23/01/2024

CSPC63
CRYPTOGRAPHY

[Principles of cryptography]

Need : Many languages → hiding of information from other people → "cypting" → protect private information from third parties

↳ used by computers for communication between machines
↳ human to human communication

computer security → password protection + antivirus software + firewall.

3 basic objectives

① confidentiality ② integrity ③ availability

CIA

① confidentiality
- data confidentiality (group)
- privacy (person)

② integrity
- protection (change data only with administration approval)

③ availability
- DoS (denial of service)

Network security → next level with network administrators. Homogeneous systems, no client server environment.

web security → heterogeneous systems with client server environment.

SYLLABUS

Unit - 1 : Mathematical Foundations

Unit - 2 : classical cryptosystem
* types of attacks * stream ciphers * PRG

unit - 3 : symmetric key ciphers → 1 key

unit - 4 : Asymmetric key ciphers → 2 keys

unit - 5 : Message authentication, Digital signatures

23/01/2024

Textbooks :

① Stinson, D cryptography : Theory & Practice
② Ferrosana

challenges of computer security

* not simple → hacker is more intelligent than the algorithm designer
* potential attacks
* procedures → counter intuitive
* secrecy
* regular / continuous monitoring
* often an after-thought

OSI (open system interconnection)

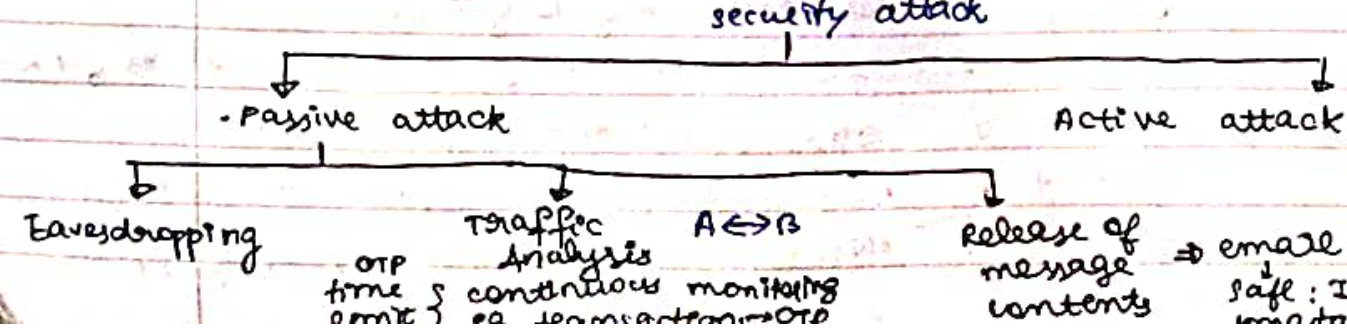
* security attacks
* security service
* security mechanisms

security attack

threat → potential for attack
attack → assault on SS

28/11 attack → satellite phones
after the attack, it was insisted to provide IDs while purchasing SIM cards

24/01/2024



23/01/2024

Textbooks :

① Stinson, D cryptography : Theory & Practice

② Ferrosana

challenges of computer security

* not simple → hacker is more intelligent than the algorithm designer
* potential attacks
* procedures → counter intuitive
* secrecy
* regular / continuous monitoring
* often an after-thought

OSI (open system Interconnection)

* security attacks
* security service
* security mechanisms

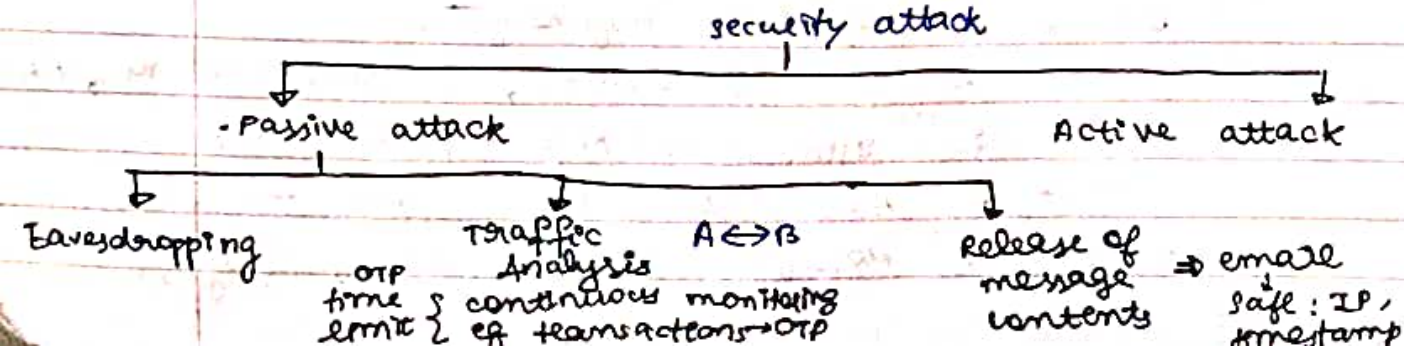
security Attack

threat → potential for attack

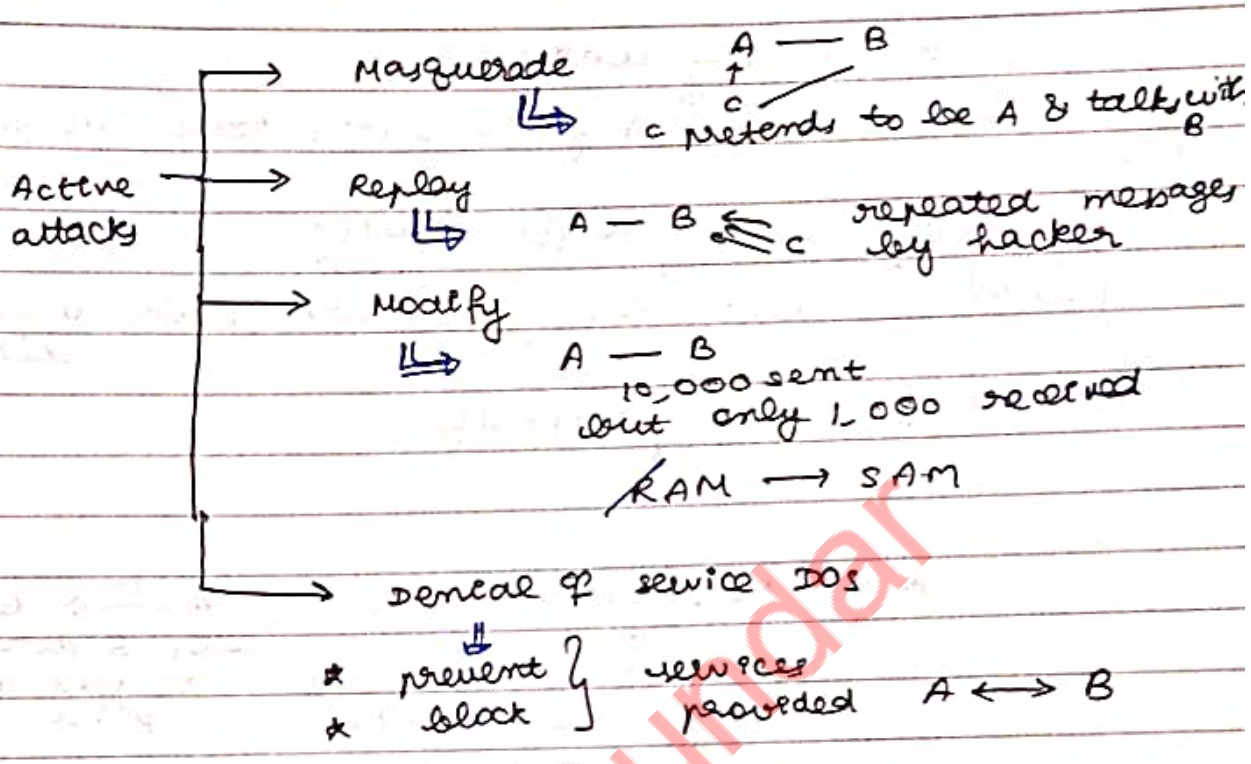
attack → assault on SS

26/11 attack → satellite phones after the attack, it was insisted to provide IDs while purchasing SIM cards

