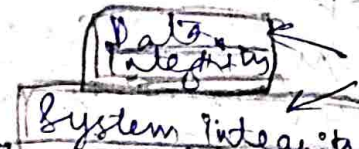
06/01/2025 CRYPTOGRAPHY

- CIA: Confidentiality, Integrity, Availability, ~~Authentication~~
Threat: might happen; attack: happened

cryptography: theory & practice — ?
(a... and n/w security: Fourouzan

07/01/2025 computer security; N/W sc; Internet sc, Web sc
browser security, web servers, web users

Objectives of Security: CIA


(Admin in n/w can only change)

C → Data confidentiality
↳ Privacy

DoS

challenges to computer security:
* Not simple * ~~Potential~~ Potential attacks
- continuously monitor * secrecy after thought

OSI → security attacks
→ security services
→ security mechanisms

threat: violation of security, attack: assault on system security

Attacks → Passive (difficult to find (it happened) / easy to prevent) (eavesdropping, Release of msg contents, Traffic analysis)
→ Active (easy to find (it happened) / difficult to prevent)

* Masquerade (Intruder pretends to be someone) * Replay * Modify * DoS

security services: to counter security attacks
Standards: X-800, RFC 2828

X-800 security services:
* authentication * access control * Data confidentiality
* Data integrity * Non-repudiation (↔ can't deny responsibility) * availability

08/01/2025 security mechanisms: of ~~eth~~ one dig

X-800: → specific SM
→ pervasive SM

Specific SM: 1. encipherment, 2. digital signature, 3. access control, 4. data integrity, 5. authentication exchange, 6. traffic padding (to make uniform size & it reach min length) 7. allow to

routing control (selecting the safest route)
& notarization A — B (some other Traffic etc. Third party)

Mapping security services to mechanisms

M1. Encipherment : confidentiality, auth, integrity
M2. Dig sign : Non Repudiation, Auth, Integrity
M3. {Access Control} : auth
M4. {Integrity} ; non repudiation
M5. Auth exchange : auth, availability
M6. Traffic padding : confidentiality : can find if packet is ACK or data.
↳ traffic flow control
M7. Routing control : confidentiality (which route is known)
M8. Notarization : Non-repudiation

Pervasive : support/enhance
1. Trusted functionality
2. Security label
3. Event detective
4. Security audit trial
5. Security Recovery

Cryptography Techniques
Symmetric Asymmetric Data Integrity, Authentication

Cryptography + Cryptanalysis = Cryptology
devising cipher breaking cipher

Symmetric : 1 key, private key
Asymmetric : 2 keys → 1 : private key
2 : public key

13/01/2025

5 tuple : (P, C, K, E, D)

Techniques : Substitution, transposition.

Caesar cipher → monoalphabetic cip → HW
Substitution → polyalphabetic → playfair cipher

Monoalph : for a given alphabet cipher same is text for all instances.
In playfair, for a given pair

Caesar: Enc: $C = (P+3) \% 26$, $P = (C-3) \% 26$

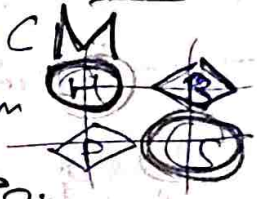
Vinalph?:

Playfair: 5×5 matrix, take a key eg. MONARCHY
↳ 25 cells, use same cell for I/J
fill unused cells in order for unused alphabets
for repeated alphabets in key write only once

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

Rule-1: If same alphabets come together put filler (x)
balloon → ba lx lx on divide as 2 in each

To encrypt: eg. AR, both in same row? Rule 2 take circular right char of each ⇒ AR → RM
Same column: bottom (down) circular MU → CM
Else: make rectangle. eg. HS → BP from



for each write the ◇ in its row?

Eg. plain text = INSTRUMENTS ← to make even?
IN: NA
GI
GATLMZ CLRQ TX

* If there is I/J in the key also we have to fill as I/J only in the matrix;
while converting if we land at I/J we may put I or J, whichever be appropriate, refer manual; freq. analysis.

15/01/2025

Hill Cipher: encryption: $C = KP \bmod 26$

plain text = ACT → $P = \begin{matrix} A \\ C \\ T \end{matrix}\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$

$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} * \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \bmod 26$

if key is 3×3 then we should take 3 characters at a time.

"Pay more money", key = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$ (key)

15 0 24

$\begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} 17 \\ 17 \\ 11 \end{bmatrix}$ → RRL

So Pay → RRL

"Attack" key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ 2×2 so use 2 characters at a time

At $\begin{bmatrix} 0 \\ 19 \end{bmatrix}$

If key is text, just make that a matrix,
key = ciphering, 3×3. →

2	8	5
7 h	4 e	17 r
8	13	6
i	n	g

$\begin{bmatrix} 2 & 8 & 5 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$

then split plaintext as 3 char each.
eg. Safe messages = plain text
PT05

CT = HDS1OEXQOL4A

Polyalphabetic cipher: key: the, pt: Hello

if key.size() < pt.size() then write the key

Hello → 7 4 11 11 14

(+) thethe → 19 7 4 19 7

enc: (pt+k)%26

%26 = a

plaintext = we are discovered save yourself

key = deceptive → 3 4 2 4 15 19 8 21 4

Z i C v t w q n g z g v t u a v 2 h c q x g l m g

20/01/2025 Caesar cipher

Additive cipher: A → K, B → -K, a+b ≡ 0 mod n

shift cipher

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

(a,b): key pair

Eg: hello → 7,4,11,11,14 $\xrightarrow{+15}$ 22,19,0,0,3 (mod 26)

k = 15

n = 26

w t a a d

Cryptanalysis: how strong it is / how fast we can break

* brute force attack 26?

* statistical attack / pattern attack.

↳ A char always has the same symbol in CT

words like and, the, of occur many times

Multiplicative cipher: $C = (P * K) \% 26$, $P = (C * K^{-1}) \% 26$

$a * b \equiv 1 \bmod n$, (a,b) is key pair $\Rightarrow b = gcd(n,3) = 1$, $\in Z_n^*$

$Z_6 = \{0,1,2,3,4,5\}$, $Z_6^* = \{1,5\} \Rightarrow \{(1,1),(5,5)\}$ ((a,b) (a,b))

are the possible pairs.

