 1]$
find out all equation

$$x_1 + x_2 + x_3 + x_4 = 0 \quad (i)$$

$$x_2 + x_3 + x_4 + x_5 = 1 \quad (ii)$$

$$x_3 + x_4 + x_5 + x_6 = 0 \quad (iii)$$

$$x_5 + x_6 + x_7 = 1 \quad (iv)$$

2019/10/2

Tatish boyel

from eqn (i) & (ii)

$$x_5 = 1 + x_1$$

from (ii) & (iii)

$$x_1 = 1 + x_2$$

from (iii) & (iv)

$$x_7 = 1 + x_3$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	1	1	1
0	1	0	1	1	0	1
0	0	1	1	1	1	0
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	0	1	1	0	1	0
1	1	0	0	0	0	1
1	1	1	1	0	1	1

2019/10/9²

Tatini Loyal

classmate

Date _____

Page _____

P=6

Let us assume there exists x_1 & x_2 such that $x_1 \neq x_2$ and

$$h_2(x_1) = h_2(x_2)$$

$$x_1 = x_1' \parallel x_1''$$

$$x_2 = x_2' \parallel x_2''$$

$$x_1', x_2' \in \{0, 1\}^{2m}$$

$$x_1'', x_2'' \in \{0, 1\}^{2m}$$

Since $h_2(x_1) = h_2(x_2)$

$$h_2(x_1' \parallel x_1'') = h_2(x_2' \parallel x_2'')$$

Since $h_2(x_1) = h_1(h_1(x_1) \parallel h_1(x_2))$

$$h_2(x_1) = h_1(h_1(x_1') \parallel h_1(x_1''))$$

$$h_2(x_2) = h_1(h_1(x_2') \parallel h_1(x_2''))$$

Since we assume

$$h_2(x_1) = h_2(x_2)$$

$$h_1(h_1(x_1') \parallel h_1(x_1'')) = h_1(h_1(x_2') \parallel h_1(x_2''))$$

$$h_1(x_1') \parallel h_1(x_1'') = h_1(x_2') \parallel h_1(x_2'')$$

$$\text{if } h_1(x_1') = h_1(x_2')$$

$$h_1(x_1'') = h_1(x_2'')$$

$$x_1' = x_2', \quad x_1'' = x_2''$$

So, it contradicts our assumption.

Therefore h_2 is collision resistant.

2019/16/72

Tatish royal

classmate

Date _____

Page _____

$$Q = 7$$

$$\nu : 210S \rightarrow 23 \times 25 \times 27$$

$$\nu(x) = (x \bmod 3, x \bmod 5, x \bmod 7)$$

$$N = 105$$

$$N_1 = 35, N_2 = 21, N_3 = 15$$

$$35x_1 \equiv 1 \pmod{3}$$

$$x_1 = 2$$

$$21x_2 \equiv 1 \pmod{5}$$

$$x_2 = 1$$

$$15x_3 \equiv 1 \pmod{7}$$

$$x_3 = 1$$

$$\nu^{-1}(x) = (-2 \times 35x_1 + 1 \times 21x_2 + 1 \times 15x_3) \bmod 105$$

$$\nu^{-1}(x) = (70x_1 + 21x_2 + 15x_3) \bmod 105$$

$$\nu^{-1}(2, 21, 3) = (70x_1 + 21x_2 + 15x_3) \bmod 105$$

$$= 227 \bmod 105$$

$$= 227 \bmod 105$$

2019/10/7
Tatin royal

classmate

Date _____

Page _____

 $\alpha = 8$

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}$$

$$a_1 = 12$$

$$m_1 = 25$$

$$a_2 = 9$$

$$m_2 = 26$$

$$a_3 = 23$$

$$m_3 = 27$$

$$M = m_1 \cdot m_2 \cdot m_3$$

$$= 17550$$

$$m_i = \frac{M}{m_i}$$

$$m_1 = \frac{17550}{m_1} = 702$$

$$m_2 = \frac{17550}{m_2} = 675$$

$$m_3 = \frac{17550}{m_3} = 650$$

$$m_1 m_1^{-1} = 1 \pmod{25}$$

$$702 (m_1^{-1}) = 1 \pmod{25}$$

$$m_1^{-1} = 13$$

Tatik Goyal
2019/10/7

classmate

Date _____

Page _____

$$m_2 \times m_2^{-1} = 1 \pmod{26}$$
$$m_2^{-1} = 25$$

$$m_3 m_3^{-1} = 1 \pmod{27}$$

$$650 m_3^{-1} = 1 \pmod{27}$$

$$m_3^{-1} = 214$$

$$x = \sum_{i \in I} a_i m_i m_i^{-1}$$

$$= a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + a_3 m_3 m_3^{-1}$$

$$x = 109512 + 151875 + 209300$$

$$= 470687 \pmod{17550}$$

~~Final Answer~~

$$x = 14387$$

Jatin Loyal
201951072

classmate

Date _____

Page _____

Q. 9

$$n = 18923 \quad e + \phi(n) = 1261$$

$$c = 6127$$

To decrypt the cipher text we will use the eqn $m = c^d \pmod{e}$

where d is decryption key which is obtained using $P \& Q$.