24/01/2024



24/01/2024



passive attacks : happen round the clock, can be detected only when any problem occurs ⇒ so difficult to detect (easy to prevent)

Active attacks : easy to detect, but difficult to prevent

Security services

↳ enhances — X.800 standard
— RFC 2828 standard

X.800 standard :

* Authentication : assurance that the communicating party is an authorized entity

∝ peer entity authentication
* data origin authentication

TCP/IP → T.L.

24/01/2024

* Access control
  ⇓
  preventing unauthorized access to a resource.
  (wrt resource)

* Data confidentiality
  ⇓
  protection of data from unauthorized disclosure
  (wrt data)

* Data integrity
  ⇓

* Non-repudiation
  ⇓
  protection of a party from denial of service ⇒ record must be maintained
  A → B
  Later B denies it was received at a later point of time
  [as signed in stamp paper]

* Availability
  ⇓
  resource availability
  [If not then DOS]

security mechanisms

specific SM pervasive SM

Specific security mechanisms :

* appropriate pervasive
* encipherment : done in application layer

A —encryption→ B —decryption→ read message

* digital signature

A —appends digital signature→ B

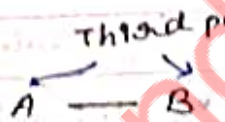
* data integrity
* authentication exchange

24/01/2024

* traffic padding
  ↓
  make all packets of same size → we cannot different rate between small and large packets.

* routing control
  >1 route, block other routes by choosing one route at the last minute

* notarization
  ||
  (non repudiation)



Mapping of security mechanisms with x.800 services

Encipherment → data confidentiality
→ data integrity
→ authentication

Digital signature → data integrity
→ non-repudiation
→ authentication

Authentication exchange → authentication
→ availability

Traffic padding → data confidentiality

Routing control → data confidentiality

notarization → non repudiation

29/01/2024

29/01/2024

Pervasive security Mechanisms

not specific →

① Trusted functionality
- ID → institute
- UID → Aadhar, passport, PAN

② security label
- eg KZ, Norton

③ Event detection
- checkpoints at different phases of event

④ security Audit Trial

⑤ security Recovery

Cryptographic Techneques

↓

cryptographic algorithms and protocols

- Symmetric → 1 key
- Assymmetric → 2 key
- Data integrity Algorithms
- Authentication protocols

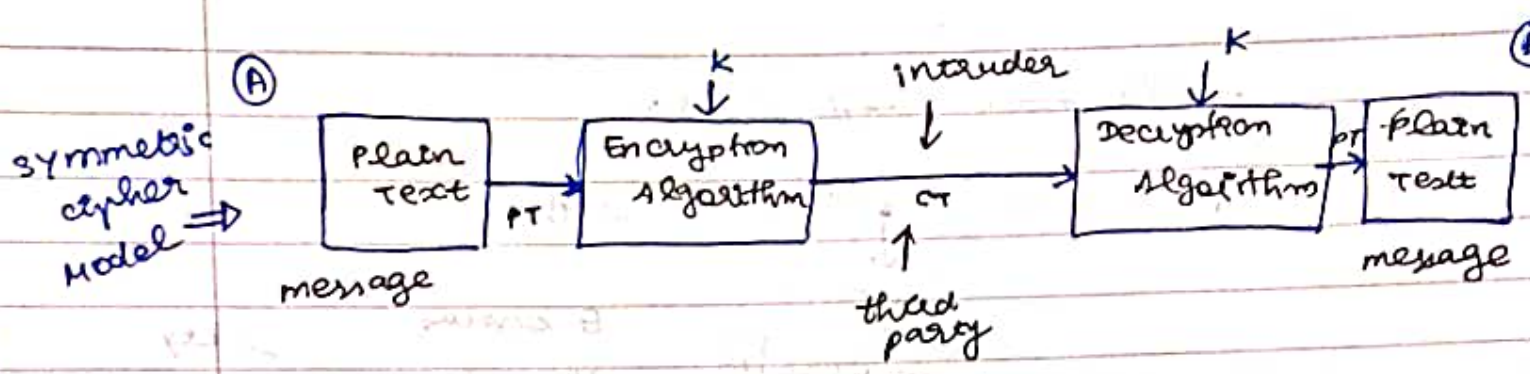
cryptology = cryptography + cryptoanalysis

- cryptography → art of deciphering ciphers
- cryptoanalysis → art of breaking ciphers

Symmetric:
- encrypt ↑ decrypt
- algo
  - public
  - key → secret

Assymmetric:
- 1 public key
- 1 private key → (secret key)

29/01/2024



symmetric cipher model ⇒

(CT: cipher text)

$CT = E_k(PT)$ $\quad D_k(E_k(x)) = E_k(D_k(x)) = x$

$PT = D_k(CT)$ [inverse functions]

m people → $^mC_2$ keys required for communication

$\left[{}^mC_2 = \frac{m(m-1)}{2}\right]$

Kerchoff's principle

* secrecy of the key: resistance of the cipher depends on key security
* guess → intruder → difficult
  - login, password → online bank; OTP sent only to registered mobile no. (time limit)
* key domain
  - must be large to ensure that it is difficult for the intruder to break it.

crypt-analysis

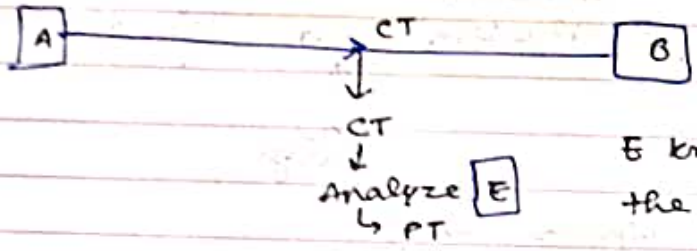
* breaking ciphers
* vulnerable

cryptanalysis attacks

- CT only attack
- KPA known plain text attack
- CPA chosen plain text attack
- CCA chosen cipher text attack

29/01/2024

Ciphertext only Attack



E knows the algorithm / key / plain text

① Brute-force Attack (or) Exhaustive key search attack
↳ trial and error of key used
try out all keys till you succeed.
↓
to prevent: keep the key domain large

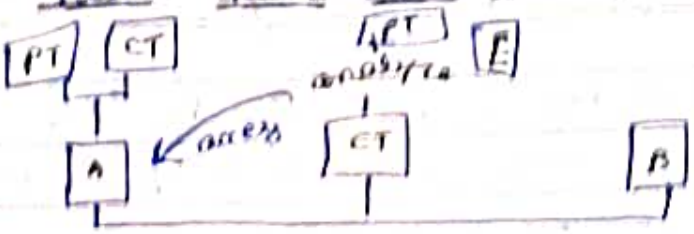
② Statistical Attack
↳ E: inherent characters of the language easily breakable
eg PT: ABBA → DEED
↳ randomization of the algorithm can help secure a lot.