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

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

6 key pairs: {(1,1),(2,4),(3,5),(4,2),(5,3),(6,6)}

Affine cipher: one key for multiplication, another for addition, $t = p * k_1 \% 26$, $C = (t + k_2) \% 26$ encryption

in decryption $t = (C - k_2) \% 26$, $p = (t * k_1^{-1}) \% 26$

Eg. PT : "hello", key pair $(\overset{k_1}{7}, \overset{k_2}{2})$. CT ?

sol: $t = (p * k_1) \% 26$ so

	h	e	l	l	o
	7	4	11	11	14
*7 =	23	2	25	25	20
+2	25	4	1	1	22
	z	e	b	b	w

$+2^{-1} = -2$ or $+24$

$*7^{-1} = 15$

Decrypt: z e b b w

	z	e	b	b	w
	25	4	1	1	22
$+2^{-1}$	23	2	25	25	20
$*7^{-1}$ (=15)	7	4	11	11	4
	h	e	l	l	o

15, 7, 105 ①
105, 26, 26, 52, 78, 104
25, (7), 78 ✓

Cryptanalysis: * Bruteforce * Statistics / pattern

Find key pair of the Affine cipher

i) PT : et CT : WC

	e	t
k_1	4	19
	$4*k_1$	$19*k_1$

$(4*k_1) + k_2 = 22$ ①

$(19*k_1) + k_2 = 2$ ②

$-15 k_1 = -20$

$-15 = +11 \% 26$

-13 = +13, 2-26

so ~~$15k_1 = 20$~~ ? $k_1 = 20 * 15^{-1}$

~~then $4k_1 = 2$~~ $k_1 = 20*7$

~~$k_1 = 140$~~

~~$k_1 \% 26 =$~~

→ ~~$k_1 = 20*$~~ $k_1 = 380 \% 26 = 16$

$\Rightarrow 11k_1 = 20 \Rightarrow k_1 = 20 * 11^{-1}$

$k_1 = 20 * 19$ $(11^{-1} = 19)$

$k_1 = 380$

But $k_1 \in Z^*_{26}$ so ???

or do 19 ① − 4 ② ⇒ $15k_2 = 410 \Rightarrow k_2 = 410 * 15^{-1}$

$k_2 = 10$

$4*k_1 + 10 = 22 \Rightarrow 4k_1 = 12 \Rightarrow k_1 = 3$

(11, 4) is ans? (i) is invalid?

ii) PT : et , CT : wf valid? $k_1 = 1$, $k_2 = 11$

Improve strength: * increase key domain.

* choose another mapping (~~like start 1 from A ... than 0 to 25~~) (circular. ⇒ 26! permutations of (0 to 25)

↳ ig like $\underset{0}{A}\ \underset{1}{B} \ldots \underset{25}{Z}$ is not necessary, give some other perm of 0-25

Polyalphabetic:

* one to many * hides the letter freq of ?
* key stream? set of keys. $K : (k_1, k_2, \ldots, k_n)$

PT $P_1\ P_2 \ldots P_n$

CT : $P_1+k_1, P_2+k_2 \ldots$

Autokey cipher:

1st subkey : A and B agree b/w a key, 2nd subkey = 1st char of PT, 3rd subkey = 2nd char of PT

Eg: K_1 = 12 agreed by A & B k_{ij}

	0	19	19	0	2	K^{10}
PT:	a	t	t	a	c	k
key:	12	0	19	19	0	2
CT:	12	19	12	19	2	12.
	m	t	m	t	c	m

261 / 38 (26 / 12   k: 1 in 10

* key domain small   * digrams, trigrams cannot be detected.

21/01/2025 Vigenere Cipher $1 \le m \le 26$

Key stream: block of m char repeatedly

	18 7 4	8 18	11 8 18 19 4 13 8 13 6
PT:	"She	is	listening"
	P A S	C A	L P A S C A L P A
26	15 0 18	2 0	11 15 0 18 2 0 11 15 0
	H H W	K S	W X S B G N T C G

Keystream: PASCAL

$C_i = P_i + K_i$

$P_i = C_i - K_i$

possibility for repitition $m, k+m$, if same char in pt

Kasiski exam, Index of coincidence   m & k+m

Cryptanalysis: as m inc, it becomes more difficult to break.

Bruteforce: (try all m = 1 to 26 poss strings)

OTP: One Time Pad / Vernam Cipher.

Key stream: length = length of PT.

So we can't reuse keys for diff PT, that's why one time pad.

$C_i = P_i + K_i$

$P_i = C_i - K_i$

PT = "CRYPTOGRAPHY"

Key = IAMINSIXPHSE

Cryptanalysis: Cannot be broken since randomly a key is each time used, even if broken next time a diff key is used.

Transposition Cipher.

No substitution, it just reordered/transposes chars

- → Keyless.
- → Keyed.

methods: row by row, col by col

Write col by col. I/P: no of rows. 2 rows:

MEET MEAT THE PARK

MEMATEAK
ETETHPRK $ ⇒ MEMATEAKETETHPRK$
CT

Decryption: 2 rows known by receiver (no of rows)
length of msg = 16, 16÷2 = 8 ⇒ so put (8 cols), write as 2 rows
(M E M A T E A K
E T E T H P R K) → Read col by col → MEETMEATTHEPARK$
3 in each row.

I/P is no of cols ⇒ write as row by row... Eg. 4 cols

M E E T
M E A T
T H E P
A R K $

MMTAEEHREAEKTIP$ is PT.

Keyed TC: PT: block ⇒ key & permute PT block

ENEMYATTACKSTONIGHT$. split into groups of 5

ENEMY ATTAC KSTON IGHT$
1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5
3 1 4 5 2 3 1 4 5 2 3 1 4 5 2 3 1 4 5 2 ⇒ Encryption
EEMYN TAACF TKONS HIT$G → CT

3 1 4 5 2
ENEMY ATTAC KSTON IGHT$ ⇒ Decryption → PT

10:30 Combining Two approaches:
Encrypt: PT row by row, then wrt key

Cryptanalysis: No change in char, only pos changes
is prone to statistical attack.

Bruteforce: C' = |PT| = |CT| key size should divide C;
usually 1 and C are not considered.
L!, is sizeof key domain.

Symmetric ciphers → stream ciphers Eg additive, multiplicative
→ block cipher

Modern Block cipher:
ECB: electronic Code-Block → each block wrt same enc key
CBC, CFB, OFB, CTR → counter, inc for each block, enc &

CBC: each block ⊕ with prev ct block then encrypted
CFB: like CBC, but before XOR some manipulation
OFB: each block ⊕ with prev block after encryption (before) (Encryption placed just like ⊕, another ver is there).

Property 1 : if $a|1$ then $a = \pm 1$

Property 2 : $a|b$ and $b|a \Rightarrow a = \pm b$

Property 3 : $a|b$ and $b|c \Rightarrow a|c$

Property 4 : $a|b \wedge a|c \Rightarrow a|(mb+nc)$

Euclidean Algo to find gcd for large numbers on two facts : $gcd(a,0) = a$, $gcd(a,b) = gcd(b, r)$, $r = a \% b$

Eg: $gcd(36,10) = gcd(10,6) = gcd(6,4) = gcd(4,2)$
$= gcd(2,0) = 2$

$gcd(161,28) = gcd(28,21) = (21,7) = 7$

$gcd(25,60) = gcd(60,25) = gcd(25,10) = gcd(10,5) = 5$

$r_1 \leftarrow a$, $r_2 \leftarrow b$;
while ($r_2 > 0$) {
  $q_1 \leftarrow r_1 / r_2$;
  $r \leftarrow r_1 - q * r_2$
  $r_1 \leftarrow r_2$;
  $r_2 \leftarrow r$;
}
return r_1;

q	r_1	r_2	r
0	306	657	306
2	657	306	45
6	306	45	36
1	45	36	9
4	36	9	0
	(9)	0	

Eg. $gcd(306, 657)$; $r_1 \leftarrow 306$, $r_2 \leftarrow 657$

$r_2 > 0 \Rightarrow q_1 : 0$, $r : 306$, $r_1 : 657$, $r_2 : 306$

$r_2 > 0 \Rightarrow q_1 : 2$, $r : 45$, $r_1 : 306$, $r_2 : 45$

q_1 :