Here in the given question only n is given.

So for me there is not possible way to decrypt the ciphertext except for brute force method to find $P \& Q$ from n .

Now to find d we will find $P \& Q$ from n using brute force.

$$n = 18923$$

$$P \& Q = 1127, 149$$

Now to calculate $\phi(n)$

we know

$$\begin{aligned}\phi(n) &= (P-1)(Q-1) \pmod{n} \\ &= 18648\end{aligned}$$

Now for d : $de \equiv 1 \pmod{18648}$

using extended euclidean

$$d = 5797$$

Now for plain text

$$M = c^d \pmod{n}$$

$$M = 6127^{5797} \pmod{18923}$$

We will get plain text with it.

Tatish boyal

2019/10/72

classmate

Date _____
Page _____

$$\text{Given } y^2 = x^2 + 5x + 3$$

$$\text{where } a = 5, b = 3$$

$$\text{when } x \in \{0, 1, \dots, 12\}$$

by brute force for every $x \in \{0, 1, \dots, 12\}$
we find y .

x	y	$y' \mod 13$
0	0	0
1	9	1
2	8	4
3	6	9
4	9	3
5	10	12
6	2	10
7	4	10
8	9	12
9	10	3
10	0	9
11	11	4
12	10	1

four points having on the curve g, g', g''
must be equal.

Tatin royal
2019/10/2

classmate

Date _____

Page _____

so, points on elliptic curve are as follow

(0, 4) (0, 9) (1, 3) (1, 10) (4, 3) (4, 10) (5, 6)
(5, 7) (7, 2) (7, 11) (8, 3) (8, 10) (9, 6)
(9, 7) (10, 0) (12, 6) (12, 7)

Started on Thursday, 10 March 2022, 2:30 PM**State** Finished**Completed on** Thursday, 10 March 2022, 3:49 PM**Time taken** 1 hour 18 mins**Grade** **24.00** out of 40.00 (**60%**)**Question 1**

Correct

Mark 1.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message M of length 1024 bits

has been encrypted using AES-128 in OFB mode of operation. During transmission 256-th bit

and 512-th bit of the ciphertext are altered. Now the receiver performs the

decryption on the received ciphertext and obtained the decrypted text M' .

Which of the following statement is true?

 a. M and M' will differ at 256-th bit to 1024-th bit b. M and M' will differ from 256-th bit to 512-th bit c. M and M' will differ at 256-th bit and 512-th bit  d. none of these

Your answer is correct.

The correct answer is:

M and M' will differ at 256-th bit and 512-th bit

Question 2

Correct

Mark 1.00 out of 1.00

Let $C_1 = DES(M, K)$ and $C_2 = DES(\bar{M}, K)$. Which of the following relation is true?

a. $C_1 = C_2$

b. none of these

c. $C_1 = \bar{C}_2$

Your answer is correct.

The correct answer is:

none of these

Question 3

Incorrect

Mark 0.00 out of 1.00

Select the most appropriate one. Hash function has the following property

a. Finding preimage, collision, second preimage all are hard

b. Preimage finding is hard

c. Second preimage finding is hard

d. Collision finding is hard

e. Finding preimage or collision or second preimage may not be hard

Your answer is incorrect.

The correct answer is:

Finding preimage or collision or second preimage may not be hard

Question 4

Incorrect

Mark 0.00 out of 1.00

The expansion function of DES is

- a. invertible

- b. not invertible

Your answer is incorrect.

The correct answer is:

invertible

Question 5

Correct

Mark 1.00 out of 1.00

What is meant by the security of an Encryption Scheme?

- a. An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext

- b. An attacker who gets hold of a ciphertext should not be able to get any function of the bits of the plaintext

- c. An attacker who gets hold of a ciphertext should not be able to get the secret key used for the encryption

- d. An attacker who gets hold of a ciphertext should not be able to know the plaintext

Your answer is correct.