③ Pattern Attack
PT → THE, AND (OR, AN) } easily identifiable patterns
CT → WICH

known plain Text Attack
↓
analyze previous transactions and key cracking
BABA → EDED
ABBA → DEED
analyze and help crack the whole algorithm

29/01/2024

Chosen Plain Text Attack



E hacks A's machine, observes (analyses) the communication with B.

chosen cipher text attack

influence decryption

30/01/2024

categories of Traditional ciphers

- substitution cipher
  - every symbol in the plain text is replaced by another symbol
  - Monoalphabetic substitution cipher
    - every occurrence gains same substitution
  - polyalphabetic substitution cipher
    - each occurrence ↓ different substitution
- Transposition cipher
  - rearranges the symbols present in the plain text.

Monoalphabetic cipher

↳ one to one relationship

eg : A → D

PT : ABBA CT : DEED

PT : BABA CT : EDED

29/01/2024

Additive cipher / shift cipher / caesar cipher

PT, CT and key → elements in Z_{26} (english alphabet)

Z_n → set with n elements from 0 to n-1

Encryption Algorithm → key

Decryption Algorithm → Inverse of the key

↓

if a is the key for encryption,

b is the key for decryption

Provided $a + b \equiv 0 \mod n$.

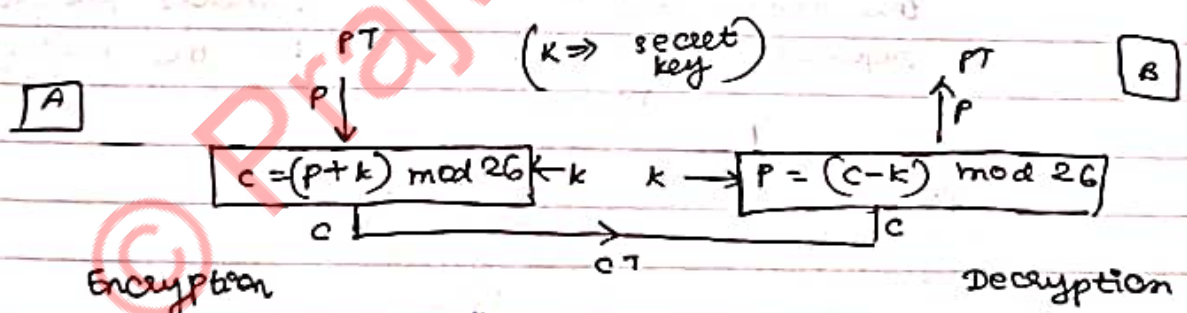
$Z_{10} = \{0, 1, \ldots, 9\}$

(a,b) pairs → {(1,9) (9,1)} {(2,8) (8,2)} ... (5,5) (0,0)

↳ total of 6 pairs

$Z_7 = \{0, 1, 2, \ldots, 6\}$ → ④ pairs

(0,0) (1,6) (6,1) (2,5) (5,2) (3,4) (4,3) → ④ pairs



Eg: PT = hello CT = ?

key = 15

Encryption:

h	e	l	l	o	+15 →	w	t	a	a	d
7	4	11	11	14		22	19	26	26	29
						≡ 22	≡ 19	≡ 0	≡ 0	≡ 3 → (mod 26)

CT = wtaad

h → (7+15) % 26 = 22 = w

e → (4+15) % 26 = 19 = t

} write full steps

29/01/2024

decryption:

w → (22-15) % 26 = 7 % 26 = 7 ⇒ h
t → (19-15) % 26 = 4 % 26 = 4 ⇒ e
a → (0-15) % 26 = -15 % 26 = 11 ⇒ l
d → (3-15) % 26 = -12 % 26 = 14 ⇒ o

cryptanalysis:

* Brute force attack: trial and error, all possible combinations
* statistical attacks:
  an, if → digrams
  the, and → trigrams

Multiplicative ciphers

$c = (p * k) \bmod 26$ during encryption

$c = (p * k)^{-1} \bmod 26$ during decryption

PT & CT → $\mathbb{Z}_{26}$ / Z_n
K key → Z_{26}^* / Z_n^*

if (a, b) are the key pair,
then $a * b \equiv 1 \bmod n$

Now, Z_n^* = subset of Z_n
↳ contains those elements in Z_n for which unique multiplicative inverse exists in Z_n.

$Z_6 = \{0, 1, 2, 3, 4, 5\}$
$Z_6^* = \{1, 5\}$
inverses = 1, 5
{(1,1) and (5,5)}
↳ 2 key pairs

29/01/2024

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$ → all no.s except 0

Aprime

↓

> shortcut to find elements in Z_n^*
> An element $x \in Z_n$, also belongs to Z_n^* if $GCD(n, x) = 1$

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$Z_{10}^* = \{1, 3, 7, 9\}$

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

$Z_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ → 12 elements

> For n even, $|Z_n^*| = n/2 - 1$

31/01/2024

key pairs

$Z_6^* = \{1, 5\}$ (1,1) (5,5)

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

(1,1) (2,4) (3,5) (6,6) ④ pairs

$Z_{10}^* = \{1, 3, 7, 9\}$

(1,1) (3,7) (9,9) ③ pairs

$Z_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

(1,1) (3,9) (5,21) (7,15) (11,19) (17,23) (25,25)