22/01/2025

Extended Euclidean Alg:
Given two integers a, b finds out d other integers s, t st. $sa + tb = gcd(a,b)$

$r_1 \leftarrow a$, $r_2 \leftarrow b$, $s_1 \leftarrow 1$, $s_2 \leftarrow 0$, $t_1 \leftarrow 0$, $t_2 \leftarrow 1$

while ($r_2 > 0$) {

$q \leftarrow r_1 / r_2$

$r \leftarrow r_1 - q * r_2$

$r_1 \leftarrow r_2$; $r_2 \leftarrow r$

$s \leftarrow s_1 - q * s_2$

$s_1 \leftarrow s_2$; $s_2 \leftarrow s$

$t \leftarrow t_1 - q * t_2$

$t_1 \leftarrow t_2$; $t_2 \leftarrow t$

}

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

Eg. for a = 161 and b = 28

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	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	
	$r_2 = 0$								

28 | 6 | 4
168
161

$161 \times (-1) + 6 \times 28 = -161 + 168 = 7 = \gcd$

Eg. (272, 1479)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	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		-2	7	
2	17	0		-38			7		

So gcd = 17, s = -38, t = 7.

Eg. 143, 227

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

3 7 2 1 12 −17 63 −19 27 −100

2 1 −17 63 27 −100

1 0 63 −100

gcd s t

$63 \times 43 - 100 \times 27 =$

03/12/2025

4. 2740, 1760 Find gcd

$r_1 = 2740$, $r_2 = 1760$ $q = 1$ $r = 980$

$q = 1$ $r = 980$ $r_1 = 980$, $r_2 = 780$

$q = 3$ $r = 200$ $r_1 = 780$ $r_2 = 180$

$q = 4$ 180, 60, 0

Linear Diophantine Equations: $ax + by = c$

(Int solns)

If $d \nmid c$, ($d = \gcd(a,b)$), then eqn has no soln.

If $d \mid c$ then ∞ solns.

Particular soln:

1. Reduce eqn to $a_1 x + b_1 y = c_1$ by $\div d$ on b/s
2. Solve for s and t in $a_1 s + b_1 t = 1$ using the extended Euclidean algo.
3. Particular soln is $x_0 = \frac{c}{d} s$, $y_0 = \frac{c}{d} t$

General soln: $x = x_0 + k(b/d)$, $y = y_0 - k(a/d)$

k is an integer

Eg: $21x + 14y = 35$, $d = \gcd(21, 14) = 7$, $7 \mid 35$

$\div 7$ $3x + 2y = 5$

$3s + 2t = 1$ using extended Euclid algo

$r_1 \leftarrow 3$, $r_2 \leftarrow 2$

q	r_1	r_2	r	s_1	s_2	$s = s_1 - qs_2$	t_1	t_2	$t = t_1 - qt_2$
1	3	2	1	1	0	1	0	1	−1
1	2	1	0	0	1	−1	1	−1	2
	1	0		1			−1		
	gcd	stop		s			t		

$s = 1$, $t = -1$.

particular: $x_0 = \frac{35}{7} \cdot 1$, $y_0 = \frac{35}{7}(-1)$

$x_0 = 5$, $y_0 = -5$

$x = 5 + 2k$, $y = -5 - 3k$

Properties of Modulo operations

1. $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
2. $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
3. $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

4. Prove that remainder of an integer divided by 3 is the same as remainder of the sum of its decimal digits.

3547 %3
0+2+1+1 %3=1

Sol. $x = d_0 + 10d_1 + 10^2 d_2 + 10^3 d_3 + \cdots$

$x \bmod 3 = d_0 \bmod 3 + 10 \bmod 3 \times d_1 \bmod 3 + (10 \times 10) \bmod 3 \times d_2 \bmod 3$

$= d_0 \bmod 3 + 10 \bmod 3 \times d_1 \bmod 3 + (10 \times 10 \times 10) \bmod 3 \times d_3 \bmod 3 \cdots$

$= d_0 \bmod 3 + d_1 \bmod 3 + d_2 \bmod 3 + d_3 \bmod 3 + \cdots$

$= (d_0 + d_1 + \cdots) \bmod 3 \quad (\because 10 \bmod 3 = 1)$

Inverse : additive inverse : $a + b \equiv 0 \bmod n$

multiplicative inverse : $a \times b \equiv 1 \bmod n$. $\gcd(a, n) = 1$

Multiplicative inv in Z_{10} : $\gcd(x, 10) = 1 \Rightarrow x = 1, 3, 7, 9$

(1, 1), (3, 7), (7, 3), (9, 9)

Use extended Euclidean also to find multiplicative inv. : $s \times n + b \times t = 1$

take mod n $\Rightarrow$ $(b \times t) \bmod n = 1 \bmod n$ so $t \equiv b^{-1} \bmod n$

5. Find $11^{-1} \bmod 26$ $\Rightarrow$ $n = 26$, $s \times 26 + 11 \times t = 1$

Sol. find t using extended Euclidean algo.

q	r	r_2	r_1	s_1	s_2	$s = s_1 - q s_2$	t_1	t_2	$t = t_1 - q t_2$
2	26	11	4	1	0	1	0	1	-2
2	11	4	3	0	1	-2	1	-2	5
1	4	3	1	1	-2	3	-2	5	-7
3	3	1	0						
	1	0							

unnecessary

$3 \times 26 - 7 \times 11 = 1 \rightarrow \bmod 26 \Rightarrow (-7) \times 11 \equiv 1 \bmod 26$

$26 - 7 = 19$ $\therefore$ $11^{-1} \equiv 19 \bmod 26$

04/02/2022 Linear Var linear eqn;

If $d \mid b$, use this $ax \equiv b \bmod n$, assume $\gcd(a,n) = d$, else it is not possible.

1. $\div$ bs by d (including the modulus),
2. $*$ bs by a^{-1}, find particular sol. x_0.
3. General solution: $x = x_0 + k\left(\frac{n}{d}\right)$. $k = 0, 1, \ldots, d-1$

Eg: $10x \equiv 2 \bmod 15$

Sol: $d = \gcd(10, 15) = 5$ $\quad 5 \nmid 2 \Rightarrow$ no soln.

