Date 19/01/24

⇒ One Way Function

$f: X \to Y$ is called a one way f 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)] → Given
q is a prime (large)]

$N = p \times q$ → this computation is easy

Given N find p, q, s.t. $N = p \times q$ is hard

↓

large primes

⇒ Substitution Box:

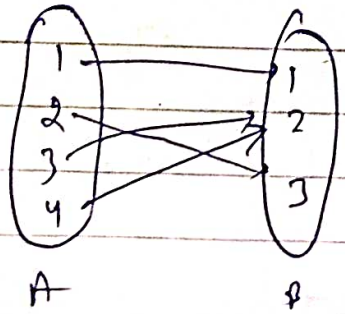
$S: A \to B$ with $|B| \leq |A|$

Mapping from Set A to B, such that no. of elements in B set is less than or equal to no. of elements in set B.

Ex $S: \{1,2,3,4\} \longrightarrow \{1,2,3\}$

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

There will be more than one element in A which is mapped to same element in B.



Spiral

Date .....

⇒ Transposition Cipher

$M = m_1 m_2 \dots m_t$ → plaintext

We have permutation e on t elements → Secret key $\{1, 2, \dots t\}$

Encryption

$c = m_{e(1)} m_{e(2)} \dots m_{e(t)} = c_1 c_2 \dots c_t$

↳ Ciphertext

Decryption

$m = c_{e^{-1}(1)} c_{e^{-1}(2)} \dots c_{e^{-1}(t)}$

Ex: Plaintext $M = CAESAR = m_1 m_2 \dots m_6$

Secret key e:

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
6	4	1	3	5	2

Ciphertext $c = RSCEAA = c_1 c_2 \dots c_6$ ⇒ Encryption

$d = e^{-1}$:

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
3	6	4	2	5	1

⇒ Decryption.

⇒ Substitution Cipher

$M = m_1 m_2 \dots m_t$

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

Spiral

Date .....

e : substitution from A to A.

e → Secret key.

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

~~$d = e_t$~~

Here, we will assume d codomain is of same size, as we will have many choices of plaintext during decryption.

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

ABC → plaintext

ZDA → Ciphertext

⇒ Affine Cipher

A	B	C	...	Z
↓	↓	↓		↓
0	1	2		25

We will consider every alphabet as integers

A → Set of alphabets $Z_{26} = \{0, \dots 25\}$

$A \longrightarrow Z_{26}$ x: Plaintext $x \in Z_{26}$

We will consider,

K = Secret key $= (a, b) \in Z_{26} \times Z_{26}$

Encryption fun^n. $e(x, k) = (ax + b) \bmod 26$

$= c$ (Ciphertext)

y will get encryption value between 0 to 25.

Spiral

Date .....

Decryption fn $d(c,x) = ((c-b)a^{-1}) \bmod 26$

$a \times a^{-1} = 1 \bmod 26$

$((c+26-b)a^{-1}) \bmod 26$

$= (ax+b+26-b)a^{-1}$

$= (ax)a^{-1} + 26a^{-1}$ → 0 as it is divisible by 26

$= x$

→ Affine Cipher $Z_{26} = \{0, 1, \ldots, 25\}$

Secret key $K = (a,b) \in Z_{26}^* \times Z_{26}$ $\gcd(a,26) = 1$

$Z_{26}^* = Z_{26} - \{0\}$

Plaintext $x \in Z_{26}$

$C = E(x,K) = (ax+b) \bmod 26$

Ex ⇒ $Z_6 = \{0, 1, 2, 3, 4, 5\}$ $x, y \in Z_6$

$+ \bmod 6 : +_6 \rightarrow z = (x+y) \% 6$

$+_6$	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						
5						

Spiral

Date .....

$x, y \in Z_6$

$*_6$	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)

Th

$x * y = z \% 6.$

$= y = x *_6 y$

1 is the multiplicative

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

$\phi(n)$: of x $\gcd(d(x,n)) = 1$

There is no element is 2 to 5, such that if we multiply with any no. between 1 to 5, such that remainder is 1.

$a \times b^{-1}$ such that multiplying a with b^{-1} gives 1.

$a/b = a * b^{-1} \bmod n$ s.t $\gcd(b,n) = 1$

→ If $n = p.q$

No. of elements which are co-prime to n (from 1 to n-1) will be

$\phi(n) = (p-1)(q-1)$

gcd (element , n) = 1

↳ element in $\phi(n)$.

Spiral

$0 \neq x \in Z_m$ $\quad gcd(x, m) = 1$

$\Rightarrow x * m\ y = 1$ Date .....

$x * y \equiv 1 \pmod m$

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

$xy - 1 = tm$

$1 = t, m + xy \quad \Rightarrow gcd(m, x)$

So, $g(d(a,b)) = a.s + b.t$.

s, t can be found using ~~Extended~~ Euclidean Algo

How to find s & t (after as $t, & y$)

Ex $\quad m = 17 \rightarrow x = 3$

$3 \overline{)17\ (5}$ $\quad 15$

$2 \overline{)3\ (1}$ $\quad 2$

$1 \overline{)2\ (2}$ $\quad 2$

0

$1 = am + yx$

$1 = 3 - (1 \times 2)$

$= 3 + (-1)2$

$= 3 + (-1)\{17 - 5 \times 3\}$

$= 3 + (-1)17 + 5 \times 3$

$= 6 \times 3 + (-1) \times 17$

6 inverse of 3

$6 \times 3 = 18$

$18 \bmod 17 = 1$

Spiral

Date .....

⇒ Playfair Cipher

Secret key = playfair example. $\quad I = J$

We will discard one element to take 5 x 5 matrix

~~H A Y F~~ $\quad$ Plaintext : HIDE

Break into 2 size.

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

↑ We will not write duplicates

Left over alphabets.

H I $\quad$ D E

↓ $\quad$ ↓

B M $\quad$ O D

Ciphertext : BMOD

We will form square & will take last element (for diagonal elements)

⇒ For same column, we will take below element (Cyclic order)

⇒ For same row, we will take next element. (Cyclic order)

⇒ For odd length add X.

~~Ex - SACHIN~~ $\quad$ Ex - BALL

BALX LX

Add extra X to make the msg. of even length.

⇒ Decryption

B M O D $\quad$ Do opp. of encryption

Same function ✓ do opposite

IM → RI

↓

HM

Spiral

Hill cipher

Date 23/01/24

$A = \{A, B, \ldots Z\}$

$E_S(M) = S(M_1) \cdots S(M_2) = C$

26^{26}, $26! = 2^{90}$ — total no. of bijective mapping

$\Rightarrow C = C_K(x) = (ax+b) \bmod 26$

$K = (a, b) \quad 0 \le a, b \le 25$

Total no. of keys for affine $= 12 \times 26$

$\Rightarrow$ Hill Cipher

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

$M = m_1 m_2 \cdots m_n$ $\rightarrow$ Plaintext

(Ciphertext) $C = A \cdot M$ $\rightarrow$ En. algo

$C_i = \sum_{j=1}^{n} a_{ij} m_j \quad i = 1, 2, \ldots n$

Decryp. $M = A^{-1} C$ — Dec. algo

Symmetric key cryptography

Block Cipher — Stream Cipher

Spiral

Date .....

Block Cipher: $M = m_0 || m_1 || \ldots || m_n$

Divide message into blocks & consider 1 block at a time & do encryption

for Eg - (m) bits into 4 of 32 bits

DES mode of operation

Encryption: $C = Enc(m_0, k) || Enc(m_1, k) \ldots || Enc(m_n, k)$

length is defined based on encry. algo.

$C = C_0 || C_1 || \ldots || C_n$

$C_i = Enc(m_i, k)$

$Enc(m, k) = C$

$Enc: M(x) \rightarrow C$

Dec $M = Dec(C_0, k) || Dec(C_1, k) || \ldots Dec(C_n, k)$

for DES, Block Size is 64 bits.

for AES, Block Size is 128 bits.

Ex:

$\Rightarrow$ Let length is not div. by Block Size.

$M = \underbrace{m_0}_{n} || \underbrace{m_1}_{n} || \underbrace{m_2}_{\ell}$

$= \ell + 2n$

$\ell < n$

$\ell + r = n$ (We can encrypt with all 0 in last block) (We can also add l_r)

$C_0 = Enc(m_0, k), \quad C_1 = Enc(m_1, k)$

$C_2 = Enc(m_2 || 0^{n-\ell}, k)$

$C = C_0 || C_1 || C_2$

Spiral

Date .....

We will provide the information that we have added $n-1$ 0's.