The correct answer is:

An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext

Question 6

Correct

Mark 1.00 out of 1.00

Assume that in a classroom there are 220 students. Form a group by

taking x many students randomly from the classroom. For which value

of x there will be atleast two students with same date of birth

with probability 0.7.

a. 30



b. 35

c. none of these

d. 28

Your answer is correct.

The correct answer is:

30

Question 7

Correct

Mark 1.00 out of 1.00

Decryption of CBC mode of operation can be implemented in parallel

a. yes



b. no

Your answer is correct.

The correct answer is:

yes

Question 8

Correct

Mark 1.00 out of 1.00

The number of valid keys in the Affine Cipher over \mathbb{Z}_{46} is

 a. b. c. none of these d. 

Your answer is correct.

The correct answer is:

Question 9

Incorrect

Mark 0.00 out of 1.00

Select the correct answer where $S_1 : \{0,1\}^6 \rightarrow \{0,1\}^4$

and $S_2 : \{0,1\}^6 \rightarrow \{0,1\}^4$ are the pre-defined S-boxes

for the round function of DES.

a. $S_1(55) = 7, S_2(43) = 6$

b. $S_1(55) = 14, S_2(43) = 15$

c. $S_1(55) = 15, S_2(43) = 14$

d. none of these

e. $S_1(55) = 6, S_2(43) = 7$



Your answer is incorrect.

The correct answer is:

$S_1(55) = 14, S_2(43) = 15$

Question 10

Correct

Mark 1.00 out of 1.00

```
If AES-Mixcolumn(23, 67, 45, 89) = (x,y,z,w) then y =
```

```
[here input and output are in integer]
```

 a. 191 b. 229 c. 159 d. 121

Your answer is correct.

The correct answer is:

```
191
```

Question 11

Correct

Mark 1.00 out of 1.00

Assume that in a classroom there are 250 students. Form a group by taking x many

students randomly from the classroom. For which value of x there will be atleast

two students with same date of birth with probability 0.9.

a. 30

b. 41 ✓

c. 35

d. none of these

Your answer is correct.

The correct answer is:

41

Question 12

Correct

Mark 1.00 out of 1.00

For a fixed key any symmetric key encryption algorithm should

a. be surjective function

b. not necessary to be injective

c. be injective function ✓

d. not necessary to be surjective

e. none of these

Your answer is correct.

The correct answer is:

be injective function

Question 13

Correct

Mark 1.00 out of 1.00

For each key DES is basically a permutation i.e., we can have 2^{56} such

permutations. With all these permutations consider the set G.

Now G with the operation composition of permutations

a. is not closed ✓

b. is closed

Your answer is correct.

The correct answer is:

is not closed

Question 14

Incorrect

Mark 0.00 out of 1.00

Let $h : \mathbb{Z}_{2^{512}} \rightarrow \mathbb{Z}_{2^{256}}$ be a hash function

defined as $h(x) = (155x^4 + 201x^3 + 2x^2 + 101x + 1) \pmod{2^{256}}$.

Is h second preimage resistant?

a. yes



b. no

Your answer is incorrect.

The correct answer is:

no

Question 15

Correct

Mark 1.00 out of 1.00

```
If AES-Mixcolumn(23, 67, 89, 45) = (x,y,z,w) then w =
```

```
[here input and output are in integer]
```

 a. 87 b. 145 c. 121 ✓ d. 159 e. none of these

Your answer is correct.

The correct answer is:

```
121
```

Question 16

Correct

Mark 1.00 out of 1.00

SUBBYTES(6A) =

 a. 24 b. 20 c. 34 d. none of these e. 02

Your answer is correct.

The correct answer is:

02

Question 17

Incorrect

Mark 0.00 out of 1.00

Let $F_k = F_{k-1} \oplus Enc(P_k, F_{k-1})$ be an iterated hash function where Enc is theAES-128 encryption algorithm and F_k, P_k each is of 128-bit.The initial F_0 is a 128-bit public data, P_k isthe k -th message block.

Which of the following statement is correct?

 a. The above iterated hash function is a collision resistant hash function b. The above iterated hash function is not a collision resistant hash function

Your answer is incorrect.

The correct answer is:

The above iterated hash function is a collision resistant hash function

Question **18**

Correct

Mark 1.00 out of 1.00

Consider playfair cipher with the key KEYWORD. Which is the correct

ciphertext of the plaintext COMMUNICATION when the plaintext is

encrypted using playfair cipher with the mentioned key.

a. LCQTNTQGRBXFES



b. LCQTNQTGRBXFES

c. LCQTNTQGBRXFES

d. none of these

e. LCQTNTRGBXFES

Your answer is correct.