Eg: $14x \equiv 12 \bmod 18$ $\quad d = \gcd(14, 18) = 2$

$2 \mid 12$ so $\Rightarrow \quad 7x \equiv 6 \bmod 9$

$7^{-1} \equiv 4 \bmod 9$ $\quad$ so $\quad 7 \times 4x \equiv 4 \times 6 \bmod 9$

$28x \equiv 24 \bmod 9 \Rightarrow \quad x = 6 \bmod 9$

$x_0 = 6$. General soln: $x = 6 + k\left(\frac{18}{2}\right)$ $\quad k = 0, 1$

$\Rightarrow x = 6 + 9k \quad \Rightarrow \quad x = 6, 15$

Set of Linear eqns:

$3x + 5y + 7z \equiv 3 \bmod 16$

$x + 4y + 13z \equiv 5 \bmod 16$

$2x + 7y + 3z \equiv 4 \bmod 16$

$A \cdot X = B$

$X = A^{-1} B$

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix}$$

A

Sol: $I = AA^{-1}$

$$\text{adj } A = \begin{bmatrix} 1 & 7 & 15 \\ 9 & 11 & 5 \\ 5 & 0 & 7 \end{bmatrix}$$

Everything is mod 16.

$|A| = 3(1) + 5(7) + 7(15) = 6 + 9 = 15$

$|A|^{-1} = 15^{-1} = 15$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{|A|} \cdot \text{adj}A \cdot \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} = |A|^{-1} \cdot \text{adj}A \cdot \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix}$$

$$= 15 \cdot \begin{bmatrix} 1 & 7 & 15 \\ 9 & 11 & 5 \\ 5 & 0 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \bmod 16$$

$A^{-1} = \frac{1}{|A|} \text{adj}A$

$$= 15 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \bmod 16$$

$$= \begin{bmatrix} 15 \\ 30 \\ 30 \end{bmatrix} = \begin{bmatrix} 15 \\ 14 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 14 & 11 \\ 9 & 5 & 0 \\ 1 & 11 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \bmod 16$$

$$\begin{bmatrix} 15 \\ 47 \\ 44 \end{bmatrix}$$

Ans: $x = 15, y = 14, z = 12$

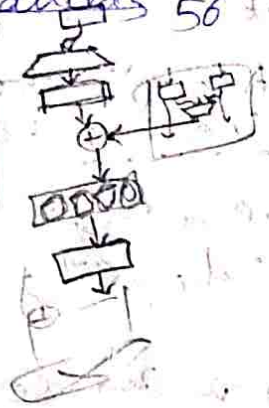
04/02/2025 10:30 DES not as secure as AES

I/P : 64 bits. Plaintext

16 rounds, 16 keys : one key for each round.

64 bit key reduced → 56 bit

Round key size : 48 bits



64 bit PT

↓

Init Perm

↓ 64 bit

Round 1

↓ 64 bit

Round 2

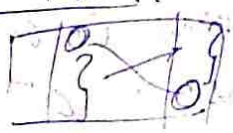
⋮

Round 16

↓

32 bit swap

expansion p-box :



05/02/2025 Meet in the middle attack

18/02/2025 Algebraic structures

Group : set of properties and axioms are satisfied by it : * closure * associativity existence of identity * inverse

ae = ea = a aa' = a'a = e

If all these and commutative : commutative group / abelian group

1. $\langle Z_n, + \rangle$ $n = 10$ 2. $G = \langle Z_n^*, * \rangle$ $n = 12$

1. $Z_n = \{0, 1, 2, \ldots, 9\}$

$x_1, x_2 \in Z_n$ $x_1 + x_2 \in Z_n$. closure ✓

$(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$ assoc ✓

0 is identity ✓

inverse : (0,0), (1,9), (2,8), (3,7), (4,6), (5,5)

So it is a group.

2. $Z_{12}^* = \{1, 5, 7, 11\}$ closure ✓ $x_1, x_2 \in Z_{12}^*$ $x_1 * x_2 \in Z_{12}^*$

assoc: $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$ ✓

Identity : $e = 1$ $x_1 * 1 = 1 * x_1 = x_1$ ✓

Inverse : (1,1), (5,5), (7,7), (11,11) ✓

∴ It is a group.

3. Given $S = \langle \{a,b,c,d\}, \cdot \rangle$

·	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

1. closure ✓ all entries $\in \{a,b,c,d\}$

2. assoc check:
$a \cdot (b \cdot c) = a \cdot d = d$
$(a \cdot b) \cdot c = b \cdot c = d$
$b(a \cdot c) = bc = d$
$(ba)c = bc = d$ ...

3. Identity is a $a \cdot x = x \cdot a = x$.

4. Inverse: $a^{-1} = a$, $b^{-1} = d$, $c^{-1} = c$, $d^{-1} = b$

Finite Group: If number of elements in the set are finite.

Order of a Group: $|G|$ = no of elements in group

Group ⟶ finite ⟹ order
Group ⟶ Infinite ⟹ order

Subgroups: Subset H of a group G is a subgroup of G if (1.) H itself is a group wrt to the ops on G.

If $G = \langle S, \cdot \rangle$ then $H = \langle T, \cdot \rangle$

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

Eg: Given $G = \langle Z_{12}, +_{12} \rangle$ find if $H = \langle Z_{10}, +_{10} \rangle$ is a subgroup.

Sol. $8, 9 \in Z_{12}$ and Z_{10} ... $(8+9) \% 12 = 17 \% 12 = 5$
$(8+9) \% 10 = 17 \% 10 = 7$
⇒ ops are not same $+_{12}, +_{10}$
⇒ H is NOT subgroup of G.

Cyclic Subgroup: If subgroup of a group can be generated using power of element, then it is a cyclic subgroup. Power - repeatedly applying the op

Eg: $G = \langle Z_6, +7$ find cyclic subgroups of G.

Sol. $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$0^0 \bmod 6 = 0$, $0^1 \bmod 6 = 0$, $0^2 \bmod 6 = 0$, ...
$1^0 \bmod 6 = 0$, $1^1 \bmod 6 = 1$, $1^2 \bmod 6 = (1+1) \bmod 6 = 2$.
$1^3 \bmod 6 = (1+1+1) \bmod 6 = 3$ $1^4 = 4$, $1^5 = 5$, $1^6 = 0$