→ ECB mode of operation → It is a way of doing encryption

$$M = m_0 \,||\, m_1 \,||\, \ldots \,||\, m_n$$

(Ciphertext) $C = Enc(m_0, k) \,||\, Enc(m_1, k) \ldots ||\, Enc(m_n, k)$

ECB is not secure

$$M = m_0 \,||\, m_0 \,||\, \ldots \,||\, m_n$$

(If identical)

$$C = Enc(m_0, k) \,||\, Enc(m_0, k) \ldots ||\, Enc(m_n, k)$$

It is revealing that 1st two blocks have same msg are identical, So, this is not more secure.

⇒ Product Ciphers

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

⇒ Substitution-Permutation Network (SPN)

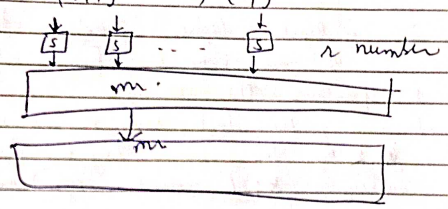
Ques It is a product cipher. There will be one or more substitution box & / or more permutation

Spiral

Date .....

$P: \{0,1\}^{m_2} \longrightarrow \{0,1\}^{m_2}$

$S: \{0,1\}^{n} \longrightarrow \{0,1\}^{m}$

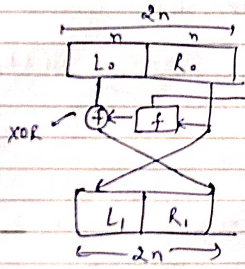


If I repeat this whole computation r no. of times, then this SPN will be of r rounds.

For decryption, just take inverse permutation, & inverse S-BOX

→ Fiestel Network

Encryption:



$f: \{0,1\}^{n} \times \{0,1\}^{k} \longrightarrow \{0,1\}^{n}$

$L_1 = R_0$

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

If we repeat this r times, then this Network is of r rounds.

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

$L_1 = R_0$

So, if f is not invertible, then also we will be able to decrypt.

Spiral

Date .....

* Iterated Block Cipher

It is a Block Cipher involving the sequential repetition of an internal fun^n, called as round fun^n. The parameters are the no. of rounds r, the block size n, & the bit size k of the input key K from which r subkeys k_i (round keys) are derived.

↳ You can generate different keys for different rounds. (Let's say we can left shift by 1 to get new keys)

Ex: 2 round iterated Block Cipher

$F(k_1, P) \rightarrow C_1 \rightarrow F(k_2, C_1)$

P → Plaintext, C → Ciphertext

round = 2

round keys = k_1, k_2

$K \rightarrow G(K) \rightarrow k_1, k_2$

(Secret key → Key Scheduling algo)

Decryption:

$G(K) \rightarrow k_1, k_2$

$C \rightarrow F^{-1}(C, k_2) \rightarrow C_1 \rightarrow F^{-1}(C_1, k_1)$

↓

Plaintext (P)

Spiral

Date .....

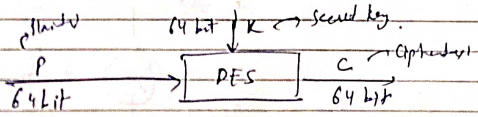
→ Data Encryption Standard (DES)

Designed by IBM.

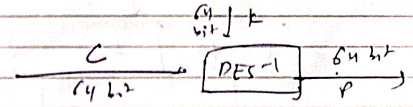
Secret key = 64-bit secret key. (56 bits + 8 parity bits)

Plaintext Block Size = 64-bit

Encryption:



Decryption:



64-bit key

↳ there are 8 parity check bits

0 1 1 1 0 1 1 1 | 1 1 0 0 1 0 1 0 | 1 0 1 0 1 0 1 0

7 bits | parity check bits (i.e. odd 1, even 0)

Actual key size 56 bit + 8 parity bits (We can generate & determine)

DES is based Feistel Network.

→ it is an iterated block cipher

↳ No of rounds = 16

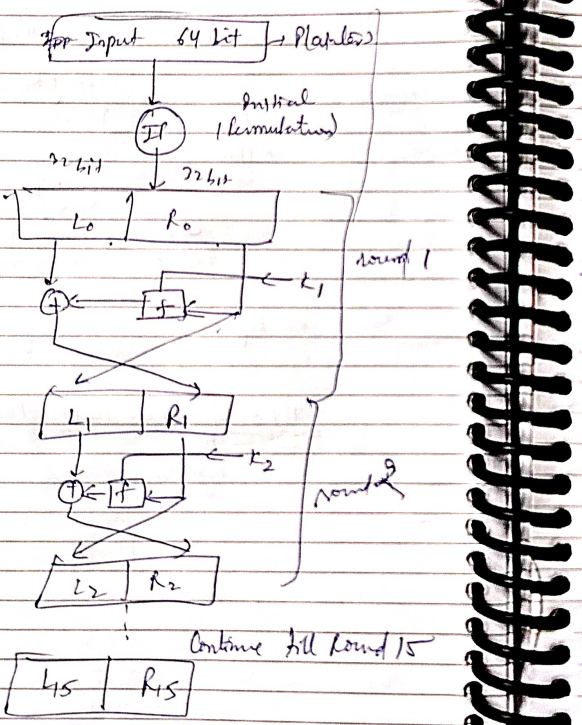
Spiral

Date .....

① Key Scheduling Algo (64 bit key)

$\rightarrow k_1, k_2, k_3 \ldots k_{16}$

k_i's are of 48 bits.

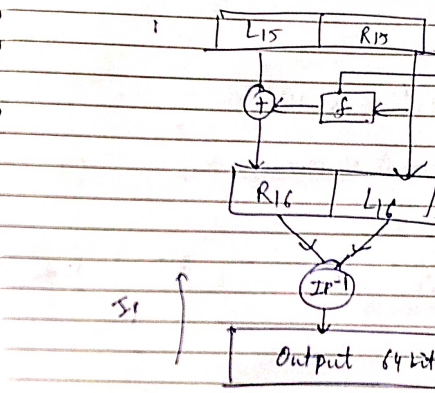


$IP : \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

1st round

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

Date .....



$R_{15} = L_{16}$

31 | 24

Decryption of DES

first do IP of ciphertext.

R_{16} L_{16}

$R_{15} = R_{16} \oplus f(R_{15}, k_{16})$

then and ~~then~~ inverse like this

then IP^{-1} to get back plaintext.

RP:

110

Date .....

1) IP → Design of IP

Front - Non linear of Applied Cryptography

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

$IP(m_1, m_2 \dots m_{64}) = m_{58}\, m_{50}\, m_{42} \dots m_7$

$IP : \left(\underset{58}{1} \quad \underset{50}{2} \quad \underset{42}{3} \quad \dots \quad \underset{7}{64} \right) \rightarrow$ Inverse

position

2) Algorithm of f

$f(R_i, k_i) = X_{i+1}$ (32 bit, 48 bit, 32 bit)

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

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

- P → permutes the position of 32 bits
- S → S-Box, 48 bit input, 32 bit output
- E → function which converts 32 bits to 48 bits

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

$E(x_1 x_2 \dots x_{32}) = y_1 y_2 \dots y_{48}$

Spiral

Date .....

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

Repetition

$E(x_1, x_2, x_3 \dots x_{32}) = (x_{32}, x_1, x_2, x_3, x_4 \dots x_{32}, x_1)$

We are repeating the last two column values.

⇒ S-box of f

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

$S(X) = Y$, X → 48 bits, Y → 32 bits

$X = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$ (8 Blocks)

length of B_i is 6-bits

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

Mapping S_i for each B_i from 6 bits to 4 bits

$S_i : \{0,1\}^6 \rightarrow \{0,1\}^4$ for all $i = 1, 2 \dots 8$

$S_i(B_i) = C_i$ (6 bit, 4 bit)

$S(X) = (S_1(B_1), S_2(B_2) \dots S_8(B_8))$

Spiral

Date .....

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

$S_i(B_i) = C_i$

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

$x = (2 \times b_1 + b_6) \quad 0 \le x \le 3$

C = integer representation $(b_2 b_3 b_4 b_5)$

$0 \le C \le 15$

S_i :

	0	1	2	... 13 - 15
0	a_{00}	a_{01}	a_{02}	...
1				
2				
3				

output $0 \le x \le 15$, $0 \le a_{ij} \le 15$

4×16

⇒ Permutation

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

$P(x_1 x_2 \dots x_{32}) = (x_{16} x_7 x_{20} x_{21} \dots x_{25})$

P_1 :	16	7	20	21
	29	12	28	17
	1	15	23	26
	5	18	31	10
	2	8	24	14
	32	27	3	9
	19	13	30	6
	22	11	4	25

Spiral

Date .....