⑦ pairs

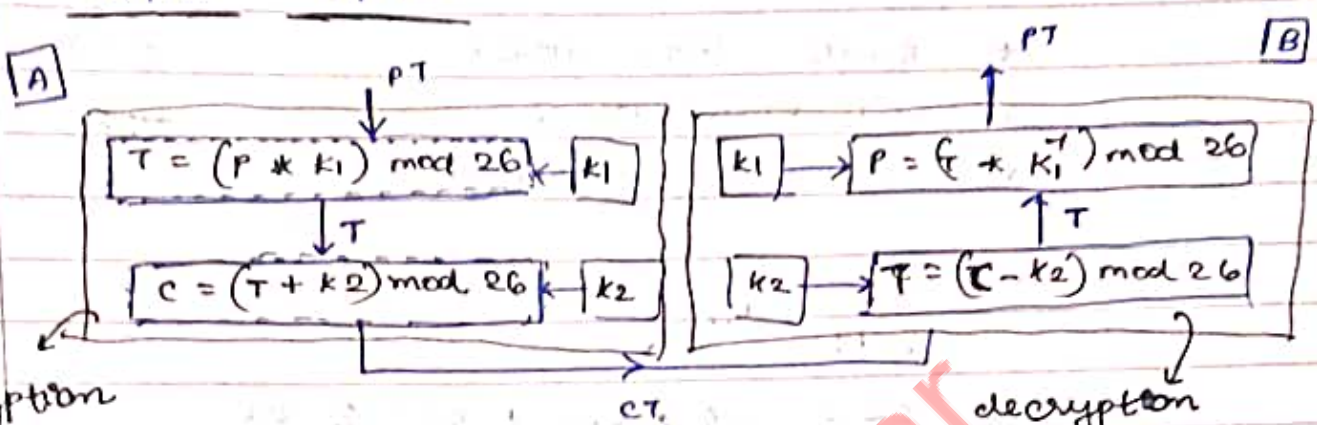
Cryptanalysis

* Brute force attack: trial & error basis
* statistical attack

Remedy: large key domain

31/01/2024

Affine cipher



combination of additive and multiplicative cipher

k_1 → 1st key → multiplicative

k_2 → 2nd key → additive

k_1, k_1^{-1} → MI while $k_2, -k_2$ ⇒ AI

$$C = ((P * k_1) + k_2) \bmod 26$$

$$P = ((C - k_2) * k_1^{-1}) \bmod 26$$

Q: use an affine cipher to encrypt a message hello using $(7, 2)$ (k_1, k_2)

a = 0
k = 10
u = 20

encryption

	h	e	l	l	o
P	7	4	11	11	14
P * k1	49	28	77	77	98
(P*k1) % 26	23	2	25	25	20
+ k2	25	4	27	27	22
% 26	25	4	1	1	22
	z	e	b	b	w

encrypted message → zebbw

decryption

	z	e	b	b	w
	25	4	1	1	22
-2	23	2	1	1	20
* k_1^{-1}	7	4	11	11	14
	h	e	l	l	o

$$(x - 2) * 7^{-1} \bmod 26$$

$$= (x - 2) * 15 \bmod 26$$

[from key pair table generated]

∴ Encryption & Decryption done successfully

31/01/2024

cryptanalysis :
* Brute force attack
* CT only attack
* chosen PT attack

solve :
ct $\xrightarrow{alg1}$ wc
ct $\xrightarrow{alg2}$ wf
find key (affine cipher)

$(4, 19) \xrightarrow{k1, k2} (22, 2)$

subtracting eqns

$22 = ((4 * k1) + k2) \% 26$
$2 = ((19 * k1) + k2) \% 26$

eqn is correct

$-20 = (15 * k1) \% 26 = 6$

$k1 = 16$
$k2 = 10$

✗ but no even no

$(4, 19) \xrightarrow{k1, k2} (22, 5)$

subtracting eqns

$22 = ((4 * k1) + k2) \% 26$
$5 = ((19 * k1) + k2) \% 26$

$-17 = (15 * k1) \% 26 = 9$

$k1 = 11$
$k2 = 4$

✓ correct

05/02/2024

$k1 = 16$ is wrong as $k1 \in \mathbb{Z}_{26}^*$ as it must have an inverse, but it doesn't exist. so $(16, 10)$ is an invalid answer.

using trial and error method, $k1 = 11$ and $k2 = 4$ are obtained. ALG2 is correct.

$PT \xrightarrow[k1=11]{M.C} \cdots \xrightarrow[k2=4]{A.C} CT \xrightarrow[k2^{-1}=22]{(A.C)^{-1}} \cdots \xrightarrow[k1^{-1}=19]{(M.C)^{-1}} PT$

encryption | decryption

Monoalphabetic substitution ciphers:

Addition cipher, Multiplicative cipher, Affine cipher

These have very small key domain

Remedy: a to z ; 0 to 25

↳ random mapping

	0	1	2	.....	25
	A	B	C	.....	Z
(1)	Z	A	B	.....	Y
(2)	Y	Z	A	.....	X
(3)	X	Y	Z	.....	

(26 possible mapping)

Polyalphabetic ciphers

* one to many ⇒ * hides letter frequency of the underlying language
* same PT character ✗→ same CT character

* Each character in the CT depends on:
  - → corresponding PT character
  - → position of the PT character
* key stream is used.
  $K = (K_1, K_2, \ldots)$
  K_i is used to cipher P_i to C_i

Autokey cipher

* key → representation of subkeys
  $k = (k_1, k_2, \ldots, k_n)$
* 1st subkey k_1 → sends, receives
* 2nd subkey → 1st PT character
* 3rd subkey → 2nd PT character

⋮

05/02/2024

$P = P_1\ P_2\ P_3 \ldots$

$C = C_1\ C_2\ C_3 \ldots$

$K = K_1\ P_1\ P_2 \ldots$

Encryption: $C_i = (P_i + K_i) \% 26$

Decryption: $P_i = (C_i - K_i) \% 26$

Eg: Perform encryption of attack using a polyalphabetic substitution with $K_1 = 12$.

attack

PT	a	t	t	a	c	k
PT	0	19	19	0	2	10
K	12	0	19	19	0	2
CT	12	19	38	19	2	12
With %26	12	19	12	19	2	12
CT	m	t	m	t	c	m

attack ≡ mtmtcm

crypto:

c	r	y	p	t	o	
2	17	24	15	19	14	
12	2	19	24	15	17	
14	19	41	39	32	31	
14	19	15	13	6	5	
o	t	p	n	g	f	

crypto ≡ otpngf

Cryptanalysis:

* hides the inherent characteristics of the P.T.
* Brute force attack: $K_1 \rightarrow 0$ to 25

One Time Pad (OTP)

* secrecy of the key ✓
* randomize (random)

PT	C	R	Y	P	T	O	G	R	A	P	H	Y
key	K	I	N	D	E	R	G	A	R	T	E	N
PT	2	17	24	15	19	14	6	17	0	15	7	24
Key	10	8	13	3	4	17	6	0	17	19	4	13
CT%26	12	25	11	18	23	5	12	17	17	8	11	11
CT	M	Z	L	S	X	F	M	R	R	I	L	L

05/02/2024

PT	C	R	Y	P	T	O	G	R	A	P	H	Y	
key	I	A	M	I	N	S	I	X	T	H	S	E	
PT	2	17	24	15	19	14	6	17	0	15	7	24	
key	8	0	12	8	13	18	8	23	19	7	18	4	
CT	10	17	10	23	6	6	14	14	19	22	25	2	
CT	K	R	K	X	G	G	O	O	T	W	Z	B	

Advantages :

* randomization : can't be broken
* CIA : confidentiality, integrity, authentication

Limitations :

* very random
* key length must be equal to the PT length
* key must be shared in advance.

08/02/2024

Play-Fair cipher → (WWI)

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

Rules :

① Plain text is scanned on a pair by pair

R1 ② If two letters in a pair are the same, a bogus letter is inserted to separate them.

R2 ③ the no. of characters is odd → then a bogus letter is inserted to make it even.

R3 ④ If two letter in a pair are located in the same row of the secret key, the letter to the right is the encrypted key.

05/02/2024

PT	C	R	Y	P	T	O	G	R	A	P	H	Y		
key	I	A	M	I	N	S	I	X	T	H	S	E		
PT	2	17	24	15	19	14	6	17	0	15	7	24		
key	8	0	12	8	13	18	8	23	19	7	18	4		
CT	10	17	10	23	6	6	14	14	19	22	25	2		
CT	K	R	K	X	G	G	O	O	T	W	Z	B		

Advantages :

* randomization : can't be broken
* CIA : confidentiality, integrity, authentication

Limitations :

* very random
* key length must be equal to the PT length
* key must be shared in advance.

