Cryptography & Network Security.

U1

U2 ~ Mathematical, Number Theory (Syllabus dekho bro)

Jul 23, 2024

UI : Intro

Cryptography → Data Security

- If all Networking systems in world worked independently there would by no need of Network Security or Cryptography.
  ↳ ∵ Since No Network!

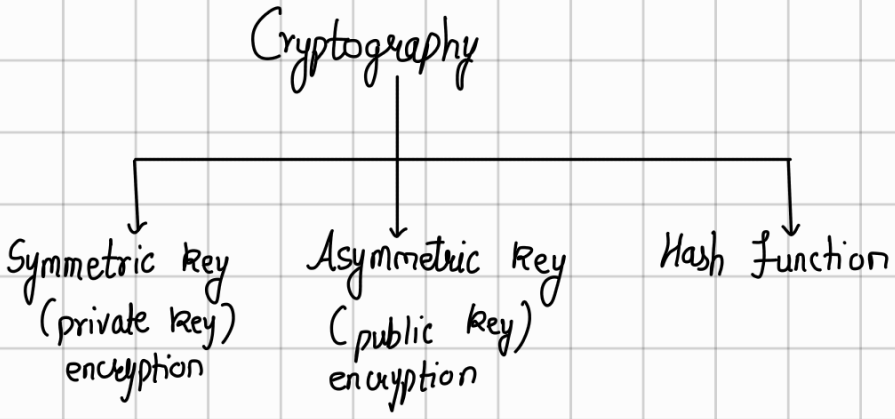
- CIA → Confidentiality, Integrity, Availability (Tripod of Securi

  Spelling?

  Confidentiality → Authorized People only should have data access. Even if available, Shouldn't be interpretable.

  Integrity → Data Should be as it was! It should not be tampered or changed from initial. → check Integrity by using "Cryptographic Checksum" called Hash functions.

  Availability → Making service available with minimum downtime to serve client requests.



- Digital Certificate

  Data → Hash algo → hashed key
  ↓
  hash with private key of Certification Authority
  ↓
  hashed key$_{CA}$
  ↓
  decrypt using public key of Certification Authority for verification

- Digital Signature?
- SSL - Secure Socket Layer

Imp terms : Threat , Vulnerability, Attack

- Threat → A Potential that can cause harm to our system
- Vulnerability → Weakness in the System
- Attack → A human exploiting a vulnerability in the computer system

VAPT → Vulnerability Assessment and Penetration testing.

- Tools available in VAPT?

- Computer Security , Network Security , Internet Security
- Data , DB, OS, Program Security

Kinds of Threat

- Interception → release of message contents by Methods like traffic analysis (e.g. Network Sniffing tools)
- Interruption → Connection is hampered / closed
- Modification → altered msg
- Fabrication → Completely different msg.

Cyber Security Attacks :

- Passive Attack
  - ↳ No data alteration ; Hard to detect ; Only listening to data.
- Active Attack
  - ↳ Attempt to alter system resources or affect the operation.

Attack Description

- IP Scan & Attack
- Web Browsing
- Virus
- Unprotected Sharing
- Mass Mail
- Simple Network Management Protocol
- Backdoors
- Password Crack
- Bruteforce
- Dictionary.

- Spoofing
- Man-in-the-middle
- Spam

how to detect DDOS attack?

OSI Security Architecture

- Substitution Cipher
- Pigpen Cipher (weak cipher)
- ADFGVX Cipher (strong cipher
- Caesar Cipher (Encrypted ⇒ $(p+k)$ MOD 26.)
  (Decrypt ⇒ $(p-k)$ MOD 26)
  $(a-b)$

	A	D	F	G	V	X
A	8	p	a			
D	—			.	.	.
F		—				
G						
V						
X						

Generated randomly

MOD 256 for ASCII

Code with nums as our computers are better with characters.

8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

sdd qgmj tskw sjw twdgfy lg mx

1 tee rh
2 uff
3 v gg
4 w hh
5 x ii
6 y jj
7 z kk
+8 all your base are belong to us

P- Plain text

- Mono alphabetic Cipher (shuffle letters arbitarily)
- Affine Cipher $C = (ap + b)$ MOD 26

  $p = (a^{-1}(c-b))$ MOD 26

e. $a = 3$
$b = 7$

$e \rightarrow (3p+7) \,\%\, 26$ ← Use this

the dog ⟶ MCTQXZ

TIVUJWL ⟶ EJW

Modular multiplicative inverse of a : $a * a^{-1} = 1$ MOD (26)

$3 * 9 = 1$ MOD 26

06-Aug-2024

Number Theory!