⇒ Key scheduling algorithm of DES

k → key size of DES ⇒ 56 + 8

First ~~delete parity check bits~~

$k_1, k_2 \dots k_{16}$

48 bit 48 bit 48 bit

Input : 64 bit key $k = k_1 \dots k_{64}$

Output : 16 round keys k_i, $1 \le i \le 16$, where length of k_i is 48 bit

i) Define $1 \le i \le 16$, v_i where $v_i = 1$, if $i \in \{1,2,9,16\}$ (i round)
otherwise $v_i = 2$

ii) Discard 8 parity check bits $\tilde{k}$.

iii) $T = PC1(\tilde{k})$ $\quad PC1 : \{0,1\}^{56} \to \{0,1\}^{56}$

iv) $(C_0, D_0) = T$, length $C_0 = 28$ bits, $D_0 = 28$ bits

v) for $i = 1$ to 16

$C_i \leftarrow (C_{i-1} \overset{\text{left 2 right component}}{\hookleftarrow} v_i)$ ↩ left Circular shift

$D_i \leftarrow (D_{i-1} \hookleftarrow v_i)$

$k_i = PC2(C_i, D_i)$

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

→ round key for i^{th} round.

Spiral

Date ....

PC1 : C_0

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

D_0

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$PC1(k_1, k_2 \ldots k_{63} k_{64}) = PC1(k_1, k_2, k_3 \ldots k_7, k_9, k_{10} \ldots k_{57}, k_{17}, k_{63})$

$= k_{57}\, k_{49}\, k_{41}\, k_{33}\, k_{25}\, k_{17} \ldots k_{36}$ ... k_4

⇒ In this PC1, we are just permuting the ~~places~~ positions

⇒ If the keys are complement, then the output will also be complement)

$PC_1(\overline{k_1}, \overline{k_2} \ldots \overline{k_{64}}) = \overline{k_{57}}\ \overline{k_{49}} \ldots \overline{k_4}$

$= \overline{PC_1(k)}$

14th ~~position~~ input bit will come at 1st position output

P.C₂ 14 17 11 24 1 5
3 28
...

Spiral

Date ....

⇒ $DES(M, k) = C$

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

$KS(k) = k_1, k_2 \ldots k_{16}$

$KS(\overline{k}) = \overline{k_1}, \overline{k_2} \ldots \overline{k_{16}}$

& every round key of KS of $\overline{k}$ will be complement of each round keys of ~~input~~ k.

$IP(M)$, $IP(\overline{M})$

They will also be complemented

So, it is keeping com. to com.

M		$\overline{M}$	
L_0	R_0	$\overline{L_0}$	$\overline{R_0}$
L_1	R_1	$\overline{L_1}$	R_1

↳ it is put same as R_0

$R_1 = L_0 \oplus f(R_0, k_1)$ $\qquad$ $R_1 = \overline{L_0} \oplus f(\overline{R_0}, \overline{k_1})$

$E(\overline{R_0}) = \overline{E(R_0)} \oplus \overline{k_1}$

$= E(R_0) \oplus k_1$

↳ $\overline{R_1} = \overline{L_0} \oplus f(R_0, k)$
$\overline{R_1}$

So R_1 will also be complement.

Date .....

Next is only IP which will also be complement
So, ~~Cipher~~ Ciphertext.

Exhaustive Search or Brute Force attack : = 2^{56} (56 bit key)

Total no. keys (S) $K_1, K_2 \dots K_{256}$

Choosen Plaintext Attack on DES

$K_1, K_2 \dots K_{256}$

M, $\overline{M}$

$DES(M, K) = C_1$

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

Attacker

$DES(M, K_i) = \overline{C_1}$ $DES(\overline{M}, \overline{K_i}) = \overline{C}$

if $\overline{C_i} \neq C_1$ → discard K_i from S. → $K_i \neq K$

if $\overline{C} \neq C_2$ discard $\overline{K_i}$ from S. → $\overline{K_i} \neq K$

If it is true then $K = \overline{K_i}$

So, we will be able to find key is 2^{55} instead of 2^{56} because we can discarding 2 keys.

Spiral

Date ...2/2/24...

Attack models

① Ciphertext only attack

Attacker is getting only ciphertext.
Goal : to get back the plaintext or recover the secret key.

2) Known plaintext attack

Attacker knows some plaintexts & corresponding ciphertexts.
Goal : find a plaintext corresponding to a different ciphertext or find the secret key of the system.

3) Choosen plaintext attack

Attacker chooses some plaintexts of his/her choices & he/she is allowed to get the corresponding ciphertext.
Goal : Generate a new plaintext, ciphertext pair or find the secret key.

4) Choosen ciphertext attack

Attacker chooses some ciphertext & she/he is provided with the corresponding plaintexts
Goal : Generate a different valid plaintext, Ciphertext pair or find the secret key.
It is the strongest attack in public key cryptography because assumption secret key is playing a role. but in symmetric key cryptography, choosen plaintext & ciphertext is almost same strong. because there is same key

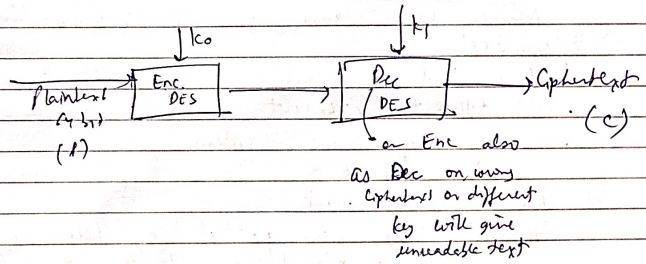
Spiral

Date .....

Double DES

⇒ To make it more secure, do 2 Encryption
DES is providing 56-bit security.
$2 \times 56 = 112$ -bit security

$k \rightarrow 128$ - bit $= (k_0, k_1)$
Among this 128 bits there are 16 parity check bits.



If we perform Exhaustive search, time complex. will be 2^{112}

Double DES

Attacker is having one valid plaintext, ciphertext pair. Assume known plaintext model

P_1 ⟶ Double DES

Select k_i

$Enc_{DES}(1, K_i) = X_i$ $\quad (X_i, k_i)$ Table 1

$Enc_{DES}(C_i, k_j) = Y_j$ $\quad (Y_j, k_j)$ Table 2

Spiral

Date .....

Problem-1 : leaf nodes utilities values generated from matlab. are:

$u_1 = 6 \quad u_2 = 19 \quad u_3 = 15 \quad u_4$

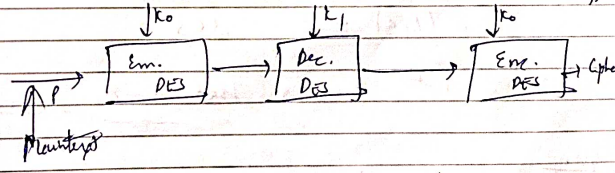
if $X_i = Y_j$, then $(k_i, k_j) \rightarrow$ Secret key.

Here both Table 1 & Table 2, both these tables are not dependent on each other, so, time Comp. will be added $2^{28} + 2^{28} = 2^{57}$ time Complexity

Increasing the length of secret key for any encryption algo does not mean increase the security.
So, we if we use 2 secret keys, complexity will still be 2^n instead of 2^{2n}.
⇒ It is known as meet in the middle attack

Triple DES

Secret key $k = (k_0, k_1)$ 2 keys 3 Encryption



We can use any combination of Enc - Dec -

So, here to meet, we will have to perform Dec on k_1 for every value of k_0 so it will get multiplied.
It will give 2^{2n} bit security (n size of key)

Spiral

Date .....

⇒ Let's say we have a algorithm, which claim n-bit security using exhaustive search (2^n). But if we have Quantum or super computer, TC will reduce to $2^{n/2}$.

To get n bit security we will use 2 keys in Triple Enc setup.

⇒ $R \subseteq X \times Y$

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

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

$$*(a,b) = c \quad \text{where } a,b,c \in S$$

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

it is not necessary that $d = c$.

⇒ **Group**

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

I) The group operation is associative —

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

Spiral

Date .....

Problem 1: Leaf node utility values generated from matlab are:

$u_1 = 6$ $u_2 = 19$ $u_3 = 15$ $u_4 = 14$ $u_5 = 5$
$u_6 = 7$ $u_7 = 17$ $u_8 = 19$ $u_9 = 13$ $u_{10} = 9$
$u_{11} = 12$ $u_{12} = 2$ $u_{13} = 16$ $u_{14} = 4$ $u_{15} = 10$ $u_{16} = 1$

(II) There is an element $I \in G$, called the identity element such that

$$a * I = I * a = a \quad \forall \; a \in G,$$

(III) For each $a \in G$, there exists an element $a^{-1} \in G$ called the inverse of a such that

$$a * a^{-1} = I = a^{-1} * a \quad \forall \; a \in G.$$

6	19	15	14	5	7	17	19	13	9	12	8

A group G is abelian (or Commutative) if $a * b = b * a \quad \forall \; a,b \in G$

* 1. Matrix multiplication over sq. matrices of order $n \times n$

$$A * B \neq B * A$$
$$A * B \neq B * A$$

I) $A * (B * C) = (A * B) * C$
II) $A * I_n = A = I_n * A$
III) $A * A^{-1} = I_n = A^{-1} * A$

Set of all invertible matrices under matrix multiplication operation forms a group.

