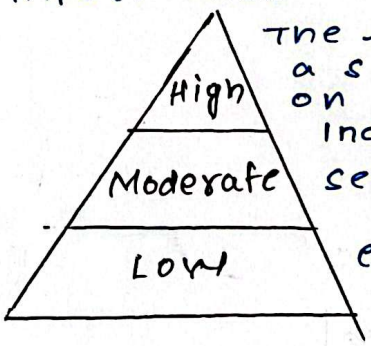
computer and Network security concepts

cryptographic Algorithms and protocols

- Symmetric Encryption
- Asymenetric Encryption
- Data-Integrity algorithms
- Authentication protocols

The field of network and Internet security consist of:-

measures to deter prevent, detect and correct security violations that involve the transmission of information



The loss could be expected to have a sever or catastrophic adverse effect on organizational operations, assets / individual

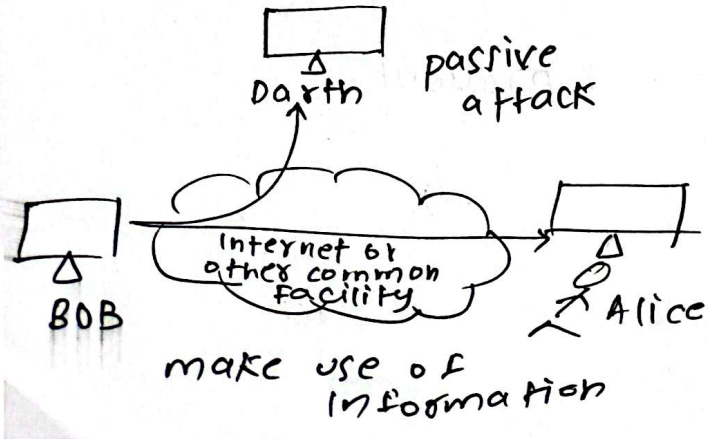
serious adverse effect " "

expected to have limited adverse "

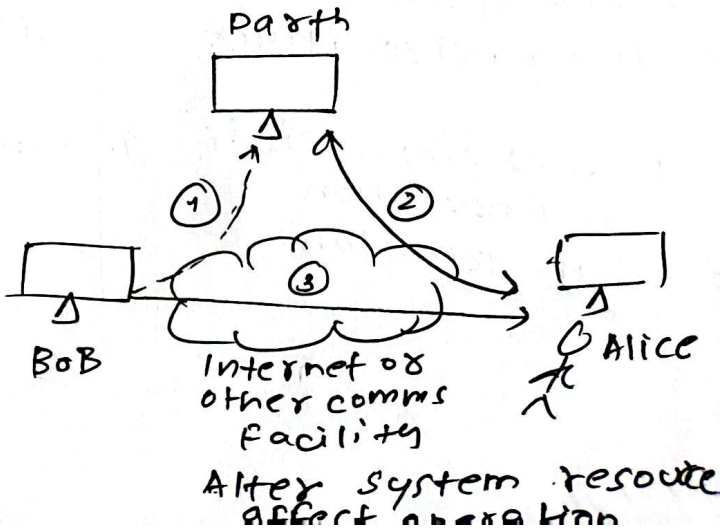
OSI security Architecture

- security attack
- security mechanism
- security service.

security Attacks



active attacks



passive Attacks

Are in the nature of eavesdropping on, or monitoring of transmissions.

Goal of opponent is to obtain information that is being transmitted.

- passive Attacks
  - Release of message contents
  - Traffic analysis

Active Attacks

- Masquerade
- Replay
- Modification of messages
- Denial of services

passive Attack	Attack Active
1. Hard to ~~deet~~ Detect	1. Hard to prevent
2. Nepther sender non receiver is aware of the attack	2. vulnerabilities include Physical, Software and network
3. Encryption prevents the passive attack	3 Detect and recover from any disruption or delays
4. More emphasis is on prevention than detection	4. Detect and prevent.

Security services

Defined by X.800 as

- A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

Defined by RFC 4949 as:

- A processing or communication service provided by a system to give a specific kind of protection to system resources.

Authentication

Concerned with assuring that a communication is authentic.

Two specific authentication services are defined in X.800

peer entity authentication:- implement same protocol in different systems.