06/02/2024

Play - Fair cipher → (WWI)

secret key

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

Rules :

① Plain text is scanned on a pair by pair

R1 ② If two letters in a pair are the same, a bogus letter is inserted to separate them.

R2 ③ the no. of characters is odd → then a bogus letter is inserted to make it even.

R3 ④ If two letter in a pair are located in the same row of the secret key, the letter to the right is the encrypted key.

06/02/2024

⑤ R4 Two letters in a pair are located in the same column of the secret key → the letter beneath "it" the same column is the encrypted key.

⑥ R5 If two letters in a pair are not located in the same row / column of a secret key, the letter in its own row, but in the same column as the other letter is the encrypted key.

PT : h e l l o he → key: ec
R1 : he lx lo lx → key: qz
lo → key: bx

cipher text: ecqzbx

Decryption: reverse the given rules.
ec qz bx → he lx lo

cryptanalysis:
Brute force → 125 Highly difficult to crack

vigenese cipher
key stream → 'm' characters → block of m characters → m < l, l → length of PT

eg PT : s h e i s l i s t e n i n g
key: pascal key : p a s c a l p a s c a l p a

PT : 18 7 4 8 18 11 8 18 19 4 13 8 14 6
key : 15 0 18 2 0 11 15 0 18 2 0 11 15 0

CT : 7 7 22 10 18 22 24 18 11 6 13 19 2 6
CT : h h w k s w y s l g n t d g

HHWKSWYSLGNTDG → (cipher text)

06/02/2024

Method : * key does not depend on the plain text
* key is decided without knowing what the plain text is
* m additive ciphers

S	H	E	I	S	L	H	E	W	A	S	I	N	G
P	A	S	C	A	L	P	A	S	C	A	L	P	A

cryptanalysis : key depends on position : if a character appears in the same position in every block (kasiski test)

02/02/2024 [:scholar]

Classical Encryption Techniques
→ substitution techniques
→ transposition techniques — rail fence
row column

Rail Fence
↓
Eg : WE ARE THIRD YEAR STUDENTS
Encode with depth = 2

W		A		E		H		R		Y		A		S		U		E		T		S
	E		R		T		I		D		E		R		T		D		N		

and write row-wise
WAEHRYASUETERTIDERTDNS → (cipher text)

Encode with depth = 3

W		R		H		D		A		T		E		S
	E		E		I		Y		R		U		N	
A		T		R		E		E		D		T		

WRHDATES
EEIYRUN
ATREEDT

Row-column
create a rectangle, write row by row and read column by column, key → decides order to follow while reading

07/02/2024

eg key = 4 3 2 1 6 7 5

4	3	2	1	6	7	5
N	E	A	R	E	T	H
I	R	D	Y	E	A	R
S	T	U	D	E	N	T
S	X	X	X	X	X	X

⇒

RYDX ADUX
ERTX WISS
HRTX EEEX
TANX

more complexity → Again fill CT in rectangle & read col by col

IAMNITTSTUDENT $\xrightarrow{3/42}$ ATUTNSEXIITNMTDX

$\xrightarrow{3/42}$ TSITTXNXANIMETID [2 passes]

12/02/2024

Symmetric cipher

- Stream cipher
  - Mono
    - additive
    - multiplicative
    - affine
    - vignese
  - Poly
- Block cipher
  - process m > 1 characters at once.
  - Play-fair cipher m = 2. [pair by pair scanning]

Polyalphabetic ciphers :

- ECB (Electronic code Block)
- CBC (cipher Block chaining)
- CFB (cipher Feed Back)
- OFB (output feed Back)
- CTR (counter based)

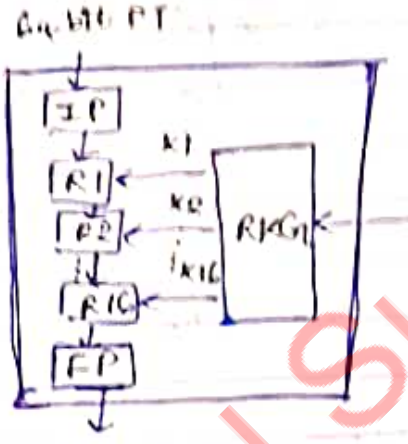
DES → Data Encryption Standard.

↓

64 bit plain text, 56 bit key, 64 bit cipher te

DES Structure

* Encryption : 2 permutations (P-boxes) : initial & final permutations + 16 Feistel rounds
* PT & CT : 64 bits
cipher key : 56 bits (round key : 48 bits)



(RKGn : round key generation)

IP : initial permutation

FP : final permutation

both are keyless transpositions

K1, K2 .... → round keys

Eg : Find output of initial permutation box when input is $(0000\ 0080\ 0000\ 0002)_{16}$

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 IP 0 0 0 0 0 0 0 0
1 0 0 0 0 0 0 0 → 0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0

ox | 0000 0000 0800 0080

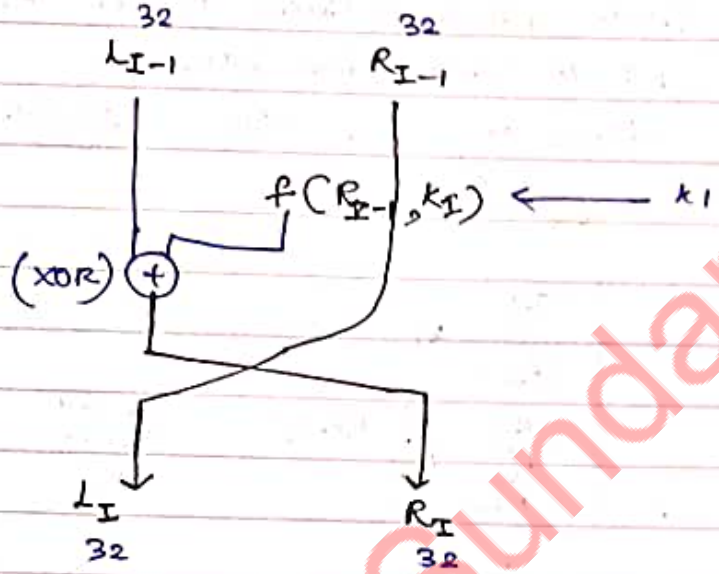
[hexadecimal] [bits presented]