$(G, *)$

Spiral

Date .....

1) Z : set of integers

$(Z, +)$

a) $a+(b+c) = (a+b)+c \quad \forall a, b, c \in Z$

b) 0 : identity elem

$a+0 = a = 0+a \quad \forall a \in Z$

c) for every $a \in Z$, there exists $-a \in Z$, s.t.

$a+(-a) = 0$

$(-a)+a = 0$

It is commutative group

2) $(Z, \times)$

i) $(a \times (b \times c)) = (a \times b) \times c \quad \forall a, b, c \in Z$

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

iii) $a \in Z$ there does not exist $a^{-1} \in Z$.

3) $(Z, -)$

4) (Q : set of all rational number.)

$*$: ordinary multiplication

$(Q, *) \quad , \quad (Q - \{0\}, *)$

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

ii) for every $a \in Q$ there exists $1 \in Q$

s.t. :

Date .....

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

⇒ $(Z_n, +_n)$ $\quad Z_3 = \{0, 1, 2\}$

$x, y \in Z_n \quad Z_n \{x \bmod n\}$

$a \in Z_n \quad , n - a \in Z_n.$

⇒ $(Z_n, *_n)$ where $*_n$: multiplication mod n

$a, b \in Z_n.$

$a *_n b = (a \times b) \bmod n$

$Z_n - \{0\}$.

$a \in Z_n$

$a * b \equiv 1 \pmod n$

If I divide $a \times 3$ by n, then I will get 1 as a remainder

---

$U_n = \{x \in Z_n - \{0\} \mid \gcd(x, n) = 1\}$

, under this $\bmod n$ operation it will form a group.

$Z_p - \{0\} = Z_p^*$ $\quad p$ - prime.

$*_p$

Date ... 6/2/24

→ A non empty subset H of a group $(G, *)$ is a subgroup of G if H is itself a group with respect to the operation $*$ of G. If H is a proper subset of group w.r.t $*$ of G & $H \neq G$ then H is called a proper subgroup of $(G, *)$

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

→ $(G, *)$ is a group.

$a \in G \Rightarrow a * a \in G, \quad a * a * a \in G$

$a * a = a^2 \qquad a * a * a = a^3 \in G$

$a * a * a * a = a^4$

↳ Notation, not by mathematically

$a^i = \underbrace{a * a * \dots * a}_{\text{many operation } *} \in G$

→ 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 $(G, *)$

→ Order of an element $a \in G$ $O(a)$ is the least positive integer m s.t. $a^m = e$, e is the identity element of G.

operating in terms (its not multiplication)

Spiral

Date .....

Ex $Z_5, *_5$ $\quad x *_5 y = (x \cdot y) \bmod 5$

(identity = 1)

$4 \in Z_5$

$4^0 = 1, \quad 4, \quad 4^2 = 16 \quad 14 \bmod 5 = 1$

$O(4) = 2$

→ $a \in G$, $a \neq e$, e is the identity element of G.

$O(a) = 5, \quad a^5 = e \rightarrow$ given $(G, *)$

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

$S = \{e, a, a^2, a^3, a^4\}$

i) $S \subseteq G$
ii) $(S, *)$ will be group or not.

$(S, *)$ is a subgroup of $(G, *)$

→ inverse of all elements exist in S ($a \to a^4$, $a^2 \to a^3$)

All elements in S are generated by a only. So, a is cyclic subgroup of G.

→ If G is a group & $a \in G$, then the set of all powers of a will form a cyclic subgroup generated by a & denoted by $\langle a \rangle$.

→ Let G be a group & $a \in G$ be an element of finite order t, then $|\langle a \rangle| = t$

Date .....

denotes the size of the subgroup generated by a & equal t.

⇒ Lagrange's Theorem

If G is a finite group & H is a subgroup of G, then $|H|$ divides $|G|$.

Ex $a \in G$, $O(a)$

$S = \{e, a, a^2, \ldots, a^{O(a)-1}\} = \langle a \rangle$

$(S, *) \rightarrow$ Subgroup of $(G, *)$

$|S| \mid |G|$

$\Rightarrow O(a) \mid |G|$

* (1) If the order of $a \in G$ is t, then the order of a^k will be $\frac{t}{\gcd(t,k)}$

$\langle a \rangle = \{e, a, \ldots a^{O(a)-1}\}$

$\langle a^t \rangle = \{e, a^t, a^{2t}, \ldots (a^t)^{O(a^t)-1}\}$

$b = a^t$

$\langle a^t \rangle = \langle b \rangle = \{e, b, b^2, \ldots b^{O(b)-1}\}$

if $\gcd(t, O(a)) = 1$

$O(a^t) = O(a)$

Date .....

⇒ ~~Z_{15}^*~~ =

~~Ex~~ ⇒ Ring:

A ring $(R, +_R, \times_R)$ consists of a set R with two binary operations arbitrarily denoted by $+_R$ (addition) & $\times_R$ (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.,
$a \times_R (b \times_R c) = (a \times_R b) \times_R c$
$\forall\ a, b, c \in R$.

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

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

Date .....

Example: $(\mathbb{Z}, +, \cdot)$: Check Ring or not

1) $(\mathbb{Z}, +)$: abelian group.

2) a,) $a + (b+c) = (a+b)+c$

b) $a + 0 = 0 + a = a$

0: Identity element

c) $a + (-a) = 0 = (-a) + a$.

2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad , \forall a, b, c \in \mathbb{Z}$.

3) $a \times 1 = a = a \times a$

1: Identity element

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

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

$(R, +_R, \times_R)$

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

then it is a commutative Ring

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

Ex: 1 is the unit element in $\mathbb{Z}(+, \cdot)$.

→ The set of units is a Ring R forms a group under multiplication operation.

This is known as group of units of R.

Spiral

Date .....

⇒ Field

A field is a non empty set F together with two binary operations + (addition) & * (multiplication) for which the following properties are satisfied.

1) $(F, +)$ is an abelian group.

2) If 0_F denote the additive identity element of $(F, +)$ then $(F - \{0_F\}, *)$ is a commutative / abelian group.

3) $\forall a, b, c \in F$, we have $a * (b+c) = (a*b) + (a*c)$

Ex $(\mathbb{Z}, +, \cdot) \rightarrow$ field ✗ (Inverse not there)

$(\mathbb{Q}, +, *) \rightarrow$ field ✓

0 : additive identity

1 : multiplicative identity

$(\mathbb{Q} - \{0\}, \cdot) \rightarrow$ Commutative group.

⇒ $\mathbb{F}_p = \{0, 1, 2, \ldots p-1\}$

p : prime number.

$(\mathbb{F}_p, +_p, *_p)$: Field.

$+_p : (x+y) \pmod p$ (Inverse : $p-x$)

$*_p : (x-y) \pmod p$

Spiral

Date .....

x^{-1} · Inverse in multiplication
· if $gcd(x, p) = 1$ which will be true if p is a prime number.

⇒ Field Extension

Suppose K_2 is a field with addition $+$ & multiplication $\times$. Suppose $K_1 \subseteq K_2$ is closed under both these operations such that K_1 itself is a field for the restrictions of $+$ and $\times$ to the set K_1. Then K_1 is called a subfield of K_2 & K_2 is called a field extension of K_1.

⇒ F → field . $(F, +, \times)$

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

↑ Polynomial ring

$F[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \mid a_i \in F\}$

Spiral

Date .....

$a_i + b_i$: addition operation in the field F.

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

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

⇒ $\mathbb{F}_2 = \{0, 1\}$, $(\mathbb{F}_2, +_2, *_2)$

$\mathbb{F}_2[x] = \{a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_2\}$
⇒ it will be a field. a_i is either 0 or 1

Ex: $p(x) = x + 1$, $q(x) = x^2 + x + 1$

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

$(1+1) \pmod 2$
$(1+1) \pmod 2$
$0+1 \pmod 2$

We will add coefficient of x^i term in field form.

For multiplication
$p(x) \cdot q(x)$
$(x+1) * (x^2 + x + 1)$
$(1 * 1) + (1*1)x + (1*1)x^2 + (1*1)x^3$
(1 * x² + x * x) done for coeff 1. (x³)
$= 1 + x^3$

Spiral

Date .....

⇒ A polynomial $p(x) \in F[x]$ of degree $n \geq 1$ is called irreducible of it cannot be written in the form $p_1(x) * p_2(x)$ with $p_1(x)$, $p_2(x)$ & degree of $p_1(x)$, $p_2(x)$ must be ≥ 1.