Divisor:

'|' → Pipe means "divides"

'/' → slash means "divided by"

b|a → b divides a

b/a → b divided by a

0 is divisible by every number.

Prime Numbers:

relatively prime/
Co-prime → GCD of two numbers is 1.
(a,b) are coprime

Fundamental theorem of arithmetic :

Primality Testing

Greatest Common Divisior : largest number that divides both (a,b)

Euclidean Algorithm: (To find GCD of given two algorithms)

↳ a,b ⇒ A=a , B=b

while B > 0 (*)

⋮

• Modular Arithmatic

- Congruence → a, a' are congruent to each other if the remider obtained is the same, i.e. $a \equiv a' \pmod b$

↳ Congruent / equivalent.

• (mod) congruence formal definition.

• Modular Arithmatic

addition ⇒ $(a+b) \bmod n \equiv (a \bmod n) + (b \bmod n)$

Subtraction ⇒ $a-b \bmod n = a+(-b) \bmod n$

Multiplication ⇒ $a*b \bmod n$ ⇒ first multiply then mod:

thus we might get $a*b \bmod n \equiv 0$, but $a,b \neq 0$

$2*3 \bmod 6 = 0$

Division ⇒ $b/a \bmod n$

- $b/a = b*a^{-1} \bmod n$
- $a^{-1}*a \equiv 1 \bmod n$

Inverse does not always exist ; it exists when $\gcd(a,n)=1$

Additive inverse property: $(a+-a)=0$.

for mod 12 (n), $a=6$, $a^{-1}=6$,

$a=7$, $a^{-1}=5$,

$\therefore a^{-1} = n-a$

Multiplicative Inverse Property: $\gcd(a,n)=1$ then only exists

Multiplication table in Z_n.

• Zero never has an inverse.

GF → Galluli's field → defined over prime numbers

find multiplicative Inverse of 15 in mod 26.

Q	A_1	A_2	A_3	B_1	B_2	B_3
-	1	0	26	0	1	15
1	0	1	15	1	-1	11
1	1	-1	11	-1	2	4
2	-1	2	4	3	-5	3
1	3	-5	3	-4	7	1

← T

$T_i = A_i - Q_i B_i$

from above we have,

$$26 * -4 + 15 * 7 = -104 + 105 = 1$$

$X \quad m \quad Y \quad n$

$mX + nY = 1$

Method 2:

→ to find GCD

15 Mod 26

$26 = 15*1 + 11$ $\quad 11 = 26 - 15*1$

$15 = 11*1 + 4$ $\quad 4 = 15 - 11*1$

$11 = 4*2 + 3$ $\quad 3 = 11 - 4*2$

$4 = 3*1 + 1$ $\quad 1 = 4 - 3*1$

$1 = 4 - 1$

PTO to Arrow

Lab Work:

(Deadline → next to next week from 23rd July)

Assignment 1: Design an implement your own encryption/decryption algorithm used for securing communications between server and client.

- Develop Client Server program (JAVA ezz) to send data

- Explorations:
  -

A good algorithm:

- Should be harder to break
  - Preimaging should be hard.
  - Key Size should be Robust
  - Gibberish text should not be decipherable
    → Vovel count 'e' appears more in english so it might be detected easily and deciphered.
    → Perhaps add weight to the variables based on frequency.
    ↳ map [26] → count Of Occurance
    [a...z]
    ↳ Use this for the algo to make frequency confusing.

① 13 Mod 22

② 17 Mod 97

Q A1 A2 A3 B1 B2 B3

-

Prime factorisation:

Euler Totient function:

$\phi(n)$ → No. of non-negative integers less than n which are relatively prime to n.

n	$\phi(n)$	Condition
p	$p-1$	p prime
p^n	$p^n - p^{n-1}$	p prime
$s \cdot t$	$\phi(s) \cdot \phi(t)$	$\gcd(s,t) = 1$
$p \cdot q$	$(p-1)(q-1)$	p, q prime

$\phi(9) =$

Fermat's Little theorem: IF p is prime & p $\nmid$ a (p does not divides a) then $a^{P-1} \equiv 1 \bmod p$

where p is prime & gcd (a,p) = 1

a	$a^6 \bmod 7$
2	$2^6 = 64 \equiv 1 \bmod 7$
3	$3^6 = 729 \equiv 1 \bmod 7$
4	$4^6 = 4096 \equiv 1 \bmod 7$
5	$5^6 = 15625 \equiv 1 \bmod 7$