Data origin authentication: Provides for corroboration of the source of a data unit.

Access control

The ability to limit and control the access to host systems and application via communication links

To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data confidentiality

The protection of transmitted data from passive attacks

- Broadcast service protects all user data transmitted between two users over a period of time.
- Narrow forms of service includes the protection of a single message or even specific fields within a message.

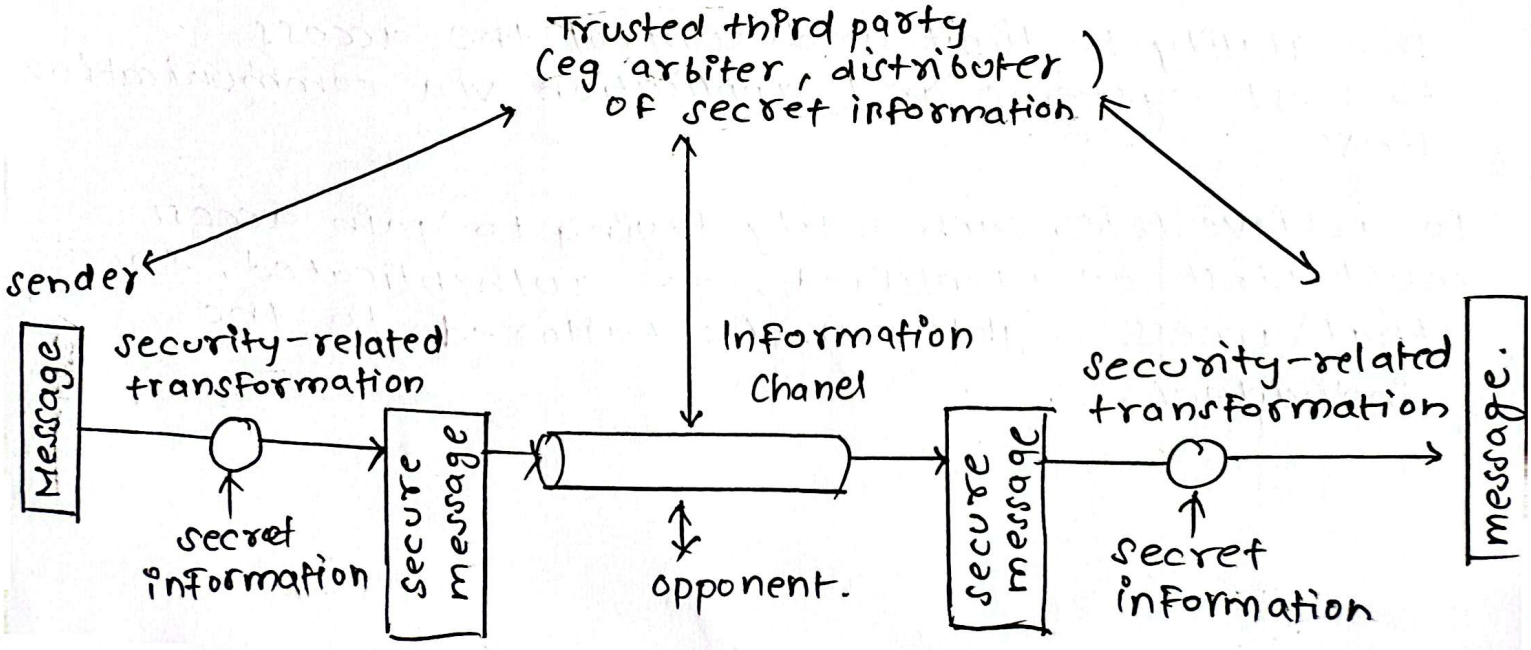
The protection of traffic flow from Analysis

This requires that an attacker not be able to observe the source and destination, frequency, length or other characteristics of traffic or communication facility.

Data - Integrity

connection-oriented integrity service, one that deals with a stream of messages are received as sent with no duplication, insertion, modification, recording, or delays.