⇒ $I = \langle p(x) \rangle = \{ q(x).p(x) \mid q(x) \in F[x] \}$ (set.)

$(F[x], +, *)$ → ring
↳ Polynomial Ring

For this, we will multiply every $q(x)$ with $p(x)$.

↳ All, the polynomials with $p(x)$ as factor.

⇒ $F[x] / \langle p(x) \rangle$ $(F[x], +, *)$

$p(x)$: irreducible polynomial

$q(x) \in F(x)$.

If we divide $F(x)$ by $p(x)$ & the remainder will be the element of $F[x]$.

→ $q(x) = d(x) * p(x) + r(x)$

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

Date .....

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

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

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

$(F[x] / \langle p(x) \rangle, +, *)$ → mod $p(x)$
↳ mod $p(x)$

It will be a field.

⇒ (x^2+1) in $\mathbb{R}[x]$ $(\mathbb{R}, +, *)$

(x^2+1)
$= q_1(x) \cdot q_2(x)$

$p(x) = q_1(x) \cdot q_2(x)$
$\deg(q_1) \geq 1$
$\deg(q_2) \geq 1$

$\deg(q_1(x)) = 1$
$\deg(q_2(x)) = 1$

↳ It is not a reducible polynomial, as to reduce it will be $(x+i)$ & $(x-i)$ which is complex no. but it is $R(x)$ (Real number). So, it is irreducible.

⇒ $x^2 + 1 = 0$
$x^2 = -1$
$\therefore x = \sqrt{-1} = \pm i$

(x) $(x+\alpha)$ → complex no

Date .....

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

$p(x)$ $\quad +$ → addition mod 2

$x+1 = 0$ mod 2

$x^2+x+1 \to$ irreducible poly.

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

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

We will put $x=0$ & $x=1$

$p(0) = 1$

$p(1) = 1$

So, $(x+0)$ & $(x+1)$ are not the factors of $p(x)$

So, there is no 1 degree factors of the $p(x)$.

So, it is not reducible.

$x^2+x+1 = g_1(x) g_2(x)$

$g_1(x) = 0 \quad$ or $g_2(x) = 0$

$x, x+1$

$x = 0 \qquad x+1 = 0$

$x = 1$

$\mathbb{F}_2[x] / \langle x^2+x+1 \rangle$, $+_{p(x)}$, $\times_{p(x)}$

is a field.

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

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

Date .....

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

$x^2+x+1 \qquad q(x)$ is having a x^2

$x^2 = x+1$

$x^2+x+1 \;\big)\; x^2+1 \;\big(\; 1$

x^2+x+1

x

x^2+1

$(x+1)+1 = x$

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

$= x^2 + x$

$= x+1+x = 1$

We will replace highest degree term with rest of the terms.

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

$= \{0, 1, x, x+1\}$

$x^2+x+1 = 0 \Rightarrow x$: root

$\{0, 1, x, x+1\}$ ← it is quotient

Date .....

Ex: $x^3 + x^2 + 1$

Total 8 degree polynomials.

$x^3 + x^2 + 1 = 0$

{ 0, 1, x, x^2, x^2+1, $x^3+x = x^2+x+1$, ~~x^3+x^2+x~~ =

$x^5 = x^3+x^2+x = x^2+1+x^2+x = x+1$,

$x^6 = x^2+x$

$x^7 = x^3+x^2 = x^2+1+x^2 = 1$

So, we generated all the 8 polynomials

So, it is primitive.

Ex $x^4 + x^3 + 1$

0, 1, x, x^2, x^3, x^3+1, $x^4+x = x^3+x+1$, $x^4+x^2+x = x^3+x^2+x+1$,

$x^4+x^3+x^2+x = x^2+x+1$, x^3+x^2+x, $x^4+x^3+x^2 = x^2+1$,

x^3+x

Ex $x^3 + x + 1$.

0, 1, x, x^2, $x+1$, x^2+x, x^3+x^2.

Primitive :- Considering a polynomial $P(x) = 0$, if x is a root of $P(x)$ & x is generated all the polynomials of degree < deg($P(x)$). x is said to be primitive.

Spiral

Date .....

AES (Advanced Encryption Standard)

AES → iterated block cipher Substitution Permutation Network (SPN)

AES - 128

i) Block size = 128 bit

ii) Number of rounds = 10.

iii) Secret key size = 128 bits

(Rijndael)

AES - 192

1) Block Size = 128 bits

2) No. of rounds = 12

3) Secret key size = 192 bit.

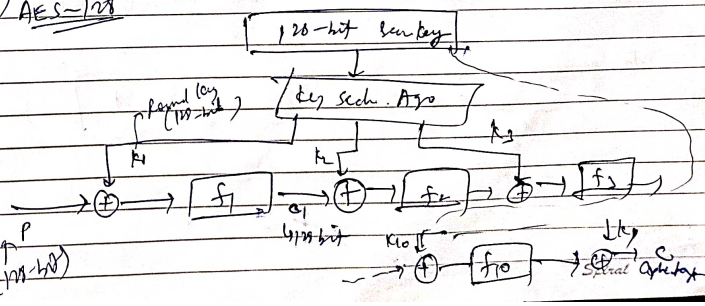
AES - 256

1) BS = 128 bits

2) Round = 14

3) S.K. size = 256 bits

i) AES-128



Date 13/2/24.

Decryption AES

XOR with last key, inverse f^{10}, then XOR, inverse — — —

Round function of AES-128

For AES 128 bits → f_1 to f_9 are exactly same, f_{10} is different

AES 192 bits → F_1 to f_{11} are exactly same

A-17 functions will be same.

First 9 rounds fun^n's (i.e., f_1 — f_9) consists of the following fun^n

i) Sub bytes : $\{0,1\}^{128} \rightarrow \{0,1\}^{128}$

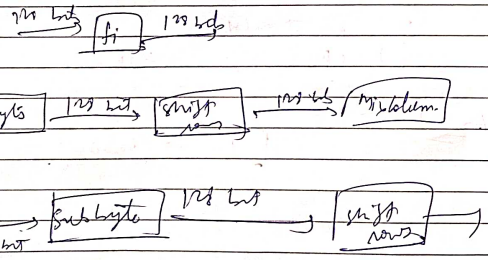
ii) Shift rows

iii) Mix Column

10th round fun^n (i.e., f_{10}) is based on

i) Sub bytes

ii) Shift rows.



Spiral

Date .....

⇒ Sub Bytes

Sub Bytes : $\{0,1\}^{128} \rightarrow \{0,1\}^{128}$

$X = x_0 x_1 x_2 x_3 \text{ —— } x_{16}$

Size of x_i = 8 bit.

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix} \rightarrow \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix}$$

$(S_{ij})_{4\times4}$

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

i) $(\overset{MSB}{C_7} C_6 C_5 C_4 C_3 C_2 C_1 C_0) \leftarrow (\overset{63}{0\,1\,1\,0\,0\,0\,1\,1})_2$

ii) $S(S_{ij}) = (a_7\, a_6\, a_5\, a_4\, a_3\, a_2\, a_1\, a_0)$

iii) for $i=0$ to 7

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

iv) $(b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1\, b_0)$

output = S'_{ij}

Spiral

Date .....

$$\begin{bmatrix} S_{00} & S_{01} & \cdots \\ S_{10} & S_{11} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \longrightarrow \begin{bmatrix} S'_{00} & S'_{01} & \cdots \\ S'_{10} & S'_{11} & \cdots \\ S'_{20} & S'_{21} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}$$

Input of 128 bits + Output 128 bits.

$S(0) = 0 = (0 \ldots 0)$

$b_i = c_i$ (as $a_i = 0$)

$b_0 \ldots b_7 = 63$.

$\Rightarrow S : \{0,1\}^8 \to \{0,1\}^8$

$S(X) = Y$

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

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

$\deg(P(x)) < 8$

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

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

$(\mathbb{F}_2[x] / \langle x^8 + x^4 + x^3 + x + 1 \rangle, +, \times)$ is a field + mod $P(x)$. So, every poly will have a inverse under mod as $P(x)$ is non-zero. (at least one bit will be 1)

Spiral

Date .....