The correct answer is:

LCQTNTQGRBXFES

Question **19**

Correct

Mark 1.00 out of 1.00

Consider Affine cipher with the key $K=(9, 19)$. Which is the correct

ciphertext of the plaintext INDIA when the plaintext is encrypted

using Affine cipher with the mentioned key.

a. NUGNT

b. NGTNU

c. NGNUM

d. none of these

e. NGUNT ✓

Your answer is correct.

The correct answer is:

NGUNT

Question **20**

Correct

Mark 1.00 out of 1.00

Consider Affine cipher with the key $K=(11, 16)$. Which is the correct ciphertext

of the plaintext MIDSEM when the plaintext is encrypted using Affine cipher

with the mentioned key.

a. SAXIGS

b. none of these

c. SAXGSI

d. SAGXIS

e. SAXGIS



Your answer is correct.

The correct answer is:

SAXGIS

Question 21

Incorrect

Mark 0.00 out of 1.00

Consider one round of Feistel network with the block size 64-bit and

the secret key K of size 32-bit. The round function is defined by

$$f(R_0, K) = S(R_0 \oplus K) \text{ where } S(X) = (X + 1) \bmod 2^{32}.$$

Find the ciphertext for the plaintext = 1 and key K = 1.

a. 2147483648

b. 2147483649

c. 4294967297

d. 4294967296

e. none of these

Your answer is incorrect.

The correct answer is:

4294967297

Question 22

Incorrect

Mark 0.00 out of 1.00

Let P , C , K be the plaintext space, ciphertext space and key space respectively.

Consider an encryption algorithm E with the following conditions:

1. $|P| = |C| = |K|$
2. every key is equiprobable
3. for every $p \in P$, $c \in C$ there is an unique key k such that $E(p, k) = c$,

Select the most appropriate option

- a.
- b.
- c.

Your answer is incorrect.

The correct answer is:

Question 23

Correct

Mark 1.00 out of 1.00

Encryption of CBC mode of operation can be implemented in parallel

- a.
- b.

Your answer is correct.

The correct answer is:

Question 24

Correct

Mark 1.00 out of 1.00

Let F denotes the AES-128 bit encryption algorithm.

Define a function $f : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ as

$f(x) = F(x, K) \oplus x$, here x, K are of 128-bits and K is a fixed secret key.

Which of the following statement is correct?

a. f is not an one-way function

b. f is an one-way function ✓

Your answer is correct.

The correct answer is:

f is an one-way function

Question 25

Correct

Mark 1.00 out of 1.00

S-boxes in DES map

a. 2 bits to 4 bits

b. 4 bits to 6 bits

c. none of these

d. 4 bits to 4 bits

e. 6 bits to 4 bits



Your answer is correct.

The correct answer is:

6 bits to 4 bits

Question **26**

Correct

Mark 1.00 out of 1.00

Expanded key size of AES-256 is

a. 56 words

b. 44 words

c. 60 words ✓

d. none of these

e. 48 words

Your answer is correct.

The correct answer is:

60 words

Question 27

Correct

Mark 1.00 out of 1.00

Let $h : \{0,1\}^* \rightarrow \{0,1\}^n$ be a preimage resistant and collision resistant

hash function. Define a new hash function $h' : \{0,1\}^* \rightarrow \{0,1\}^{n+1}$

by using following rule $h'(x) = 0||x$ if $x \in \{0,1\}^n$,

otherwise $h'(x) = 1||h(x)$. Which of the following statement is true.

a. h' is neither preimage resistant nor collision resistant

b. h' is not a preimage resistant but collision resistant

c. h' is a preimage resistant as well as collision resistant

Your answer is correct.

The correct answer is:

h' is not a preimage resistant but collision resistant

Question **28**

Incorrect

Mark 0.00 out of 1.00

What are the correct values of x, y such that $23x+43y=\gcd(23,43)$?

a. none of these

b.

c.

d. X

e.

Your answer is incorrect.

The correct answer is:

Question 29

Incorrect

Mark 0.00 out of 1.00

Which is the multiplicative inverse of $(x^4 + x^3 + x + 1)$ in $(\mathbb{F}_2[x])/<x^8 + x^4 + x^3 + x + 1>, +, *$.

Here + and * are the polynomial addition and polynomial multiplication under modulo $x^8 + x^4 + x^3 + x + 1$.

a. $x^7 + x^6 + x^3 + x^2$

b. $x^7 + x^6 + x^3 + x^2 + 1$

c. $x^7 + x^6 + x^2 + x + 1$

d. $x^7 + x^6 + x^5 + 1$

e. none of these

Your answer is incorrect.