$2^{1924} \bmod 7$

a

$\equiv 2^{(320*6+4)} \bmod 7$

$1924 = 320*6 + 4$

$= 2^{(320*6)} * 2^4 \bmod 7$

$= (2^{(320*6)} \bmod 7) * (2^4 \bmod 7)$

$= 1 * 16 \bmod 7$

$= 1 * 2$

$= 2$

Euler's theorem:

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

- where gcd (a,n) = 1

$\phi(n) = 6$ ∵ 7 is prime

$2^{1924} \bmod 7$

$2^{(320+4)} \bmod 7$

$2^{(320*6)} \cdot 2^4 \bmod 7$

$2^4 \bmod 7 = 16 \bmod 7 = 1 \bmod 7$

$$
\begin{array}{r|l}
 & 320 \\
\hline
6 & 1924 \\
 & -18 \\
\hline
 & 12 \\
 & -12 \\
\hline
 & 04
\end{array}
$$

- Primitive Roots: - Congruence classes

LIAIE

- Discrete Logarithms

- Algebric structure : Group . . . .

- Finite (Galois) field.
- Polynomial Arithmetic.

1) 2^{50} Mod 17

$2^{(16*3+2)}$ Mod 17

$\frac{2^{16*3}}{1} \cdot 2^2$ Mod 17

$\equiv$ 4 Mod 17

2) 4^{532} Modulo 11

$\rightarrow 4^{(53*10+2)}$ Modulo 11

$\rightarrow 4^2$ Mod 11

$\rightarrow$ 16 Mod 11

$\rightarrow$ 5 Mod 11

$$
\begin{array}{r|l}
11 & 532 \quad (48 \\
 & -44 \\
\hline
 & 92 \\
 & -88 \\
\hline
 & 4
\end{array}
$$

$$
\begin{array}{r|l}
11 & 256 \quad (23 \\
 & -22 \\
\hline
 & 36 \\
 & -33 \\
\hline
 & 3
\end{array}
$$

What is remainder when 3^{100} divided by 7

$p = 7$

$\rightarrow a = 3$

$\rightarrow 3^{(6*16+4)}$ Mod 7

$\rightarrow 3^4$ Mod 7

$\rightarrow$ 4 Mod 7

4) 2^{63} Mod 99 ... Solvable $\because$ gcd $(a,p) = 1$ gcd(2,99) = 1

.... Euler's theorem

$\because$ 99 $\neq$ prime.

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

$\phi(99) = \phi(11) * \phi(3)^2$

$= 10 * 6$

$\phi(99) = 60$

2^{63} Mod 99

$\rightarrow 2^{60} \cdot 2^3$ Mod 99

$\rightarrow$ 8 Mod 99 $\because \phi(99) = 60$ $\therefore 2^{60}$ Mod 99 = 0

find remainder of the division $\frac{3^{45}}{45}$

3^{45} Mod 45

$3^{24} \cdot 3^{21}$ Mod 45

$\phi(45) = \phi(5) * \phi(3^2)$

$= 4 * 6$

$= 24$

$\frac{3^{45}}{45} = \frac{3^2 \times 3^{43}}{9 * 5} = \frac{3^{45}}{5}$

3^{43} Mod 5

$\rightarrow 3^{40+3}$ Mod 5

$\phi(5) = 4$

→ $3^{40} \cdot 3^3 \bmod 5$

→ $3^3 \bmod 5$

→ $27 \bmod 5$

→ $2 \bmod 5$

→ $2 * 9 = 18$

5) $2x \equiv 5 \bmod 7$

$\gcd(2,7) = 1$ $\qquad$ $\gcd(\text{coefficient}, \text{divisior}) = 2$.

$4 \cdot 2x = 4 * 5 \bmod 7$

$= 6 \bmod 7$

$2x \equiv 5 \bmod 8$

$\gcd(2,8) = 2 \neq 1$ $\qquad$ $\therefore$ No solution.

Highest Common factor (HCF)

Type1) 12, 18, 30 = 6 (HCF)

Type 2) 14, 20, 32 = remainder = 2

Type3) (12 - 2, 18 - 3, 30 - 0) $\qquad$ HCF = 5

(10, 15, 30)

find out the number which divides 12, 18, 30 leaving remainders 2, 3, 0. ⇒ 5

LCM types → Smallest number divisible by x, y, z.

Type 1: 6, 9, 12 = 36

Type 2: find smallest - largest n^{th} digit number divisible by x

↳ Smallest 3 digit divisible by 6, 9, 12.

Smallest → 108

largest → 972

9, 12

Type 3:

find out smallest number when divided by x, y, z leaves same remider.

e.g. Number divisible by 6, 9, 12 leaves reminder 2. ⇒ 38.