$P(x)$ is a non-zero polynomial $\Rightarrow x^8 + x^4 + x^3 + x + 1 \nmid P(x)$

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

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

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

Example : $S(0\,1\,0\,1\,0\,0\,1\,1) \to \{0,1\}^8 \to \{0,1\}^8$

$0\,1\,0\,1\,0\,0\,1\,1 \longrightarrow x^6 + x^4 + x + 1$

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

$q(x) = x^7 + x^4 + x^3 + x + 1$

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

$q(x)$

$x^6 + x^4 + x + 1 \;\big)\; x^8 + x^4 + x^3 + x + 1 \;\big(\; x^2 + 1$

$x^8 + x^6 + x^3 + x^2$

$x^6 + x^4 + x^3 + x^2 + x + 1$

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

$x^2 \;\big)\; x^6 + x^4 + x + 1 \;\big(\; x^4 + x^2$

x^6

$x^4 + x + 1$

x^4

$x + 1 \;\big)\; x^2 \;\big(\; x + 1$

$x^2 + x$

x

$x + 1$

1

Spiral

Date .....

$$1 = x^2 + (x+1)(x+1)$$
$$= x^2 + \left[(x^6+x^4+x+1) + x^2(x^4+x^2)\right](x+1)$$
$$= (x+1)(x^6+x^4+x+1) + \left[1 + (x^4+x^2)(x+1)\right]x^2$$
$$1 = (x+1)(x^6+x^4+x+1) + (1+x^5+x^4+x^3+x^2)x^2$$
$$= (x+1)(x^6+x^4+x+1) + (1+x^5+x^4+x^3+x^2)$$
$$\left[(x^3+x^4+x^3+x+1) + (x^2+1)(x^6+x^4+x+1)\right]$$
$$= (1+x^5+x^4+x^3+x^2)(x^3+x^4+x^3+x+1) + (x+1+(x^2+1))(1+x^5+x^4+x^3+x^2)(x^6+x^4+x+1)$$
$$= h(x)g(x) + (x+1+x^2+x^3+x^6+x^5+x^4+1+x^5+x^4+x^3+x^2)(x^6+x^4+x+1)$$
$$1 = h(x)g(x) + (x^7+x^6+x^3+x^2)(x^6+x^4+x+1)$$

$(x^7+x^6+x^3+x)$ is the multiplicative inverse of (x^6+x^4+x+1) under modulo $(x^8+x^4+x^3+x+1)$

$$S(01010011) = (11001010)$$
$$= (a_7 a_6 \dots a_0)$$

Spiral

Bus & Net Security — Stinson Book (Douglas)

Date .....

$$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + t(i)) \bmod 2$$

$$b_0 = (a_0 + a_4 + a_5 + a_6 + a_7 + 1) \bmod 2$$
$$= (0+0+0+0+1+1) \bmod 2$$
$$= 1$$

$b_1 = 0$

$(b_7 b_6 \dots b_0) = (11101101)$ (E, D)

Subbyte (01010011) — 5 → row no., 3 → col. no.

$= 1110\,1101$ (E, D)

Subbyte (53) = ED

(256 values (8 bit))

So, we can look at the table (16 × 16 table) for the subbyte value.

→ Shift rows

Shift rows : $[0,1,3]^{in} \rightarrow [0,1,3]^{out}$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \rightarrow \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{bmatrix}$$

Spiral

Date .....

⇒ Mix Column:

Mix Column : $\{0,1\}^{128} \rightarrow \{0,1\}^{128}$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \rightarrow \begin{bmatrix} s'_{ij} \end{bmatrix}_{4\times4}$$

$$s'_{00} = \left(x \times s_{00} + (x+1) s_{10} + 1 \times s_{20} + 1 \times s_{30} \right) \bmod (x^8+x^4+x^3+x+1)$$

Consider the column $C \in \{0,1\}^{32}$

for $i = 0$ to 3

t_i = Binary to poly (s_{ic})

$$t_0 = \left[(x * t_0) + (x+1) * t_2 + t_2 + t_3 \right] \bmod \langle x^8+x^4+x^3+x+1 \rangle$$

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

s'_{ic} = Polynomial to Binary (t_i)

$$S' = \begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \begin{bmatrix} s_{00} & s_{01} \\ s_{10} & s_{11} \\ s_{20} & \\ s_{30} & \end{bmatrix} \bmod (x^8+x^4+x^3+x+1)$$

Spiral

Date ..16/2/..

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

* Mix Column

Mix Column. : $\{0,1\}^{128} \hookrightarrow \{$.

$$S' = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_{00} \\ s_{10} \\ s_{20} \\ s_{30} \end{bmatrix}$$

Spiral

Date .....

Example:

$$\begin{bmatrix} s_{00}' \\ s_{10}' \\ s_{20}' \\ s_{30}' \end{bmatrix} = \begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \begin{bmatrix} s_{00} \\ s_{10} \\ s_{20} \\ s_{30} \end{bmatrix}$$

$s_{00} = 95 \quad s_{10} = 65 \quad s_{20} = FD \quad s_{30} = F1$

$s_{00} = 95 = 1001\ 0101 = x^7+x^4+x^2+1$
$s_{10} = 65 = 0110\ 0101 = x^6+x^5+x^2+1$
$s_{20} = FD = 1111\ 1101 = x^7+x^6+x^5+x^4+x^3+x^2+1$
$s_{30} = F3 = 1111\ 0011 = x^7+x^6+x^5+x^4+x+1$

$(s_{00})x = (x^7+x^4+x^2+1)x$
$= (x^8+x^5+x^3+x) + (x+1)$

$(s_{00})x = (x^7+x^4+x^2+1)x + (x+1)(x^6+x^5+x^2+1)$
$+ (x^7+x^6+x^5+x^4+x^3+x^2+1)$
$+ (x^7+x^6+x^5+x^4+x+1)$

$= (x^8+x^5+x^3+x + x^7+x^6+x^3+x + x^6+x^5+x^2+1$
$+ (x^7+x^6+x^5+x^4+x^3+x^2+1)$
$+ (x^7+x^6+x^5+x^4+x+1)) \bmod (x^8+x^4+x^3+x+1)$

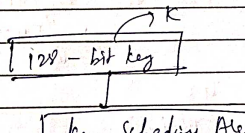
$= x^7+x^4 = 10010000$
$= 90 \rightarrow$ In hexadecimal.

$x^8+x^5+x^3+1$
$(x^4+x^3+x+1)\ (x^5+x^3+1)$
$=$

Spiral

Date .....

⇒ AES – 128 bit key Scheduling Algo.



$k_1, k_2, \ldots, k_{11}$
length of each k_i = 128 bit.

K = key[0], key[1], ... key[15]
length of key[i] = 128 bit - 8 bit
= 128 bit

(i) ROTWORD (B_0, B_1, B_2, B_3)
$= (B_0', B_1', B_2', B_3')$
$= (B_1, B_2, B_3, B_0)$
length of B_i = 8 bit.

(ii) SUBWORD (B_0, B_1, B_2, B_3)
$= (B_0', B_1', B_2', B_3')$
$B_i' =$ Subbytes (B_i)

Rcon[1] = 01000000
Rcon[2] = 02000000
Rcon[3] = 04000000
~~Rcon[4]~~
Rcon[4] = 08000000
Rcon[5] = 10000000

Spiral

Date .....

for i=0 to 3
    w[i] = (key[4i], key[4i+1], key[4i+2], key[4i+3])

for i=4 to 43
    temp = w[i-1]
    if i ≡ 0 (mod 4)
    then temp = SUBWORD (ROTWORD (temp)) ⊕ RCon[i/4]
    w[i] = w[i-4] ⊕ temp.
return (w[0], w[i], ... , w[43])

Each w[i] is of 32 bit, total 44 ws., so 44×32 bits total. On taking 128 bits at one time, there will be 11 blocks.

k_1 = w[0] || w[1] || w[2] || w[3]
k_2 = w[4] || w[5] || w[6] || w[7]
:
k_{11} = w[40] || w[41] || w[42] || w[43]

For decryption:
i) We have to take inverse of each function.
ie, Shift rows, Subbytes & Mix columns
(Invertible) (Invertible) (Invertible Matrix)

Date .....

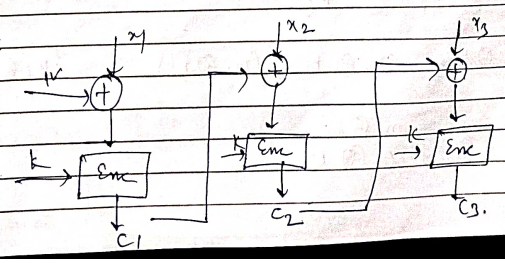
⇒ Modes of Operation

ECB, CBC, CFB, OFB, IGE
4 Most Used.