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

$3^0 = 0$, $3^1 = 3$, $3^2 = 6 \bmod 6 = 0$

$4^0 = 0$, $4^1 = 4$, $4^2 = (4+4) \bmod 6 = 2$,

$4^3 = (2+4) \bmod 6 = 0$,

$5^0 = 0$, $5^1 = 5$, $5^2 = (5+5) \bmod 6 = 4$, $5^3 = (4+5) \bmod 6 = 3$

$5^4 = (3+5) \bmod 6 = 2$, $5^5 = (2+5) \bmod 6 = 1$, $5^6 = (1+5) \bmod 6 = 0$

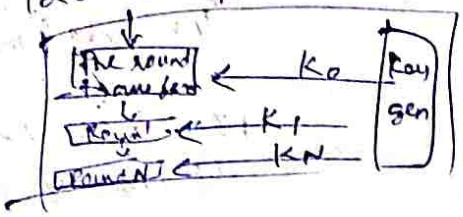
~~$6^0 = 0$, $6^1 = 6$~~

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

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

24 | 02 | 2025 AES

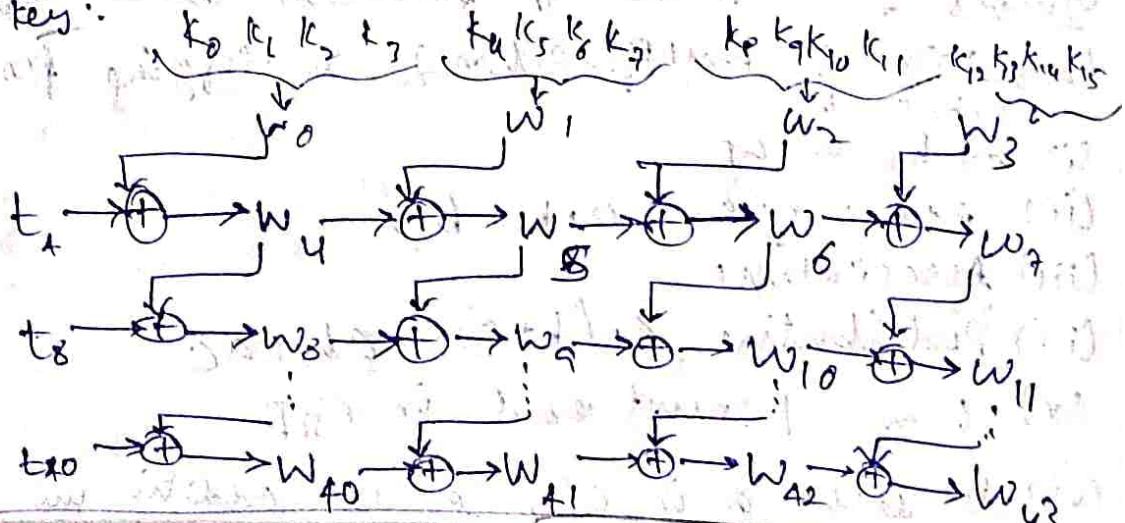
128-bit PT : AES

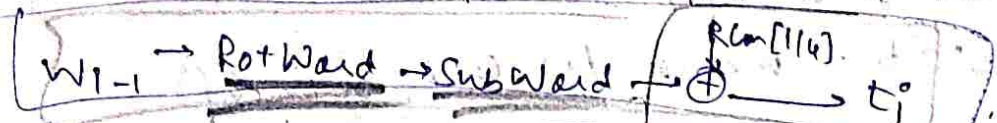


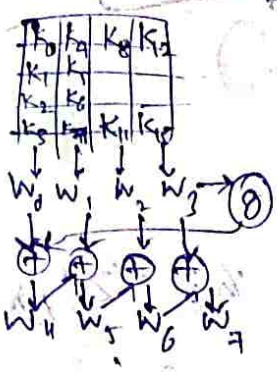
Nk	
10	128
12	168
14	192

Key expansion in AES:

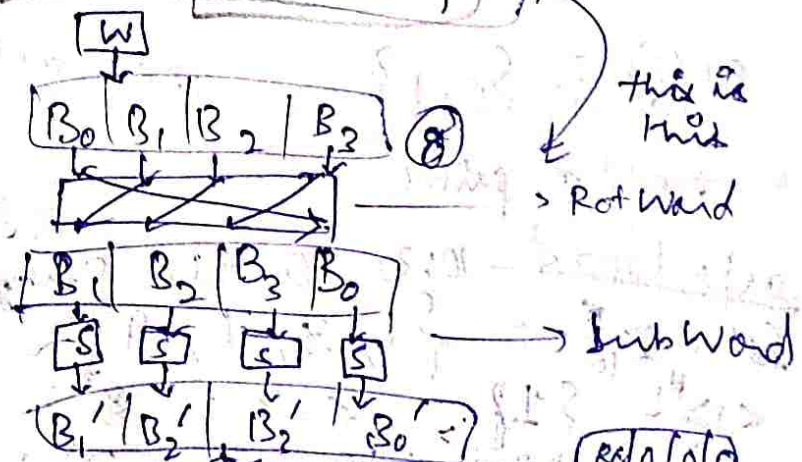
.cipher key.



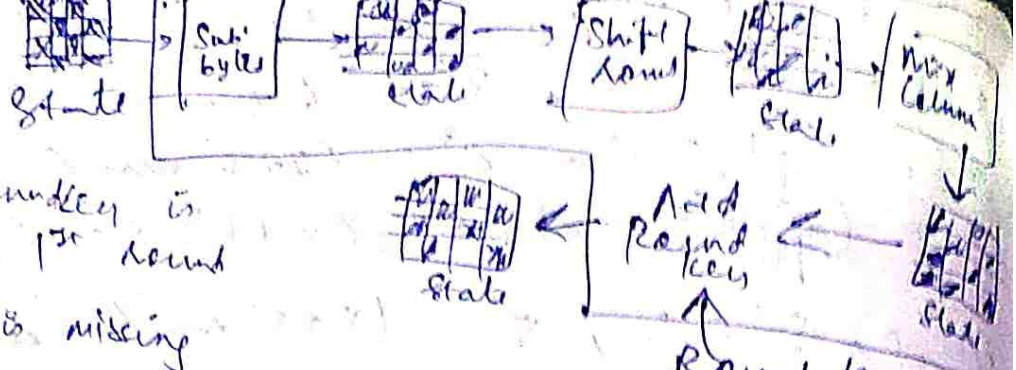




w_{40} w_{41} w_{42} w_{43}



25/02/2025 9:20



1. Additional roundkey is applied before 1st round
2. Third key is missing

SubBytes transformation: ab means see row a, col b entry in the SubBytes trans table.

Encryption:
first: AddRoundKey
then for each round: subBytes, ShiftRows, MixColumns, AddRoundKey
for last round, NO MixColumns

Decryption:
~~first~~: InvMixCol, AddRoundKey
Round 1-9: InvSubBytes, InvShiftRows
for last round (InvMixCol omitted)

Galois Field: set of elements with two operations (addition & multiplication) satisfying properties:
a, b, c in
(i) a+b in GF
(ii) a+b = b+a, a·b = b·a
(iii) Associative
(iv) Distributive a·(b+c) = ab+ac
(v) 0 and 1 must exist in GF
(vi) For each a in GF, a has addition inv -a
(vii) multiplicative inverse for each a in GF

GF(2) = {0, 1} AES works on GF(2^8)
↑ should be prime

~~05/02/2025~~ 10:30 Cyclic subgroups of $G = \langle Z_{10}^*, * \rangle$

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

$\langle 1 \rangle = \{1\}$ H_1

$\langle 3 \rangle \Rightarrow 3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \bmod 10 = 7$, $3^4 = 81 \pmod 3 = 1$

$7^0 = 1$, $7^1 = 7$, $7^2 = 49 \bmod 10 = 9$, $7^3 = 9 \times 7 \bmod 10 = 3$

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

$9^0 = 1$, $9^1 = 9$, $9^2 = 81 \bmod 10 = 1$

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

Q. $G = \langle Z_{12}, + \rangle$ $\quad \langle 0 \rangle = H_0 = \{0\}$ $\quad \langle 1 \rangle = H_1 = \{0, 1, 2, \ldots, 11\}$

$H_2 = \{0, 2, 4, 6, 8, 10\}$, $H_3 = \{0, 3, 6, 9\}$, $H_4 = \{0, 4, 8\}$

$H_5 = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$

$H_6 = \{0, 6\}$ $\quad H_7 = \{0, 7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5\}$

$H_8 = \{0, 8, 4\}$, $H_9 = \{0, 9, 6, 3\}$, $H_{10} = \{0, 10, 8, 6, 4, 2\}$

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

Cyclic group: A group which has a generator.

cyclic subgroup is same as the group Eg H_1, H_5 in $\langle Z_6, + \rangle$.

these elements are called generators.