Type 4:

find out smallest number when divided by 2, 3, 4, 5, 6 ⇒ 60

leaves the remainder 1, 2, 3, 4, 5 ⇒ 59

find greatest number of 5 digit which on divided by 9, 12, 24 and 45 leaves remainders 3, 6, 18, 39 respectively.

9, 12, 24, 45 ⇒ 360 (LCM)

3 6 18 39 354

99720 (Largest divisible number)

∴ 99720 − 6 is the answer

find smallest number, when divided by 7, 9, 11 gives 1, 2, 3 as remainder

7, 9, 11

1, 2, 3

Chinese remainder theorem:

$x = ax_1 + bx_2 + cx_3$

$a = 9 * 11$

$b = 7 * 11$

$c = 7 * 9$

$x = 99x_1 + 77x_2 + 63x_3$

x_1 ① $99 = 14 * 7 + 1$

x_2 ② $77 = 9 * 9 + 5$

$5x_2 = 20 \quad x_2 = 4$

$x_3 = 10$

$x = 99 * 1 + 77 * 4 + 63 * 10$

$= 99 + 308 + 630$

$= 1037 \mod LCM(7, 9, 11)$

$= 1037 \mod 693$

$\boxed{x = 344}$

Nos:	7	9	11
remainder	1	2	3

Chinese Remainder Theorem (CRT)

$x = 99x_1 + 77x_2 + 63x_3$

$99 = 7*14 + 1$ → remainder = 1 → x_1

$77 = 9*8 + 5$; $x_2 =$

we want remainder 2 when x_2 divided by 9,

$9*2 + 2 = 20$

$\therefore 5x_2 = 20$

$\boxed{x_2 = 4}$

$63 = 11*5 + 8$

$8x_3 = 80$

$\boxed{x_3 = 10}$

·/.		·/.MOD Res
8	11	8
16	11	5
24	22	2
32	22	10
40	33	7
48	44	4
56	55	1
64	55	9
72	66	6
80	77	3

$x = 99x_1 + 77x_2 + 63x_3$

$= 1037$

Chinese Remainder

Let $n_1, n_2 \ldots n_k$ be pairwise relatively prime numbers. Then there exists a unique integer 'x modulo $M = n_1, n_2 \ldots n_k$' that satisfies the linear congruences

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$
$$\vdots$$
$$x \equiv a_k \bmod n_k$$

$$x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 \ldots + a_k M_k Y_k \pmod M$$

where,

$$M_i = M/n_i \quad \& \quad M_i Y_i = 1 \bmod n_i$$

Steps:

- Check if all are pairwise relatively prime.

e.g: $x \equiv 1 \pmod 5$

$x \equiv 2 \pmod 6$

$x \equiv 3 \pmod 7$

$M = 5 * 6 * 7 = 210$

	M=210	
$a_1=1$	$M_1 = 42$	$Y_1 = 3$
$a_2=2$	$M_2 = 35$	$Y_2 = 5$
$a_3=3$	$M_3 = 30$	$Y_3 = 4$

$x = 206$ ∫ confirm ans

$x \bmod 5 = 206/5 = 1$

$x \bmod 6 = 206/6 = 2$

$x \bmod 7 = 206/7 = 3$

$M_1 = 210/5 = 42$

$M_2 = 210/6 = 35$

$M_3 = 210/7 = 30$

① $42Y_1 \equiv 1 \bmod 5$

$2Y_1 \equiv 1 \bmod 5$ ... 42 Mod 5

$2 * 3Y_1 \equiv 3 \pmod 5$

$6Y_1 \equiv 3 \pmod 5$

$Y_1 \equiv 3 \bmod 5$ operate Mod 5 on both sides

$\boxed{Y_1 = 3}$

$35Y_2 \equiv 1 \bmod 6$

$5Y_2 \equiv 1 \bmod 6$

$5.5Y_2 \equiv 5.1 \bmod 6$

$25Y_2 \equiv 5 \bmod 6$

$Y_2 \equiv 5 \bmod 6$

$\boxed{Y_2 = 5}$

$30Y_3 \equiv 1 \bmod 7$

$2Y_3 \equiv 1 \bmod 7$ ... Mod operator 7 on LHS

$2.4Y_3 \equiv 1.4 \bmod 7$

$8Y_3 \equiv 4 \bmod 7$

$Y_3 \equiv 4 \bmod 7$

$\boxed{Y_3 = 4}$

$x = a_1 M_1 Y_1 + a_2 M_2 Y_2 + a_3 M_3 Y_3 \pmod M$

$= 1 * 42 * 3 + 2 * 35 * 5 + 3 * 30 * 4 \pmod{210}$

$= 126 + 350 + 360 \pmod{210}$

$= 836 \bmod 210$

$= 204 \bmod 210$

$\boxed{x = 206}$

Assignment 2: Implement any 2 classical encryption techniques using any programming language.