Model for Network security



Cryptography

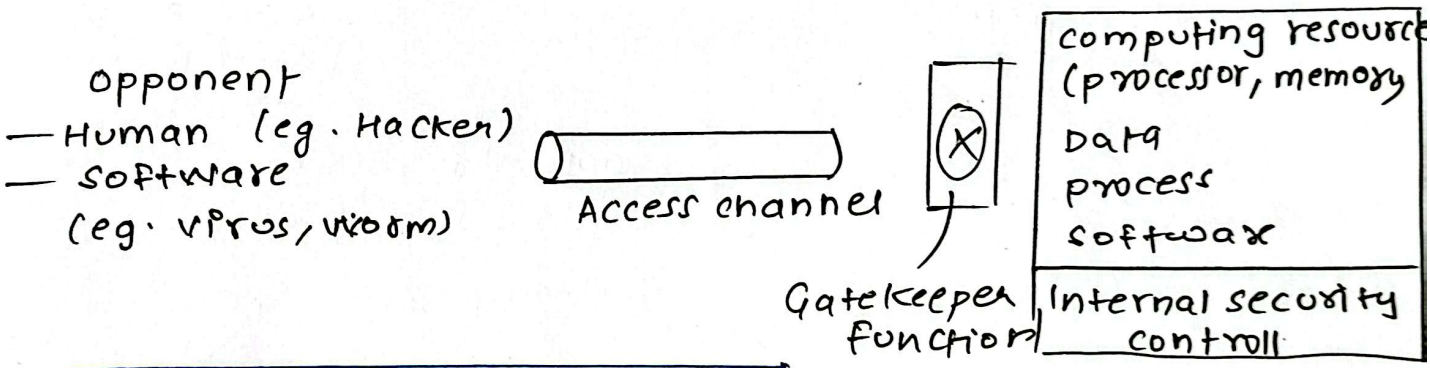
→ Cryptography is a Greek word which means "secret writing"

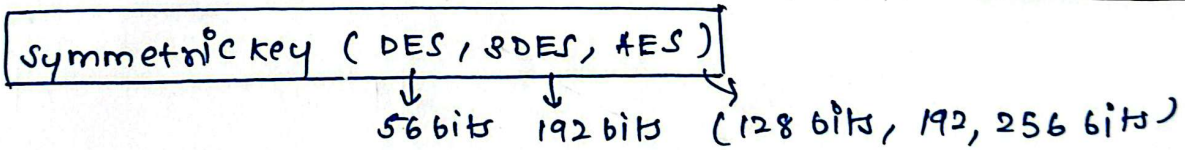
- Cryptography involves three different mechanisms

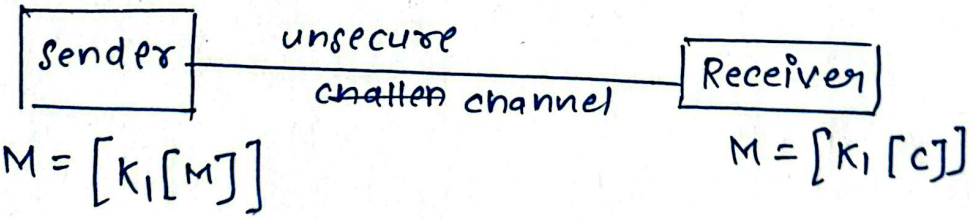
Symmetric key encipherment :- uses a single secret key for both encryption and decryption.

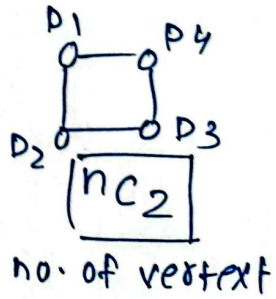
Asymmetric key encipherment : uses two keys like public key and private key to encrypt and decrypt.

Hashing :- A fixed length message is digest is created out of variable-length message.

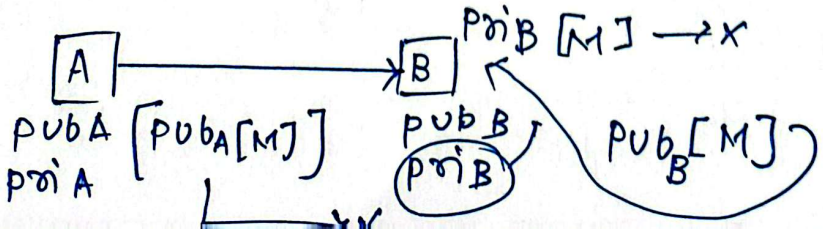








"Asymmetric key" OR Public key (RSA)



Receiver public key

Property

Commutative-Laws $(a+b) \bmod n = (b+a) \bmod n$
$(a \times b) \bmod n = (b \times a) \bmod n$

Associative-Laws $[(a+b)+c] \bmod n = [a+(b+c)] \bmod n$
$[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$

Distributive-Laws $[a \times (b+c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$

Identities $(0+a) \bmod n = a \bmod n$
$(1 \times a) \bmod n = a \bmod n$

Additive Inverse $a + (-a) \equiv 0 \bmod n$

Example 1.