The correct answer is:

$x^7 + x^6 + x^3 + x^2$

Question **30**

Incorrect

Mark 0.00 out of 1.00

Consider one-bit encryption $C = P \oplus K$. If $Pr[K = 0] = 0.5$ and $Pr[P = 1] = 0.3$

then $Pr[P = 0 | C = 1]$ is

a. none of these

b.

c.

d.

e. X

Your answer is incorrect.

The correct answer is:

Question 31

Incorrect

Mark 0.00 out of 1.00

A sequence of plaintext blocks x_1, \dots, x_n are encrypted by

using AES-128 in CBC mode. The corresponding ciphertext blocks

are y_1, \dots, y_n . During transmission y_1 is transmitted incorrectly

(i.e., some 1's are changed to 0's and vice versa).

The number of plaintext blocks that will be decrypted incorrectly is

a. 3

b. 2

c. n

d. none of these

e. 1



Your answer is incorrect.

The correct answer is:

2

Question 32

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in CFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in CFB mode of operation.

Now to decrypt the ciphertext which of the following process needs to be followed

a. decryption of AES-128 needs to fit in CFB mode



b. encryption of AES-128 needs to fit in CFB mode

Your answer is incorrect.

The correct answer is:

encryption of AES-128 needs to fit in CFB mode

Question 33

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in OFB mode of operation. Now to decrypt the

ciphertext which of the following process needs to be followed

a. decryption of AES-128 needs to fit in OFB mode



b. encryption of AES-128 needs to fit in OFB mode

Your answer is incorrect.

The correct answer is:

encryption of AES-128 needs to fit in OFB mode

Question **34**

Correct

Mark 1.00 out of 1.00

Consider playfair cipher with the key MIDSEM. Which is the correct

ciphertext of the plaintext VADODARA when the plaintext is

encrypted using playfair cipher with the mentioned key.

a. none of these

b. MHELMCPC



c. MHLEMCP

d. MHEMLCPC

e. MHELCMP

Your answer is correct.

The correct answer is:

MHELMCPC

Question 35

Correct

Mark 1.00 out of 1.00

Let $n = p \times q$ where p, q are two large primes.

Here n is known to everyone and p, q are hidden.

Consider the hash function $h(x) = x^2 \pmod n$.

a.



b.

Your answer is correct.

The correct answer is:

Question 36

Incorrect

Mark 0.00 out of 1.00

a.

b.

c.

d.



Your answer is incorrect.

The correct answer is:

Question 37

Correct

Mark 1.00 out of 1.00

If all the 16 round keys of DES are identical then

a. DES encryption and decryption functions will not be identical due to the IP

b. DES encryption and decryption functions will be exactly equal ✓

c. none of these

d. only the last round and first round of DES will be identical

Your answer is correct.

The correct answer is:

DES encryption and decryption functions will be exactly equal

Question 38

Incorrect

Mark 0.00 out of 1.00

Which of the following statement is correct?

a. if encryption function is oneway then decryption is not possible

b. encryption function is oneway if the private key is unknown

c. only hash functions are oneway functions ✗

Your answer is incorrect.

The correct answer is:

encryption function is oneway if the private key is unknown

Question 39

Incorrect

Mark 0.00 out of 1.00

Which is the multiplicative inverse of $(x^3 + x^2 + 1)$ in

$(\mathbb{F}_2[x]/\langle x^8 + x^4 + x^3 + x + 1 \rangle, +, *)$. Here $+$ and $*$ are

the polynomial addition and polynomial multiplication under

modulo $x^8 + x^4 + x^3 + x + 1$.

a. $x^7 + x^6 + x^3 + x^2$

b. none of these

c. $x^7 + x^6 + x + 1$ ✗

d. $x^7 + x^6 + x^5 + 1$

e. $x^7 + x^6 + x^2 + 1$

Your answer is incorrect.

The correct answer is:

$x^7 + x^6 + x^5 + 1$

Question **40**

Correct

Mark 1.00 out of 1.00

Let $h : \mathbb{Z}_{512} \times \mathbb{Z}_{512} \rightarrow \mathbb{Z}_{512}$ be a hash

function defined as $h(x, y) = (ax + by) \bmod 512$, $a, b \in \mathbb{Z}_{512}$.

Which of the following is correct?

a. h is not an ideal hash function



b. h is an ideal hash function

Your answer is correct.

The correct answer is:

h is not an ideal hash function

[◀ Announcements](#)

Jump to...