12/02/2024

Rounds

DES uses 16 rounds → each round is a feistel cipher

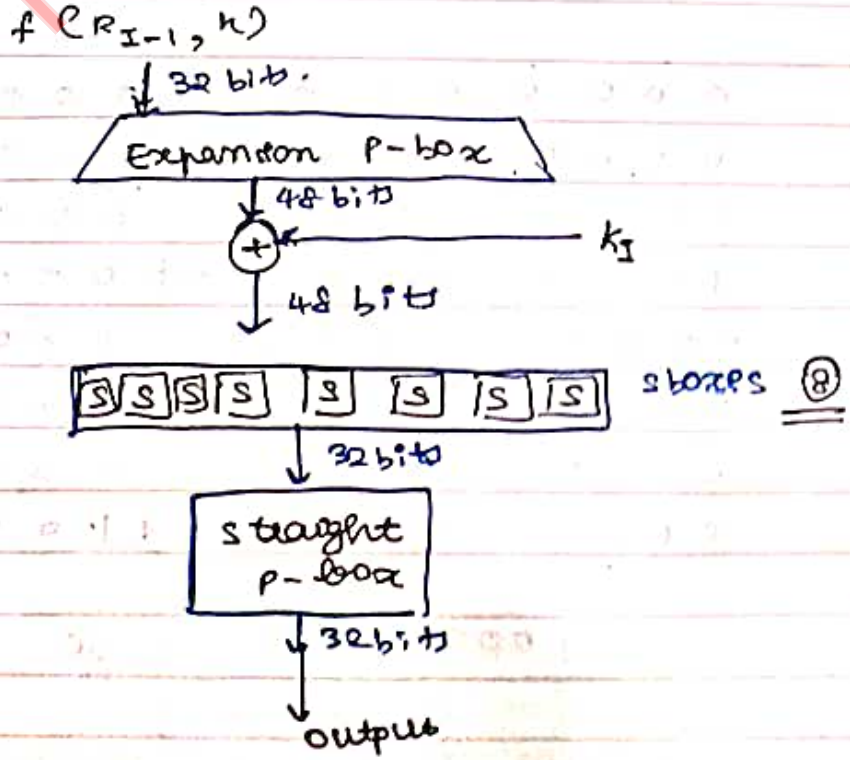
operation performed in one feistel round :



DES function f

↳ heart of DES.

48 bit key to rightmost 32 bits to produce 32 bit output.



12/02/2024

Expansion p-box

32 bits = 8 * 4
48 bits = 8 * 6
} convert each 4 bits to 6 bits

1 & 34
0 1 2 3 4 5
0: last bit of previous nibble
5: first bit of next nibble

DES uses a table to define this p-box

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

[ins-DES]
1 2 3 4
↓
[4 1 2 3
2 3 4 1]

Whitener (XOR)
↳ XOR on expanded right section and the round key. Both right and key are now 48 bits in length.

S-Box

Bit 1 2 3 4 5 6
row: bits 1 & 6
col: bits 2 3 4 5

r = 2 bits → row (4 rows)
c = 4 bits → column (16 columns)
take the position value at (r, c)
↳ 4 bit output as defined in the table

12/02/2024

Eg: 100011 is the input given to S-box (1) find the output

0001 row = 11 = 3
col = 0001 = 1

row 3 col 1 → table value = (12) → 1100

(8) Different S-boxes are used each time.

13/02/2024

cipher and Reverse cipher:
mixers & swappers → ciphers & reverse ✓

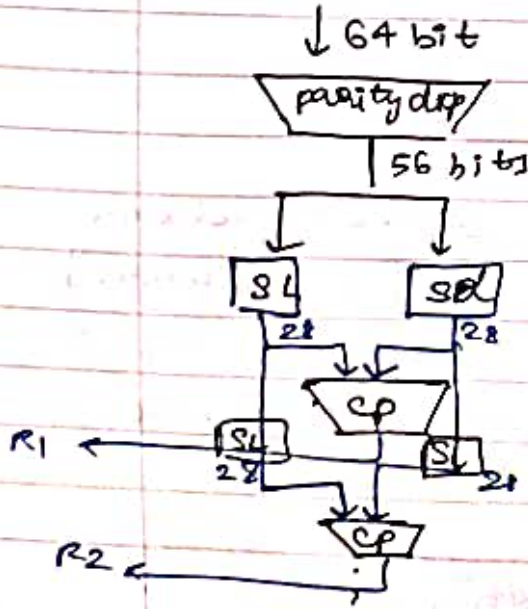
Key generation
use 58 bit key to generate 16 48 bit keys

parity → odd · 00011100 ← P
even 00011101 ← P

0 parity
1 parity

56 bits = 8 (no. of grps) * 7 (size of a group)

Attaching one parity bit to each group:
8 * (7+1) = 8 * 8 = 64 bits



CP → compression P-boxes

shifting

Rounds	shift
1, 2, 9, 16	one bit
others	two bits

* parity drop table
* key compression table

10/02/2024

DES Analysis :
* avalanche effect } desired characteristics of
* completeness } Block cipher

Avalanche Effect : A small change in the PT or key (a single bit) should create a significant change in the CT.

completeness Effect : Each bit of the ciphertext needs to depend on many bits of the plain text.

SECURITY OF DES [CRYPTANALYSIS] :
* Brute-Force Attack
* Differential cryptanalysis
* Linear cryptanalysis

Brute-Force Attack :
↳ key domain → 2^{56}.
Half of the keys are complement of each other. $2^{56}/2 = 2^{55}$
time of brute force attack
[approx 22 h 15 mins]

DES weaknesses
weaknesses in cipher design are found in S-boxes, P-boxes and key.

weak keys :
4 out of 2^{56} are called weak keys.
Round keys generated → all same.
Round keys are same as the cipher text.
2 encryptions ≡ plain text.

13/02/2024

semi-weak keys :

* 6 key pairs are called semi weak keys.
* k_1 in set 1 = k_{16} in set 2 .... so on
* $E_{k_2}(E_{k_1}(P)) = P$ [keys are inverses of each other]

Possible-weak keys

* 48 keys are possible weak keys.
* Each key generates 4 distinct round keys.
* Out of 16, 4 + 4 + 4 + 4 keys are generated.

Q: Find probability of selecting a weak, semi-weak or possible-weak key.

domain = 2^{56}.

weak = 4, semi weak = 12, possible weak = 48

$4 + 12 + 48 = 16 + 48 = 64 = 2^6$

$P = \frac{2^6}{2^{56}} \Rightarrow P = 2^{-50}$ ↳ very less

Multiple DES

① Double DES → double DES improves vulnerability to the Meet-in-the-Middle Attack
② Triple DES

2keys / 3 keys

Security of DES

① Brute Force Attack
② Differential cryptanalysis
③ Linear cryptanalysis

DES and AES → study from PPTs

19/02/2024

19/02/2024

MATHEMATICS OF CRYPTOGRAPHY

tn, $t\overset{*}{n}$

Divisibility : $a = q * n$ $\quad a \div n$ where $r = 0$

n divides a (or) a is divisible by n $\quad n/a$

eg 4 divides 32 → 4 / 32

8 doesn't divide 42 → 8 ✱ 42

13 / 78 $\quad$ −6 / 24 $\quad$ 11 ✱ −32

7 ✱ 50 $\quad$ 4 ✱ 41 $\quad$ 7 / 98

Properties of Divisibility :

(P1) If $a|1$, then $a = \pm 1$ ✓

(P2) If $a|b$ and $b|a$, then $a = \pm b$

eg 3|3 and 3|3, then $3 = \pm 3$ ✓

(P3) If $a|b$ and $b|c$, then $a|c$.

eg 3|15 and 15|45, then 3|45 ✓

(P4) If $a|b$ and $a|c$, then $a|(m*b + n*c)$

eg 3|15 and 3|9, then $3|(1*15)+(2*9)$ ✓

Euclidean Algorithm :

GCD → large

2 facts :

Fact 1 : GCD(a, 0) = a.