Solve $23^3 \bmod 30$

$\Rightarrow -7^3 \bmod 30$

$= -7^2 \times -7 \bmod 30$

$= 49 \times -7 \bmod 30$

$= -133 \bmod 30$

$= -13 \bmod 30$

$= 17 \bmod 30$

$\boxed{23^3 \bmod 30 = 17}$

$31^{500} \bmod 30$

$1^{500} \bmod 30$

$1 \bmod 30$

$= 1$

$242^{329} \bmod 243$

$(-1)^{329} \bmod 243$

$(-1) \times -1^{328}$

$= -1 \bmod 243$

$= 242$

$11^7 \bmod 13$

$(2)^7 \bmod 13$

~~2×64~~

$2 \times 2^6 \bmod 13$

$256 \bmod 13$

$1 \mid 30$

~~$13 \bmod 12$~~

$13 \times 2 = 26$

30 | 23 (0), 0, 23, 30, -7

242, 243

133, 120, 013

11 | 13 (1), 11, 2

13 | 256 (12), 13, 026, 26, 0

Properties of Divisibility

if $a|1$ then $a \pm 1$

if $a|b$ and $b|a$ then $a = \pm b$

Any $b \neq 0$ divides 0

if $a|b$ and $b|c$ then $a|c$

$11|66$ and $66|198 = 11|198$

if $b|g$ and $b|h$ then $b(mg+nh)$ for arbitrary integers m and n.

GCD : Greatest common Divisor

Because we require that the greatest common divisor be provid

Modularity :

congurency: In cryptography congruence ($\equiv$) instead of equity

$15 = 3 \pmod{12}$

$23 = 11 \pmod{12}$

$$12 \overline{)\,15\,(\,1} \quad 12 \overline{)\,23\,(\,1}$$
$$\underline{12} \qquad\qquad \underline{12}$$
$$3 \qquad\qquad 11$$

$a \equiv b \pmod{m}$

i.e $a = km + b$

$$m \overline{)\,a\,(\,k} \qquad \text{i.e } a = mk + b$$
$$b$$

properties of Modular Arithematic

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

$11^{23} \bmod 187$

$11^1 \bmod 187 = -176$ OR 11

$11^2 = \bmod 187 =$

$(11)(11) \bmod 187$

$121 \bmod 187$

-66 OR 121

$11^4 = (-66)(-66) \bmod 187$

$4356 \bmod 187$

55 OR -132

$(55)(55) \bmod 187$

$3025 \bmod 187$

~~2838~~

33 OR -154

$33 \times 55 \times 55 \times 11 \times 11 \times 11 \bmod 187$

$132867075 \bmod 187 = 22$

$187 \times 1 = 3025 -$

$187 \times 2 = 4356 -$

$187 \times 16 = 2992 -$

$187 \times 4 = 748 -$

$187 \times 3 = 561 -$

$23^{16} \bmod 30$

$23^1 \bmod 30 = -7$ or 23

$23^2 \bmod 30 = (-7) \times (-7) \bmod 30$

$49 \bmod 30$

$= -19$ OR 11

$23^4 \bmod = (11) \times (11) \bmod 30$

$= 22 \bmod 30$

$= \cancel{-8 \text{ OR } 22}$

$(-8)(-8) \bmod 30$

$+64 \bmod 30$

4 OR -26

$(4) \quad -26 \times -26 \bmod 30$

$23^{16} \bmod 30 = \cancel{23^{8} \bmod 30}$

$4 \times 4 \bmod 30$

$16 \bmod 30$

$(-19)(-19) \bmod 30$

$361 \bmod 30$

1 OR -29

$1 \bmod 30$

$= 1$

$30 \overline{)23}$ (0) — $23 - 30 = -7$

$30 \overline{)49}$ (1) — $49 - 30 = -19$ or 11

$30 \overline{)64}$ (2) — $64 - 60 = 4$

$30 \overline{)16}$ (0) — $16 - 30 = -14$ or 16

$30 \overline{)361}$ (12) — $361 - 360 = 1$

solve $88^7 \bmod 187$ —(i)