For $\langle Z_{10}^*, * \rangle$ 3, 7 are generators.

No. of elements in subgroup:

Eg. $|\langle Z_{12}, + \rangle| = 12$, divisors $= 1, 2, 3, 4, 6, 12$ orders will be the order of the subgroups.

Defn: Lagrange's Theorem

Relates the order of group to the order of subgroup.

G is a group, H is a subgroup of G, order $|H|$ $|G|$

used to find potential subgroups of a group.

Order of element a in a group ord(a) is the smallest integer n such that $a^n = e$ [n is the order of cyclic subgroup $\langle a \rangle$]

Eg. $\langle Z_6, + \rangle$ $\quad ord(0) = 1$, $ord(1) = 6$, $ord(2) = 3$,

$ord(3) = 2$, $ord(4) = 3$, $ord(5) = 6$, ~~$ord(6)$~~

Ring : $R = \langle \{\}, \cdot, \square \rangle$ let, 2 ops.

1st op : abelian group

2nd op : first 4 properties (closure, assoc).

Distributivity : 2nd op and 1st op

$a \square (b \cdot c) = (a \square b) \cdot (a \square c)$ must be followed

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

Need this be true? Yes

Commutative ring → 2nd op is comm

Eg : $R = \langle Z_n, +, * \rangle$ $\langle Z_n, + \rangle$ is an abelian group ✓

$\langle Z_n, * \rangle$ closure ✓ * distributes over + ✓

assoc ✓

So R is a ring.

Field : $F = \langle \{\}, \cdot, \square \rangle$

* F is a commutative ring

* 2nd op : Five properties satisfied except identity of op 1 and no inverse in op2

Finite Field / Galois Field :

↓ finite no. of elements. p^n p is prime.

n=1 : $GF(p^1) = GF(p)$

Eg. $\langle Z_7, +, * \rangle$

p = 2 · $GF(2) = \{0, 1\}$, mod 2 :

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

a	0	1
-a	0	1
a^{-1}		1

GF(5) ops +, * is this a field?

$Z_5 = \{0, 1, 2, 3, 4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

All properties ✓

e = 0

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

e = 1

a	0	1	2	3	4
-a	0	4	3	2	1
a^{-1}	-	1	3	2	4

So it is a GF

Group	$(+,-)$ or $(*,\div)$	Z_n or Z_n^*
Ring	$(+,-)$ and $*$	$\cdot Z$
Field	$(+,-)$ and $(*,\div)$	Z_p

GF(2^n) fields : $(0, 2^{n-1})$

Two choices (1) use $GF(p) \rightarrow Z_p$, p is largest prime no $< 2^n$

Eg: $n = 4 \Rightarrow 2^4 - 1 = 15$, $p = 13$ so we cannot use 13, 14, 15.

since we will use Z_{13}, >13 more to there

IIIrd for $n = 8$ — $p < 255$ is $p = 251$.

(2) use $GF(2^n)$ set of 2^n elements.

Elements are n-bit words

Eg. $n = 3$ $\{000, 001, \ldots, 110, 111\}$ ops are done in binary format

$GF(2^2) = \{00, 01, 10, 11\}$

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$e = 00$

*	0 (00)	1 (01)	2 (10)	3 (11)
0 (00)	00	00	00	00
1 (01)	00	01	10	11
2 (10)	00	10	11	01
3 (11)	00	11	01	10

a	00	01	10	11
$-a$	00	01	10	11

a	00	01	10	11
a^{-1}	—	01	11	10

04/03/2025 GF(2^n): n bit representation.

modulus = poly of deg n, cannot be factored

3 bit : 0 – 7 (irreducible polynomials), mod is $x^3 + x + 1$

multi: $(p_1 \cdot p_2) \bmod (\text{deg 2-poly})$ of 2 bits

	00	01	10	11
	0	1	x	x+1

Eg. $00 \cdot 00 = 0 \cdot 0 = 0$ (∵ for all 0's).

$01 \cdot 01 = 1 \cdot 1 = 1 = 01$; $01 \cdot 10 = 1 \cdot x = x = 10$

IIIrd for $01 \cdot ? = ?$, $? \cdot 01 = ?$.

$10 \cdot 10 = (x) \cdot (x) = x^2$, deg >= 2, so take mod with $x^2 + x + 1$

$x^2 \bmod (x^2+x+1) = x+1 = 11$

So $10 \cdot 10 = 11$

$10 \cdot 11 = x \cdot (x+1) = x^2 + x$, take mod x^2+x+1

$= x+1$

so $10 \cdot 11 = 01$

$11 \cdot 11 = (x+1)(x+1) = x^2 + x + x + 1$ ($x + x \to 0$)

$= x^2 + 1$

$\Rightarrow 11 \cdot 11 = 10$

All properties are satisfied. GF(2^n) is a galois field.

Addition of polynomials.

$(x^5 + x^3 + x) \oplus (x^3 + x^2 + 1)$ in GF(2^8)

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

mult : $(x^5 + x^2 + x) \cdot (x^7 + x^4 + x^3 + x^2 + 1)$ in GF(2^8)

irreducible poly is $x^8 + x^4 + x^3 + x + 1$.

$(x^5 + x^2 + x)(x^7 + x^4 + x^3 + x^2 + 1)$

$= x^{12} + x^9 + x^8 + x^7 + x^5 + x^9 + x^6 + x^5$

$+ x^8 + x^5 + x^4 + x^3 + x$

$= x^{12} + x^7 + x^6 + x^5 + x^3 + x^2 + x$

$x^8 + x^4 + x^3 + x + 1$ | $x^{12} + x^7 + x^6 + x^5 + x^3 + x^2 + x$ | $x^4 + 1$

$x^{12} + x^8 + x^7 + x^5 + x^4$

$x^8 + x^6 + x^4 + x^3 + x^2 + x$

$x^8 + x^4 + x^3 + x + 1$

$x^6 + x^2 + 1$

05/03/2025

Asymmetric Cryptography

Find if n prime : If all primes $< \sqrt{n}$, n is div by any of them then it is not prime else prime.

Euler's phi / totient $\phi(n)$ = no of int smaller than n and relatively prime to it. $n \cdot \prod (1 - \frac{1}{p})$ (how can I obtain this?)