* ECB
Electronic CodeBook.
Input : key k :, n-bit plaintext $x_1, \ldots x_t$
i) Encry. : $Enc(x_i, k) = C_i$ $1 \le i \le t$.
$C = C_1 \ldots C_t$.
2) Decryption : $Dec(C_i, k) = x_i$ $1 \le i \le t$

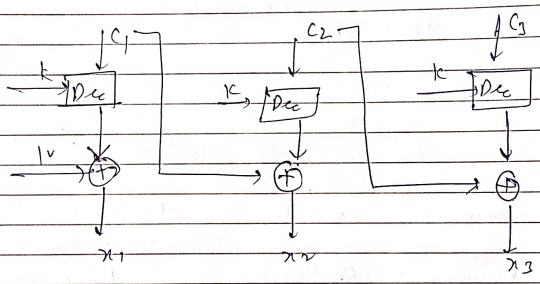
* CBC
Cipher Block Chaining
Input : key k, n-bit plaintext blocks $x_1, x_2, \ldots x_t$
i) Encryption : $C_0 = IV$ (Initial Vector)
$C_j = Enc(C_{j-1} \oplus x_j, k)$
$1 \le j \le t$
ii) Decryption : $C_0 = IV$
$x_j = Dec(C_j, k) \oplus C_{j-1}$
$1 \le j \le t$

Enc



Date .....

Decryption:



⇒ Stream Cipher

⇒ Stream ciphers encrypt bitwise.

$M = m_0 \ldots m_e \; ; \; m_i \in \{0,1\}$

$Enc(m,k) = e(m_0, z_0)\, e(m_1, z_1) \ldots e(m_e, z_e)$

⇒ $M = m_0 m_1 \ldots m_e \quad m_i \in \{0,1\}$

$k = k_0 k_1 \ldots k_e$

$C = M \oplus k = (m_0 \oplus k_0) \cdot (m_1 \oplus k_1) \ldots (m_e \oplus k_e)$

Enc $C_i = m_i \oplus k_i$

Dec $M = C \oplus K$

Date .....

Shannon's Notion of Perfect Secrecy

If the ciphertext of an Algorithm does not reveals any information about the message, it is called as perfectly ~~secure~~ secure algo.

$P_r[M = m_1 \mid C = C_{11}] = P_r[M = m_1]$

⇒ On imposing some conditions, stream cipher will be perfectly secure algorithm.

$m \in \{0,1\}$ $\quad k \in \{0,1\}$

$P_r[m=0] = p$ $\quad P_r[k=0] = 1/2$

$P_r[m=1] = 1-p$ $\quad P_r[k=1] = 1/2$

$c = Enc(m,k) = m \oplus k$

$c \in \{0,1\}$

$P_r[c=0] = P_r[\{m=0, k=0\} \cup \{m=1, k=1\}]$

$= P_r[m=0, k=0] + P_r[m=1, k=1]$

$= (P_r[m=0] \times P_r[k=0]) + (P_r[m=1] \times P_r[k=1])$

$= (p \times 1/2) + (1-p) \times 1/2$

$= p/2 + 1/2 - p/2$

$P_r[c=0] = 1/2$

Similarly $P_r[c=1] = 1/2$

Date .....

$C = Ch_i \mid M = m_1$ (fixed)

$Ch_i = m_1 \oplus K$

$\Rightarrow K = Ch_1 \oplus m_1$

→ Here, this is not known

$\rightarrow Pr[M = m_1 \mid C = Ch_i]$

$= \frac{Pr[M = m_1, C = Ch_i]}{Pr[C = Ch_i]}$

$= \frac{Pr[M = m_1] \times Pr[C = Ch_i / M = m_1]}{Pr[C = Ch_i] = 1/2}$

$= \frac{Pr[C = Ch_1 \oplus m_1] \times Pr[M = m_1]}{1/2}$

$= \frac{1/2 \times Pr[M = m_1]}{1/2}$

$= Pr[M = m_1]$

→ Providing Perfect Secrecy.

---

1) $C = M \oplus K$

$C_1 = M_1 \oplus K$

$C_2 = M_2 \oplus K$

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

If we know that $C_1 \oplus C_2 = 0$, then it is revealing $(M_1 \oplus M_2 = 0)$, So, it is revealed that both are same bits.

Spiral

Date .....

So, we will use different Keys.

$C_1 \oplus C_2 = (1\ 0\ 0\ 0\ 0 - - 1)$

$M_1 \oplus M_2 = (1\ 0\ 0\ 0 - - 1)$

Let's say, we have to encrypt 2 bit message & we have 20 bit key. So, we say we repeat any 1 bit to make it 21 bits. Let's say we repeated 1st bit to the last bit.

$K = k_0 - - - k_n$

$M = m_0 - - m_n$

$K_1 = K \,||\, k_0 - - - k_{n-1}$

$C = M \oplus K_1$

$\tilde{C}_i = C_0 - - C_{n-1}$

$C_{n+1} = m_{n+1} \oplus k_0$

$C_0 = m_0 \oplus k_0$

$C_{n+1} \oplus C_0 = m_{n+1} \oplus m_0$

If this comes 0, then it is revealed that both m_0 & m_{n+1} are same.

⇒ Two Conditions are

1) We can't reuse the same key (You can not use same key to encrypt different messages)

2) $len(K) \geq len(M)$

OTP → One Time Padding

To This is not practical.

Spiral

Date 20/2/24

v) $F(k, IV) = z_i$ $\quad 0 \le i \le n$, length of the output bits will be >>> length of k.
k → Secret key, IV → Public
128 bit

vi) $F(k, IV)$
If we modify atleast one bit of IV or k then there will be an unpredictable change in the output (z_i)

$F(k, IV_1) = z_i^{(1)} \quad 0 \le i \le n-1$
$F(k, IV_2) = z_i^{(2)} \quad 0 \le i \le n-1$

$z_i^{(1)}$, $z_i^{(2)}$ → Uncorrelated.

A
K → Pseudo random bit generator function
$F(k, IV_1) = z_i$
$C_i = m_i \oplus z_i$ $\xrightarrow{C_i, IV_1}$

B
K
$F(k, IV_1) = z_i$
$C_i \oplus z_i = m_i$

$F(k, IV_2) = z_i^{(2)}$
$C_i^{(2)} = m_i^{(2)} \oplus z_i^{(2)}$ $\xrightarrow{C_i^{(2)}, IV_2}$ $F(k, IV_2) = z_i^{(2)}$
$C_i^{(2)} \oplus z_i^{(2)} = m_i^{(2)}$

Spiral

Date .....

Stream Cipher

Synchronous Stream Cipher

Self-Synchronizing or asynchronous stream cipher

≠ Synchronous Stream Cipher

A Syn. Stream Cipher is one in which the key stream is generated independently of the plaintext bits & the ciphertext bits.

State Update function : $S_{i+1} = f(S_i, k)$

Keystream generation fun^n : $z_i = g(S_i, k)$

Ciphertext generation fun^n : $C_i = h(z_i, m_i)$

Here, S_0 is the initial state & may be determined from the secret key k & IV.

• Self Synchronizing / Stream Cipher:

A SSC or asynchronous stream cipher is one in which the keystream bits are generated as a fun^n of the key & a fixed no. of previous ciphertext bits.

State : $\sigma_i = (C_{i-t}, C_{i-t+1}, \ldots, C_{i-1})$
State updat : $\sigma_{i+1} = E(\sigma_i, k)$
key generation fun^n : $z_i = g(\sigma_i, k)$

Spiral

Date .....

Crypto. gen fn ⇒ $C_i = h(z_i, m_i)$

Linear Feedback Shift Register (LFSR)

$s_i \in \{0,1\}$ $i = 0, \ldots, n-1$

| s_{n-1} | s_{n-2} | . — — | s_0 |

Register of length n.
State of length n
can store n-bits.

$t=0$ → Clocking number

$S_0 =$ | s_{n-1} | - - - | s_1 | s_0 |

$t=1$

$S_1 =$ → ⊕ | s_{n-1} | - - - | s_2 | s_1 | → s_0 Output.

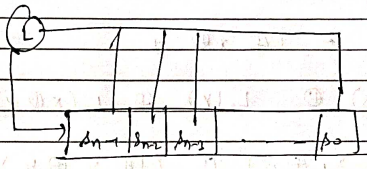
Feedback bit ← $s_n = L(s_0, s_1, \ldots, s_{n-1})$ (linear fn → it is either 0 or 1.)

$= L(S_0)$

$t=2$ $S_2 =$ | ⊕ | s_n | s_{n-1} | - - | s_3 | s_2 | → s_1 output.

Feedback bit ← $s_{n+1} = L(S_1)$

Date .....



$L(s_0, \ldots s_{n-1}) = s_n \in \{0,1\}$

$L : \{0,1\}^n \to \{0,1\}$

* $La = a_0 s_0 \oplus a_1 s_1 \oplus \ldots \oplus a_{n-1} s_{n-1}$

$a_i \in \{0,1\}$

* $L = a_0 s_0 \oplus a_1 s_1 \oplus \ldots \oplus a_{n-1} s_{n-1} \oplus a_n$
$a_i \in \{0,1\}$

$a_n = 0$, $L = La$
$a_n = 1$ $L \neq La$

For non zero a_n, L is known as affine fn.