$88^1 \bmod 187 = 88$

$187 \overline{)88}\ (0.47$

0

88

$187 \times 0 = 0$

$\therefore 88 - 0 = 88$

$\therefore 88 \bmod 187 = 88$

$88^2 \bmod 187$ —(ii)

$= 88^1 \times 88^1 \bmod 187$

$= 7744 \bmod 187 = 77$

$187 \overline{)7744}$

41×187

$7667 - 7744 = 77$

$88^4 \bmod 187$

$= 88^2 \times 88^2 \bmod 187$

$= 77 \times 77 = 5929 \bmod 187$

$31 \times 187 = 5797$

$88^4 \bmod 187 = 132$ —iii)

$88^1 + 88^2 + 88^4 = 88^7 \bmod 187$ iv

$\therefore 88 + 77 + 132 = 297$

$\therefore 88^7 \bmod 187 = 88^4 + 88^2 + 88^1 \bmod 187$

$= (132 \times 77 \times 88) \bmod 187$

$= 894,432 \bmod 187$

$88^7 \bmod 187 = 1$ ANS

Important Example :-

Q2) last two digits of 29^5 ?

$29^1 \bmod 100$

29

$3 \times 29 = 87$

$100 - 87 = 13$

$0 \times 100 = 0$

$29 - 0 = 29$

$29 \overline{)200}$

$100 \overline{)29}\ (0$

0

29

$29^2 \bmod 100 = 29^1 \times 29^1 \bmod 100$

$= 29 \times 29 = 841 \bmod 100 = 41$

$100 \overline{)}$

$29^4 \bmod 100 = 29^2 \times 29^2 \bmod 100 = 41 \times 41 = 1681 \bmod 100$

$= 81$

$29^5 \bmod 100 = 29^4 \times 29^1 \bmod 100$

$= -\cdot$

Another Method

What is "the last two digit" of 29^5

$\boxed{29^1 \bmod 100 = 29 \text{ or } -71}$

$29^2 \bmod 100 = 29 \times 29 \bmod 100$

$= 841 \bmod 100$

$= 41 \text{ or } -59$

$$\begin{array}{r} 0.1 \\ 100 \overline{)\ 29} \\ 0 \\ \hline 29 \\ 100 \\ \hline -71 \end{array} \qquad \begin{array}{r} 8 \\ 100 \overline{)\ 841} \end{array}$$

$29^5 \bmod 100 = 29^2 \times 29^2 \times 29^1 \bmod 100$

$\times -71$

$29^4 \bmod 100 = 41 \times 41 = 1681 \bmod 100 = 81 \text{ or } -19$

$29^4 \times 29^1 \bmod 100$

$= -19 \times 29 \bmod 100$

$= -551 \bmod 100$

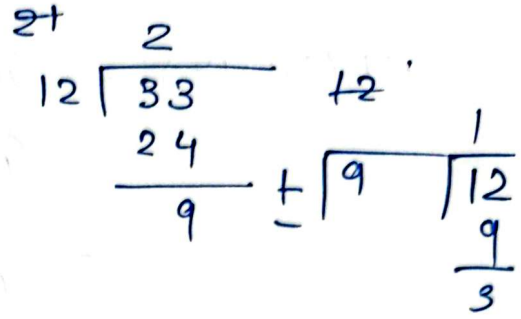
$= \underline{49}$

$$-551 \overline{)\ 100} \qquad \begin{array}{r} 5 \\ 100 \overline{)\ -551} \\ 500 \\ \hline 49 \end{array}$$

EUCLIDS ALGORITHM TO COMPUTE GCD

Q) Find the GCD(12, 33)