- Polyalphabetic Cipher:
- Transposition Cipher: (Classical)
- Row transposition cipher
- One time pads.
- Key range
- Brute force attack.

Types of Cryptanalytic Attacks:

Modern Block Cipher
↳ process plain text in terms of blocks/stream of bits.

- Feistel Cipher structure
- Substitution - Permutation Cipher (Shanon)

AES algorithm:

* Mix column transformation

① Substitute byte
② Shifting up the rows
③ Mixed Column transformation
④ Add Round key

$$\text{Row} = \begin{vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{vmatrix}$$

- At any point 128-bit input is present in AES

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

$$\begin{vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{vmatrix} * \begin{matrix} d4 \\ bf \\ 5d \\ 30 \end{matrix} = \begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix}$$

$r_0 = 02 * d4 + 03 * bf + 01 * 5d + 30 * 01$

$= 2 * 212$

Multiplication cases:

case 1 ⇒ 01 → 01 * XX = XX

case 2 ⇒ 02 → 02 * XX = 1 bit left shifting followed by conditional XOR with 1b, → 0001 1011

↳ if leftmost bit is 1 before leftshift

case 3 ⇒ 03 → 03 * XX

↳ 11 (binary)

↳ 10 XOR 01

∴ 03 * XX = {10 XOR 01} x {XX}

= 10 * XX XOR 01 * XX

02 * D4

r0) 1101 0100 → 1 1010 1000 ∵ Leftmost (MSB) is 1, XOR with 1b

left shifted bit ← left shift by 1

110 1000 XOR 1b

0001 1011

1101 0011

b3

$r_0 = b3$

r1) 03 * bF →

02 · BF XOR BF

1011 1111 → left shift → 0111 1110 XOR with 1B

01 11 11 1 0

00 01 10 1 1

01 1001 0 1 → 65

GS XOR BF

0110 0101
⊕ 1011 1111
1101 1010 → DA

γ_{02} = DA

γ_{03} = 01 * 5D = 5D

γ_{04} = 01 * 30 = 30

b3 ⊕ DA ⊕ 5D ⊕ 30

1011 0011
⊕ 1101 1010
⊕ 0101 1101
⊕ 0011 0000
0000 0100 → 04

∴ γ_0 = 04

γ_1 = 01 * d4 ⊕ 02 * b5 ⊕ 03 * 5D ⊕ 01 * 30

d4 ⊕ 02 * b5 ⊕ 03 * 5D ⊕ 30

02 * b5 = 1011 0101 → (left shift) LS → 65

02 * 5D ⊕ 5D = 01 01 11 01

1011 1010

LS 10 11 10 10 → ba

b a

⊕ 01 01 11 01

11 10 01 11

e 7 → e7

d4 ⊕ 65 ⊕ e7 ⊕ 30

11 01 01 00
01 10 01 01
11 10 01 11
00 11 00 00
0 1 1 0 0 1 1 0
6 6

γ_2 = 66

γ_3 = d4 ⊕ bf ⊕ 02 * 5D ⊕ 03 * 30

ba

01 01 11 01 → LS → 10 11 10 10 → ba

30 → 00 11 00 00 → LS → 01 10 00 00 ⊕

⊕ 00 11 00 00

01 01 00 00 → 50

$r_3 =$

```
  11  01  01  00
  10  11  11  11
  10  11  10  10
  01  01  00  00
-------------------
  10  00  00  01   → 81
-------------------
```

- DES Algorithm
- Stream Cipher
- RC4 owned by RSA (a proprietary cipher)
  - Key schedule
  - Stream generation
  - Security → secure against known attacks
- RC5 → world
  - Key expansion — $t = 2r + 2$
  - Encryption — $S[i], i = 0 \ldots t-1$ subkeys are stored
    - Rotation (left circular shift by 3 bits) is the main impacting factor on randomization.

RC4 example:

Assn : 2 Hill cipher encryption algo + 2 random classic

Lab Assignment:

Assn 3) Implement Simplified DES Algorithm.

RC4 Example: (Expected to Remember RC4 algorithm)

Instead of 256, we use 8×3 bits (for state vector)

S.: can be 0 ... 7

K = [1 2 3 6]

P = [1 2 2 2]

S = [0 1 2 3 4 5 6 7]

T = [1 2 3 6 1 2 3 6]

.
.
.
.
.

S = [2 3 7 4 6 0 1 5]