⇒ if $L(x) \oplus L(y) \oplus L(x \oplus y) = 0$, then L is linear $\forall\, x, y \in \{0,1\}^n$.

Example: $L_1(x,y) = x \oplus y$

$L_1(x) \oplus L_1(y) \oplus L_1(x \oplus y)$
$= (x_1 \oplus x_2) \oplus (y_1 \oplus y_2) \oplus ((x_1 \oplus y_1) \oplus (x_2 \oplus y_2))$
$= 0$

Date .....

Example for Affine fun^n:

$L_2(x,y) = 1 \oplus x \oplus y$

$L_2(x) \oplus L_2(y) \oplus L_2(x \oplus y)$

$= (1 \oplus x_1 \oplus x_2) \oplus (1 \oplus y_1 \oplus y_2)$

$= (1 \oplus x_1 \oplus y_1 \oplus x_2 \oplus y_2)$

$= 1$

Example: $L = s_0 \oplus s_2$ 3 bit LFSR

$t=0$ | s_2 | s_1 | s_0 | 1 | 0 | 1 |

XOR these bits.

$t=1$ | 0 | 1 | 0 | Output 1

feedback

$t=2$ | 0 | 0 | 1 | Output 0

$t=3$ | 1 | 0 | 0 | Output 0

$t=4$ | 1 | 1 | 0 | Output 0

$t=5$ | 0 | 1 | 1 | Output 1

$t=6$ | 1 | 0 | 1 | Output 1

Spiral

Date .....

$t=8 \longrightarrow t=1$

$t=9 \rightarrow t=2$

$t=10 \rightarrow$

We can produce 2^3-1 non-zero states (length of the output) & it will repeat after 7 clocking. (initial state)

If I consider a non-zero initial state.

Ex-2

$L = s_0$ → We will simply consider LSB bit.

$t=0$ | 0 | 0 | 1 |

$t=1$ | 0 | 1 | 0 | Output = 1

$t=2$

⇒ Period of an LFSR

s_0 → non zero initial state : s_0 will be repeated after m Clocking of the LFSR then m will be the period of the LFSR.

$L = s_0 \oplus s_2$ 3 bit LFSR.

Period $= 7 = 2^3 - 1$

⇒ An n-bit LFSR will be full periodic if the period of the LFSR is $2^n - 1$.

Spiral

Flashback of Applied Cryp. (Stream Ciphers)

Date .....

LFSR

i) n - bit register

ii) linear feedback.

$L = s_0$

Period $= 1 \to ?$

$t = 0$ | 1 | 1 | 1 |

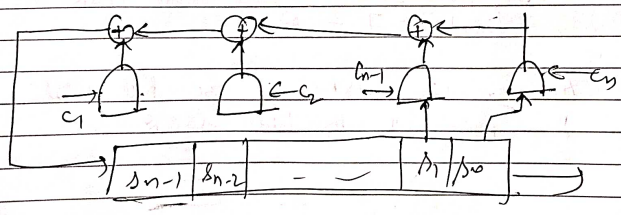
$t = 1$ | 1 | 1 | 1 | $\longrightarrow$ 1

Period $= LCM\{P_1, P_2, \ldots, P_{2^n-1}\}$

$\Rightarrow$ | s_n | s_{n-1} | s_{n-2} | | | . . | s_0 |

$s_n = L(s_0, c_1 s_{n-1} \oplus s_2 \ldots$

$s_{n+1} = L(s_1 \ldots s_n)$



Spiral

Date .....

$L = c_1 s_{n-1} \oplus c_2 s_{n-2} \oplus \ldots c_n s_0$

$f(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_n x^n$ ← Connection poly^n of LFSR

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

deg of conn. poly^n will be atmost n. ← primitive

with LFSR $\longleftrightarrow$ linear feedback

↓

Poly^n of degree n in $\mathbb{F}_2[x]$

$s_0 \to$ repeats after $2^n - 1$ clocking

↑ Full periodic LFSR (feedback poly^n)

i) If conn. poly^n is primitive, then corr. LFSR will be full period $2^n - 1$. (for n- bit LFSR).

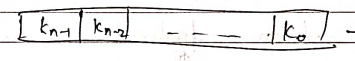
Spiral

Date ..23/2/24

(ii) If the poly^n is irreducible then the period of the LFSR will divide (2^n-1)

(iii) If it is reducible then diff. state will have different cycle length (different period)

⇒ n-bit LFSR



$K = (k_0, \ldots k_{n-1})$

Output bits $x_i \longrightarrow$ key stream bits Z_i

$m_i \oplus Z_i = C_i \rightarrow$ Ciphertext bits

1) Known plaintext attack

$Z_i = m_i \oplus C_i \quad 0 \le i \le n-1$

$Z_0, Z_1, \ldots Z_{n-1}$

$Z_0 = k_0, Z_1 = k_1, \ldots Z_{n-1} = k_{n-1}$

If I give you keystream bits then you will be able to prepare a system of linear eq^{n}s.
By solving the system, you will get the state.

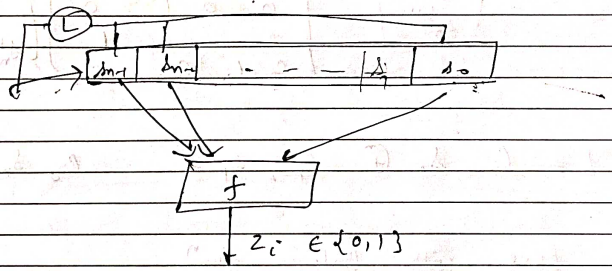
Spiral

Date .....

⇒ LFSR with Non linear filter function

$f : \{0,1\}^l \rightarrow \{0,1\}$ (Boolean Non-linear fun^n)

n-bit LFSR , $n \ge l$



State Update of LFSR
1) Linear feedback
2) Shifting

$C_i = m_i \oplus Z_i$

State update f^n of LFSR is α

$$S_{t+1} = \alpha(S_t)$$

$$Z_{t+1} = f(S_{t+1})$$

t-th State

$s_{n-1}^t, s_{n-2}^t, \ldots, s_0^t$

(t+1)-th State $s_{n-1}^{t+1}, s_{n-2}^{t+1}, \ldots, s_0^{t+1}$

where $s_0^{t+1} = s_1^t$, $s_1^{t+1} = s_2^t$

$s_{n-2}^{t+1} = s_{n-1}^t$, $s_{n-1}^{t+1} = L(s_0^t, s_{n-1}^t)$

Spiral

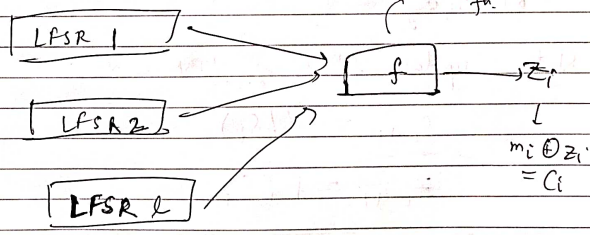
Date .....

$$S^{t+1} = \begin{pmatrix} s_0^{t+1} \\ s_1^{t+1} \\ \vdots \\ s_{n-1}^{t+1} \end{pmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & & & & \ddots & 1 \\ C_{n-1} & C_{n-2} & C_{n-3} & \cdots & C_0 \end{bmatrix} \begin{bmatrix} s_0^t \\ s_1^t \\ \vdots \\ s_{n-1}^t \end{bmatrix}$$

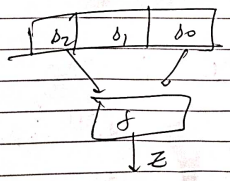
$$L = C_{n-1} s_0 \oplus C_{n-2} s_1 + \cdots C_0 s_{n-1}$$

LFSR with Combinin fun^n

$f : \{0,1\}^k \to \{0,1\}$



Ex



$f : \{0,1\}^2 \to \{0,1\}$

$f(x_0, x_1) = x_0 . x_1$

$h[z>0] = 3/4$

Spiral

Date .....

x_0	x_1	f
0	0	0
0	1	0
1	0	0
1	1	1

It is not pseudo random bit generator.
It is biased f^n & not good.

→ Non-linear feedback shift Register (NFSR)

→ feedback f^n is non-linear.

$f : \{0,1\}^k \to \{0,1\}$

$t = f(x) + f(y) + f(x+y)$

$t = 0,1$	$f(x_0, x_1, x_2) = x_0 + x_1 x_2$

$t = 0$ if linear
$t = 1$, if affine
$t = 0, 1$ if non-linear.

→ HASH Function

$h : A \to B$

$h(x) = y$

1) If X is altered to X' then h(X') will be completely different from h(X).

Spiral