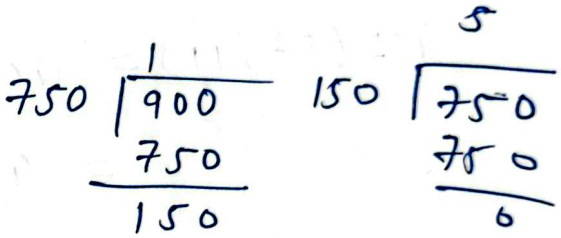
Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X



Ans GCD(12,33) = 3

Q2) Find the GCD(750, 900)

Q	A	B	R
1	900	750	150
5	750	150	0
0	150	0	0



GCD(750, 900) = 150 Ans

EUCID'S ALGORITHM METHOD-2 FOR FINDING GCD

pre-requists a > b

```
Euclid_GCD(a,b):
    if b = 0
        return a
    else
        return Euclid-GCD(b, a mod b);
```

Find GCD (50, 12)

Solution : GCD(a,b) = GCD (b, amod b)

GCD(50,12) = GCD (12, 50mod 12)

= GCD(12, 2)

= GCD (2, 12mod 2)

= GCD (2, 0)

GCD(50,12) = 2

Find GCD(83,19) = GCD (b, amodb)

GCD (83, 19) = GCD (19, 83mod 19) =

= GCD (19 , 7)

= GCD (7, 19mod 7)

GCD (7, 5)

= 5, 7mod5

= GCD(5, 2)

(2, 5mod2)

GCD(2,1)

1, 1mod2

GCD (1, 0) = 1

Relatively prime Numbers

Two numbers are said to be relatively prime, if they have no prime factors in common, and their only common factor is 1.

* GCD (a, b) = 1 then 'a' and 'b' are relatively prime numbers.
* co-prime.

Q) Find the GCD (790, 121) using GCD method 2 and determine whether they are relatively prime or not.

GCD (790, 121) = GCD (b, a mod b)

GCD (121, 790 mod 121)

GCD (121, 64)

GCD (64, 121 mod 64)

GCD (64, 57)

GCD (57, 64 mod 57)

GCD (57, 7)

GCD (7, 57 mod 7)

GCD (7, 1)

GCD (1, 7 mod 1)

GCD (1, 1)

= 1

Home-work (HW) Question

790 is a composite number and also 120 is a composite number BUT THEY ARE RELATIVELY PRIME NUMBERS

Euler's Totient Function

$\phi(n)$ = Number of positive integers less than "n" that are relatively prime to n

$\phi(5)$

$n = 5$ $\quad n < 5 : \{1, 2, 3, 4\}$

$\therefore \boxed{\phi(5) = 4}$

find $\phi(11)$

$n < 11 : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\therefore \boxed{\phi(11) = 10}$

find $\phi(8)$

$n < 8 : \{1, 2, 3, 4, 5, 6, 7\}$

$\boxed{\phi(8) = 4}$

$\phi(n)$	criteria of 'n'	Formula
	'n' is prime	$\phi(n) = (n-1)$
	$n = p \times q$ 'p' and 'q' are primes	$\phi(n) = (p-1) \times (q-1)$
	$n = a \times b$ Either 'a' or 'b' is composite Both 'a' and 'b' are composite	$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots$ p_1, p_2 are distinct primes

Example 2. find $\phi(31)$

Here $n = 31$

$\phi(n) = \phi(n-1)$ 'n' is prime

$\phi(n) = \phi(37-1) = 30$

∴ 30 Relatively Prime numbers in 31

Example 3 : find $\phi(35)$

Here $n = 35$

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

∴ $\phi(5 \times 7) = \phi((p-1) \times (q-1))$

$= \phi((5-1) \times (7-1))$

$\phi(4 \times 6) = 24$

24 +ve no. Relatively prime numbers in 35

Example 4 :- Find $\phi(1000)$

$\phi(n) = \phi(1000)$

$\phi(n) = \phi(2^3 \times 5^3)$

distinct prime factors are 2 and 5

$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots$

$= 1000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$1000 \times \left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 1000 \times \frac{4}{10}$