Fact 2 : GCD(a, b) = GCD(b, r)

Where r is the remainder when a is divided by b. $r = a \% b$.

19/02/2024

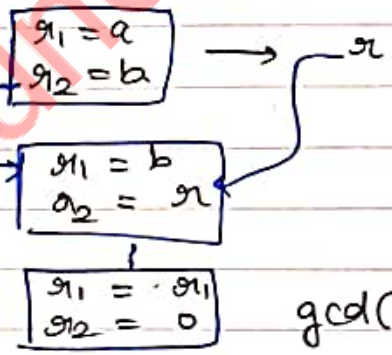
GCD (30, 10) = GCD(10, 6) = GCD(6, 4) =
GCD(4, 2) = GCD(2, 0) = (2)

GCD (161, 28) = GCD(28, 21) = GCD(21, 7)
= GCD(7, 0) = (7)

GCD(25, 60) = GCD(60, 25) = GCD(25, 10)
= GCD(10, 5) = GCD(5, 0) = (5)

(EA) $r_1 \leftarrow a$ $r_2 \leftarrow b$

while($r_2 > 0$) { $q \leftarrow r_1 / r_2$
$r \leftarrow r_1 - q * r_2$
$r_1 \leftarrow r_2$; $r_2 \leftarrow r$ }
GCD(a, b) $\leftarrow r_1$

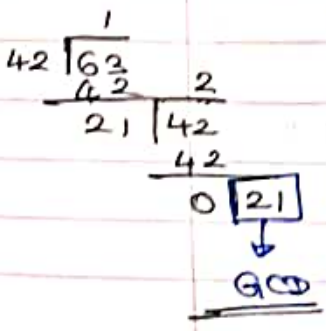


FLOW CHART :

GCD (2740, 1760) = GCD(1760, 980)
= GCD(980, 780) = GCD(780, 200)
= GCD(200, 180) = GCD(180, 20)
= GCD(20, 0) = (20)

GCD (306, 657) = GCD (657, 306)
= GCD (306, 45) = GCD (45, 36)
= GCD (36, 9) = GCD (9, 0) = (9)

Tabular Representation. eg GCD (42, 63)



q	r_1	r_2	r
0	42	63	42
1	63	42	21
2	42	21	0
	21	0	

result

GCD = (21)

20/02/2024

20/02/2024

EXTENDED EUCLIDEAN ALGORITHM (EEA)

☆ GCD (a, b)
☆ s and t, such that $s*a + t*b = GCD(a,b)$

} Both these can be calculated

{ $r_1 \leftarrow a$ $s_1 \leftarrow 1$ $t_1 \leftarrow 0$
$r_2 \leftarrow b$ $s_2 \leftarrow 0$ $t_2 \leftarrow 1$ } (initialization)

while ($r_2 > 0$)

(procedure) {
$q \leftarrow r_1 / r_2$ $s \leftarrow s_1 - q * s_2$ $t \leftarrow t_1 - q * t_2$
$r \leftarrow r_1 - q * r_2$ $s_1 \leftarrow s_2$ $t_1 \leftarrow t_2$
$r_1 \leftarrow r_2$ $s_2 \leftarrow s$ $t_2 \leftarrow t$
$r_2 \leftarrow r$ }

$GCD(a,b) \leftarrow r_1$ $s \leftarrow s_1$ $t \leftarrow t_1$

Q: a = 161, b = 28, find GCD(a,b) and (s, t) using the extended euclidean algorithm.

$r_1 \leftarrow 161$ $s_1 \leftarrow 1$ $t_1 \leftarrow 0$
$r_2 \leftarrow 28$ $s_2 \leftarrow 0$ $t_2 \leftarrow 1$

$r_2 > 0$ ✓

$q \leftarrow 161/28 = 5$ $s \leftarrow 1$ $t \leftarrow -5$
$r \leftarrow 21$ $s_1 \leftarrow 0$ $t_1 \leftarrow 1$
$r_1 \leftarrow 28$ $s_2 \leftarrow 1$ $t_2 \leftarrow -5$
$r_2 \leftarrow 21$

$r_2 > 0$ ✓

$q \leftarrow 28/21 = 1$ $s \leftarrow -1$ $t \leftarrow -4$
$r \leftarrow 7$ $s_1 \leftarrow 1$ $t_1 \leftarrow -5$
$r_1 \leftarrow 21$ $s_2 \leftarrow -1$ $t_2 \leftarrow -4$
$r_2 \leftarrow 7$

$r_2 > 0$ ✓

$q \leftarrow 21/7 = 3$ $s \leftarrow 4$ $t \leftarrow -23$
$r \leftarrow 0$ $s_1 \leftarrow -1$ $t_1 \leftarrow -4$
$GCD \leftarrow r_1 \leftarrow 7$ $s_2 \leftarrow 4$ $t_2 \leftarrow -23$
$r_2 \leftarrow 0$

GCD = 7, $4 * 161 + -23 * 28 = 7$ ✓

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	[7]	0		[-1]	4		[6]	-23	
	GCD			s			t		

GCD (161, 28) = 7

(-1 * 161) + (6 * 28) = 7 ✓

Q: Apply EEA on (272, 1479)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	272	1479	272	1	0	1	0	1	0
5	1479	272	119	0	1	-5	1	0	1
2	272	119	34	1	-5	11	0	1	-2
3	119	34	17	-5	11	-38	1	-2	7
2	34	17	0	11	-38	87	-2	7	-16
	[17]	0		[-38]	87		[7]	-16	
	GCD			s			t		

Q: Apply EEA on (143, 227)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	143	227	143	1	0	1	0	1	0
1	227	143	84	0	1	-1	1	0	1
1	143	84	59	(-1	2	0	1	-1	
1	84	59	25	-1	2	-3	1	-1	2
2	59	25	9	2	-3	8	-1	2	-5
2	25	9	7	-3	8	-19	2	-5	12
1	9	7	2	8	-19	27	-5	12	-17
3	7	2	1	-19	27	-100	12	-17	63
2	2	1	0	27	-100	227	-17	63	57
	[1]	0		[-19]	227		[63]	57	

20/02/2024

EEA on (17, 0) EEA on

Multiplicative Inverse calculation

MI of b in Z_n → Z_n^* $r_1 \leftarrow a$ $r_2 \leftarrow b$

MI of b → t_1 $t_1 \leftarrow 0$ $t_2 \leftarrow 1$

while ($r_2 > 0$)

{ $q \leftarrow r_1 / r_2$ $t \leftarrow t_1 - q * t_2$

$r \leftarrow r_1 - q * r_2$ $t_1 \leftarrow t_2$

$r_1 \leftarrow r_2$ $t_2 \leftarrow t$

$r_2 \leftarrow r$

}

[if $r_1 = 1$ then $b^{-1} = t_1$] finally after loop.