1. $\phi(1) = 0$
2. $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ — m, n are relatively prime.
3. $\phi(p) = p - 1$, p is prime
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime,

$\phi(10) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$

$\phi(240) = \phi(5 \cdot 48) = 4 \cdot \phi(48) = 4 \cdot \phi(3 \cdot 16) = 4 \cdot 2 \cdot \phi(2^4)$
$= 4 \cdot 2 \cdot (2^4 - 2^3) = 8 \cdot 8 = 64$

$\phi(49) = \phi(7^2) = 7^2 - 7 = 42$
$\phi(63) = \phi(7) \cdot \phi(3^2) = 6 \cdot (3^2 - 3^1) = 6 \cdot 8 = 48$
$\phi(165) = \phi(11 \cdot 15) = 10 \cdot \phi(5-3) = 10 \cdot 4 \cdot 2 = 80$

Fermat's Little Theorem:

1st version: if p is a prime and a is an integer such that p doesn't divide a then $a^{p-1} \equiv 1 \bmod p$

Find $6^{10} \bmod 11 = 6^{11-1} \bmod 11 \equiv 1 \bmod 11$ (since 11 is prime and it doesn't divide 6).

$a = 2, p = 5$ $\quad 2^4 \bmod 5 \equiv 16 \bmod 5 \equiv 1$.

10/03/2025

condition: p is a prime and a is an integer,

$a^p \equiv a \bmod p$ Eg. $145^{102} \bmod 101 = 145^{101} \times 145 \bmod 101$

$= 145 \times 145 \bmod 101 = 44 \times 44 \bmod 101 = 17$ ig

* If p is a prime, a is an int, $a^{-1} \bmod p \equiv a^{p-2} \bmod p$

Q. $8^{-1} \bmod 17 \equiv 8^{17-2} \bmod 17 \equiv 8^{15} \bmod 17 \equiv$ ~~$2^{45} \bmod 17 = (2^3)^{15} \bmod 17 \equiv 8^{10} \bmod 17$~~ ?

Q. $5^{-1} \bmod 23 = 5^{21} \bmod 23 = (5^2)^{10} \cdot 5 \bmod 23 = 2^{10} \cdot 5 \bmod 23 = (2^5)^2 \cdot 5$
$= 9^2 \cdot 5 = 405 \equiv 14$

Q. $60^{-1} \bmod 101 \equiv 60^{99} \equiv 32$

Euler's theorem:

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

when n is prime, $\phi(n) = n-1$

2nd version of Euler's theorem: used in RSA
* Removes the condition on a and n
If $n = p \times q$, $a < n$, k is an integer then

$$a^{k \cdot \phi(n) + 1} \equiv a \bmod n$$

$\phi(n) = n-1$ (prime n); $k = 1$ then $a^{\phi(n)+1} \equiv a \bmod n \rightarrow a^n \equiv a \bmod n$

Alice: $a^{k \cdot \phi(n)+1} \bmod n \equiv (a^{\phi(n)})^k \cdot a^1 \bmod n$
$\equiv 1 \cdot a^1 \bmod n \equiv a \bmod n$.

Multiplication Inverse: if a, n are coprime - then
$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$ multiplied by a
$a \cdot a^{-1} = a \cdot a^{\phi(n)-1} = a^{\phi(n)} \bmod n \equiv 1 \bmod n$

Eg: $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{60-1} \bmod 77$
$\phi(77) = \phi(7) \cdot \phi(11) = (7-1)(11-1) = 6 \cdot 10 = 60$

Eg: $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{8-1} \bmod 15$

Primality Testing: self
Deterministic
Probabilistic

11/03/2025: B sends to A
Encryption: Public key: B → A's public enc
A → A's private dec; can't guess message is from Bob
Private: B: B's private enc, A: B's public dec
(Anyone can find out what message B sent)

12/03/2025
1. Find d if $e = 17$, $n = 187$ → $\phi(187) = 17 \times 11 = 160$
Sol: $ed \equiv 1 \bmod \phi(n) \Rightarrow d = 17^{-1} \bmod 187 = 17^{\phi(160)-1} \bmod 160$
$= 17^{16 \times 10 - 1} \bmod 187 = 17^{159} \bmod 187 \equiv 17^{63} \bmod 160$?

2. Given $p=7, q=11, e=13$, find d. $d=117$

$n = pq = 77$, $\phi(n) = 6 \cdot 10 = 60$

$d \equiv e^{-1} \bmod n = 13^{-1} \bmod 60 \equiv 13^{\phi(60)-1} \bmod 60$

$= 13^{15} \bmod 60 = 13 \cdot 13^2 \cdot 13^{12} = 13 \cdot 49 \cdot 13^2 =$

$60 = 2^2 \cdot 3 \cdot 5$

$(2^2-2) \cdot 2 \cdot 1 = 16$

3. $p=53$, $q=59$, $e=3$.

i) what is public key ii) what is pvt key?

iii) send msg 'HI' using RSA. Pt is 'HI'

Ct is ? Find!

i) $n = pq = 3127$, $(e, n) = (3, 3127)$ is public key

ii) $d = e^{-1} \bmod \phi(n) = 3^{-1} \bmod (52 \cdot 58) = 3^{-1} \bmod 3016$

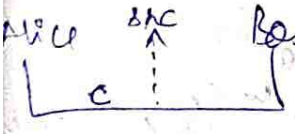
$d = \frac{k \cdot 3016 + 1}{3}$, put $k=2$ gives $\Rightarrow d = 2011$

iii) $H = 7, I = 8$ $\quad C = P^e \bmod n = 17^3 \bmod 3127$

17/03/2025

Attacks on RSA:

1. Factorization Attack: public: n, e private: d



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

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

$n > 300$ decimal digits? modulus ≥ 1024 bits

Choosen CT attacks: Alice: $c = p^e \bmod n$ to Bob

Eve intercepts c

i) choose a random int x in Z_n^* Assume Bob will send decrypted text to alice.

ii) Calculate $y = c \cdot x^e \bmod n$

iii) Eve sends y to Bob

iv) Bob decrypts y $y^d \bmod n \equiv (cx^e)^d \bmod n = c^d x^{ed}$

$= p \times x^1 = z$ (say) then $p = (z \cdot x^{-1}) \bmod n$

$x^{ed} \bmod n = x^{1+k\phi(n)} \bmod n = x \cdot (x^{\phi(n)})^k \bmod n \equiv x \cdot 1^k \bmod n$

(chosen x) $\quad a^{\phi(n)} \equiv 1 \bmod n$ Euler

Attacks on encryption exp:

- If encryption time, small values for e

$e = 3$

$e = 2^{16} + 1 = 65537$

Coppersmith if $m < n^{1/e}$ found, $P^e = C$ solve

$e=3$, $2/3$ of P is known

Broadcast attack : $e = 3$

Alice : 3 diff people. $C_1 = P^3 \bmod n_1$, $C_2 = P^3 \bmod n_2$, $C_3 = P^3 \bmod n_3$

Chinese remainder Theorem unique soln if moduli are relatively prime else > 1 soln.