Q: calculate MI of 11 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

b^{-1}

[(11, 19) is a key pair]

$b^{-1} = -7 \equiv -7 \% 26 \equiv \boxed{19}$ → MI of 11 in Z_{26}

Q: calculate MI of 12 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	-2
6	12	2	0	1	-2	13
	(2)	0		-2	13	

$\neq 01$

MI does not exist for 12 in Z_{26}

21/02/2024

21/02/2024

MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY

ALGEBRIC STRUCTURES

cryptography → set of integers $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}_n^*, \mathbb{Z}_p, \mathbb{Z}_p^*$
→ + operations applied
→ Algebric structures
[Groups, Fields, Rings]

Group (G)

set of statements with binary operation '.' that satisfy the following 4 axioms:

1) closure
If a and b are elements of G
$c = a \cdot b$ is also an element of G

2) Associativity
If a, b, c are elements of G, then
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3) Identity
$\forall a \in G$, $\exists$ an element e such that
$e \cdot a = a \cdot e = a$

4) Existence of an Inverse
$\forall a \in G$, $\exists$ an element a' called the inverse of a, such that
$a \cdot a' = a' \cdot a = e$

ONE MORE PROPERTY:

5) commutativity
$\forall a, b \in G$, $a \cdot b = b \cdot a$

In additional to ① – ④, if ⑤ is also satisfied the group is refered to as a commutative group or Abelian Group.

21/02/2024

Q: Find out whether $G = \langle Z_n, + \rangle$ is a commutative group. (take %n by default)

$Z_n = \{0, 1, \ldots, n-1\}$

1) closure ✓ 2) associativity ✓

3) identity ✓ → 0

4) inverse ✓ → (0,0) else $(x, n-x)$ ✓

5) commutativity ✓

commutative group **YES** ✓

Q: Find out whether $G = \langle Z_n^*, + \rangle$ is an Abelian group.

YES ✓

Q:

•	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

From the given table, check if $S = \{a, b, c, d\}$ is an Abelian Group or not.

1) closure ✓ 2) associativity ✓ **YES**

3) identity → (a) ✓ 4) inverse (a,a) (b,d) (c,c) ✓

5) commutativity → symmetric matrix ✓

Finite Group

A group is called a finite group if it has finite no. of elements, otherwise it is called an infinite group

order of a group

$|G|$ = no. of elements present in the group

21/02/2024

Subgroup

A subset H of a group G is a subgroup of G if : 1) H is a group wrt operations on G

If $G = \langle S, \cdot \rangle$ is a group
then $H = \langle T, \cdot \rangle$ is a group under the same operations
AND

2) T is a non-empty subset of S.

Q: Is the group $H = \langle Z_{10}, + \rangle$ a subgroup of $G = \langle Z_{12}, + \rangle$?

↳ NO As n differs, operations differ
[one is $+\%10$, other is $+\%12$]
Inverse differs for the same element between Z_{10} and Z_{12}.

cyclic subgroup

If a subgroup of a group can be generated using the power of an element, then the subgroup is called a cyclic subgroup.

[Power → repeatedly applying the group operation]

$a^n = a.a.a \ldots a$ $a^2 = a.a$ $a^3 = a.a.a$

↳ $\langle a \rangle$

Duplicate elements are removed (discarded)

$a^0 = e$

Q: Find the subgroups of $\langle Z_{12}, + \rangle$.

order of $Z_{12} = |Z_{12}| = 12$

↳ devisors of 12 = 1, 2, 3, 4, 6, 12

↳ no. of subgroups = no. of devisors

$H_1 = \langle 0 \rangle = \{0\}$ (1)

$H_2 = \langle 1 \rangle = \{0, 1, \ldots, 11\}$ (12)

21/02/2024

$H_3 = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ ⑥

$H_4 = \langle 3 \rangle = \{0, 3, 6, 9\}$ ④

$H_5 = \langle 4 \rangle = \{0, 4, 8\}$ ③ [sizes]

$H_6 = \langle 6 \rangle = \{0, 6\}$ ②

$H_7 = \langle 12 \rangle = \{0\}$ ← same as $\langle 0 \rangle$

$\{ \langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle \}$ are the set of cyclic subgroups

26/02/2024

Q: Find out the cyclic subgroups of $\langle Z_6, + \rangle$

$H_1 = \langle 0 \rangle = \{0\}$

$H_2 = \langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$

$H_3 = \langle 2 \rangle = \{0, 2, 4\}$

↳ all possible cyclic subgroups

$H_4 = \langle 3 \rangle = \{0, 3\}$

0: $0^0 \bmod 6 = 0$

1: $1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = 2$
$1^3 \bmod 6 = 3$
$1^4 \bmod 6 = 4$
$1^4 \bmod 6 = 5$

2: $2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = 4$

3: $3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

4: $4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = 2$
same as $\langle 2 \rangle$

5: same as $\langle 1 \rangle$

6: same as $\langle 0 \rangle$

n^k means n & k not power

∴ Found the cyclic subgroups are

$\{ \langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle \}$

1 6 3 2 [sizes]

26/02/2024

Q: Find cyclic subgroups of $\langle Z_{12}, + \rangle$

$Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$

$\langle 3 \rangle = \{0, 3, 6, 9\}$.

$\langle 4 \rangle = \{0, 4, 8\}$

$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \langle 1 \rangle$

$\langle 6 \rangle = \{0, 6\}$.

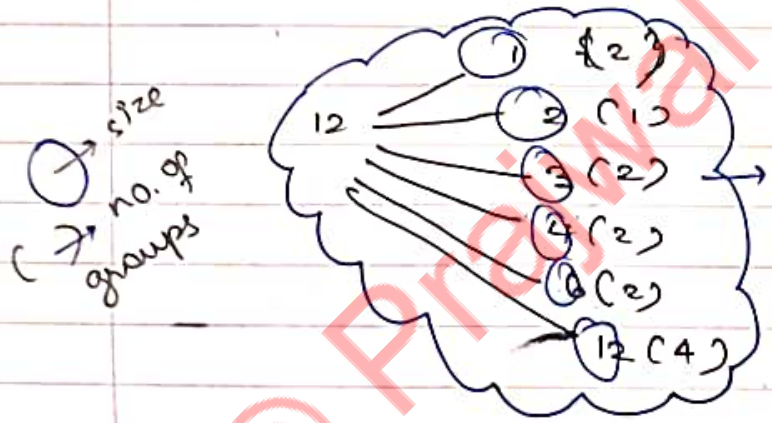
$\langle 7 \rangle = \{0, 7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5\} = \langle 1 \rangle$

$\langle 8 \rangle = \{0, 8, 4\} = \langle 4 \rangle$

$\langle 9 \rangle = \{0, 9, 6, 3\} = \langle 3 \rangle$

$\langle 10 \rangle = \{0, 10, 8, 6, 4, 2\} = \langle 2 \rangle$

$\langle 11 \rangle = \{0, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1\} = \langle 1 \rangle$



!! size → always a divisor !!

Q: Find the subgroups of $\langle Z_{10}^{*}, * \rangle$

$Z_{10}^{*} = \{1, 3, 7, 9\}$ $\quad |Z_{10}^{*}| = 4 \begin{matrix} = 1 \\ = 2 \\ = 4 \end{matrix}$

H_1:

$\langle 1 \rangle = \{1\} \rightarrow$ ①

$\langle 3 \rangle = \{1, 3, 9, 7\} \rightarrow$ ④ (are the sizes)

$\langle 7 \rangle = \{1, 7, 9, 3\} \rightarrow$ ④

$\langle 9 \rangle = \{1, 9\} \rightarrow$ ②

* Here n^k means multiplication *