Related msg attack : P_1, P_2 : related eqns if P_1, P_2 linear for related, eve can get P_1, P_2 from C_1, C_2

Short pad attack.

alice $(M+r)$ ✗ bob

(eve intercepts & resends) and drops, so Bob doesn't get it, so Alice resends

$(M+r_2)$ eve like alice retransmitting and keeps intercepting, now using C_1, C_2 if r_1, r_2 were short she could find M.

$$d > \frac{1}{3} n^{1/4}$$

Cycling attack : $C = P^e \bmod n$

$C_1 = C^e \bmod n$, $C_2 = C_1^e \bmod n$, $C_3 = C_2^e \bmod n$

$C_k = C^{(k-1)e} \bmod n$, stop when getting $C_k = C$, then C_{k-1} is P.

if C is permutation of P?

Chinese Remainder Theorem :

One var, diff moduli → gcd $= 1$ ⇒ unique soln

→ gcd > 1 ⇒ > 1 soln

Given $x = a_1 \bmod m_1$, $x = a_2 \bmod m_2$, ... $x = a_k \bmod m_k$

Steps :

1. Find $m = m_1 m_2 \cdots m_k$ common modulus
2. Find $M_1 = \frac{m}{m_1}$, $M_2 = \frac{m}{m_2}$, ..., $M_k = \frac{m}{m_k}$
3. Find M_i^{-1} of $M_1, M_2, \ldots, M_k$ wrt $m_1, m_2, \ldots, m_k$ let it be $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$
4. $x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1})$

Eg: Find x if $x \equiv 2 \bmod 3,\ 3 \bmod 5,\ 2 \bmod 7$

Sol. $M = 3 \cdot 5 \cdot 7 = 105$ $\gcd(3,5,7) = 1$ so unique soln

$M_1 = 35,\ M_2 = 21,\ M_3 = 15$

$M_1^{-1} = 35^{-1} \bmod 3 = 2,\ M_2^{-1} = 21^{-1} \bmod 5 = 1,\ M_3^{-1} = 15^{-1} \bmod 7 = 1$

$x = 2 \times 2 \times 35 + 3 \times 1 \times 21 + 15 \times 1 \times 2$

$= 140 + 63 + 30 = 233$

140
63
30
233

Ex. $x \equiv 3 \bmod 4,\ 5 \bmod 6,\ 2 \bmod 5$ → same as 2 mod 3.

$M_1 = 30,\ M_2 = 20,\ M_3 = 24$

Application:

Solve quadratic congruence:?

Represent very large/small ind

Eg. $z = x + y$, $x = 123$, $y = 334$. we can represent numbers only < 100 in the system so

$x \equiv 24 \bmod 99$ $\quad y \equiv 37 \bmod 99$

$x \equiv 25 \bmod 98$ $\quad y \equiv 40 \bmod 98$

$x \equiv 26 \bmod 97$ $\quad y \equiv 43 \bmod 97$

$x+y = (24+37) \bmod 99$

$x+y = (25+40) \bmod 98$

$x+y = (26+43) \bmod 97$

} use CRT to find $x+y$ now

18/3/2025 $c = 2,\ d = \frac{1}{2}$ in RSA

public: n, private: (p,q)

Rabin? Cryptosystem

$c = p^2 \bmod n$, $p = c^{1/2} \bmod n$

$p \neq q$

p, q : $4k+3$ form, $p \neq q$

p, q are large numbers

$(4k+3) \equiv 3 \bmod 4$

$a_1 \leftarrow +c^{(p+1)/4} \bmod p$, $a_2 = -a_1$ [four PT's (see Q)]

$b_1 = c^{(q+1)/4} \bmod q$, $b_2 = -b_1$

Q. Given $p = 7, q = 11, c = 23$. what is P? using Rabin

$a_1 \leftarrow +c^{(7+1)/4} \bmod p$, $a_2 = -4 \bmod 7 = 3$

$= 23^2 \bmod 7 = 9^2 = 4$

$b_1 = 23^{\frac{11+1}{4}} \bmod 11 = 23^3 \bmod 11 = 1^3 = 1$, $b_2 = 1 = 10$

for Robin, the decryption will give 4 PT's ⇒

CRT (a_1, b_1, p, q); CRT (a_1, b_2, p, q)

CRT (a_2, b_1, p, q), CRT (a_2, b_2, p, q)

$a_1, a_2, b_1, b_2 = 4, 3, 1, 10$

P_1 = CRT $(4, 3, 7, 11)$

$a_1 = 4 \bmod 7$, $b_1 = 1 \bmod 11$

$M_1 = 11$, $M_2 = 7$, $M_1^{-1} = 11^{-1} \bmod 7 = 9 \bmod 7$

$M_2^{-1} = 7^{-1} \bmod 11 = 8 \bmod 11$

$P_1 = 4 \times 11 \times 9 + 1 \times 7 \times 8 = 396 + 56 = 452$

$P_1 = 67$

$P_2 = 32$, $P_3 = 45$, $P_4 = 10$

p^2 is 4489, 1024, 2025, 100

$P^2 \bmod 77$ is 23, 23, 23, 23 : matches ciphertext!

Primitive Root:

G is primitive root mod n iff G is generator of the multiplicative group of integers mod n.

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

x	x^1	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1 ✓
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1 ✓

order of primitive root is $\phi(n)$

ElGamal: e_1 is a primitive root mod p, x is random integer in $\langle Z_p^*, \times \rangle$

Eleser, Sonnetring

$e_2 = e_1^d \bmod p$

$C_1 = e_1^x \bmod p$

$C_2 = (e_2^x \times P) \bmod p$

Public key: (e_1, e_2, p)

Decryption: $PT = C_2 (C_1^d)^{-1} \bmod p$

given $p = 11$, $e = 2$, $d = 3$ $\lambda = 4$. e_1 e_2 p

private key $d = 3$, encrypt & decrypt the plain text 7 using ELGamal. how?

Sol: $C_1 = e_1^r \bmod p$, $C_2 = (P \times e_2^r) \bmod p$

$C_1 = 2^4 \bmod 11 = 16 \bmod 11 = 5$ $\quad C_2 = 7 \times 8^4 \bmod 11$

Decr $6 \cdot (5^3)^{-1} \bmod 11 = 6 \cdot (5^{-1})^3 \bmod 11 = 6 \cdot 9 \bmod 11 = 10$

$= 6$

Analysis: Alice sends C_1, C_2

$C_2 = e_2^r \cdot p \bmod p = [e_1^{rd} \text{ (mask)}] \cdot p \bmod p$, rd is not revealed, so cannot be found out by anyone.

19/03/2025 Key Distribution Centre

Kerberos: authentication

Diffie Hellman $R_1 = g^x \bmod p$ $\quad R2 = g^y \bmod p$ $\quad K = g^{xy} \bmod p$

discrete log, man in middle

Station to station key agreement

25/02/2025 CCM, CMAC, GCM 2 fns → GHASH & CTR

PRNG

Security: 4) low modulus, large $p \approx 300$ digits, DLP can't be solved

a) Known PT: same 'r', $C_2 = Pe_2^r \bmod p$, $C_2' = P' e_2^r \bmod p$

if Eve comes to know P, she gets e_2^r also, so she can get P' also. $= C_2 \times P'$