$\boxed{\phi(n) = 400}$

Home-work

$\phi(372)$

$31 \times 3 \times 2 \times 2$

$\phi(31 \times 12)$

$\phi(31 \times 3 \times 2^2)$

all are prime

2	372
2	186
2	93
3	31

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)$$

$$372\left(1-\frac{1}{31}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right)$$

$$372\left(\frac{30}{31}\right)\left(\frac{2}{3}\right)\left(\frac{1}{2}\right)$$

$$372 \times \frac{60}{186}$$

$2 \times 60 = 120$

Ans

$\boxed{\phi(n) = 120}$

Fermat's Little Theorem

If 'p' is a prime number and 'a' is a +ve integer not divisible by (p) then

$$a^{p-1} = 1 \pmod{p}$$

$p = 6$ and $a = 2$

$a^{p-1} = 1 \bmod p$

$a^{6-1} = 1 \bmod 6$

$2^5 = 1 \bmod 6$

$32 \not\equiv 1 \bmod 6$

No.

Eulers Theorem

For every +ve integer 'a' and n which are said to be relatively prime then

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

$a = 3 \quad n = 10$ prove Eulers theorem hold true for

solution $a = 3, n = 10$

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

$\phi(n) = 10$

$\phi(n) = 2 \times 5 = (2-1)(5-1)$

$= 1 \times 4$

$\phi(n) = 4$

$3^4 = 1 \bmod 10$

$3 \times 3 \times 3 \times 3$ $\quad 81 \bmod$

$81 \equiv 1 \bmod 10$ ✓ for a, n

Does Fermat's theorem hold true for $p=5$ and $a=2$

Given $P=5$ and $a=2$

$$a^{P-1} = 1 \pmod P$$

~~a^{5-1}~~

$$2^{5-1} \equiv 1 \pmod 5$$

$$2^4 \equiv 1 \pmod 5$$

$$\boxed{16 \equiv 1 \bmod 5}$$

Therefore fermat's theorem hold true ~~if~~ a,p

prove $p=13$ $a=11$

$$a^{p-1} = 1 \pmod p$$

$$11^{13-1} = 1 \pmod{13}$$

$$11^{12} = 1 \bmod 13$$

$$(-2)^{12} = 1 \bmod 13$$

$$(-2)^{4\times 3} = 1 \bmod 13$$

$$(3)^3 = 1 \bmod 13$$

$$\boxed{27 = 1 \pmod{13}}$$

Yes it apply fermat theorem

Example 2 : Does Euler's theorem hold true for $a=2 \quad n=10$

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

$$\phi(n) = \phi(10) = 4$$

$$2^4 = 1 \bmod 10$$

$$\underbrace{2 \times 2 \times 2 \times 2}$$

$16 \neq 1 \bmod 10$ not ~~✓~~ for $a=2, n=10$

Q2) check for $a=10 \quad n=11$

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

$$\phi(n) = \phi(11) = \phi(11-1) = 10$$

$$10^{10} = 1 \bmod 11$$

$$(-1)^{10} = 1 \bmod 11$$

~~$1 \neq 1 \bmod 11$~~

$1 \equiv 1 \bmod 11$ ~~✓~~ for $a=10, n=11$

Primitive Root

A number 'α' is a primitive Root modulo n if every number coprime to n is congruent to a power of 'α' modulo n

'α' is said to be primitive root of prime number 'p' if $\alpha \bmod p$ $\alpha^2 \bmod p$, $\alpha^3 \bmod p$ .. α^{p-1} are distinct

Q Is 2 a primitive root of prime number 5.

$2^1 \bmod 5$	$2 \bmod 5$	2	✓
$2^2 \bmod 5$	$4 \bmod 5$	4	✓
$2^3 \bmod 5$	$8 \bmod 5$	3	✓
$2^4 \bmod 5$	$16 \bmod 5$	1	✓

$$5 \overline{)16}\ 3,\ 15,\ 1$$

$n < 5 = \{1, 2, 3, 4\}$

Yes 2 is a primitive root of prime no. 5

Q) Is 3 a primitive Root of prime no. 7

$3^1 \bmod 7$	$3 \bmod 7$
$3^2 \bmod 7$	$9 \bmod 7$
$3^3 \bmod 7$	$27 \bmod 7$
$3^4 \bmod 7$	$81 \bmod 7$
$3^5 \bmod 7$	$243 \bmod 7$
$3^6 \bmod 7$	$729 \bmod 7$

3, 2, 6, 4, 5, 1 ✓

$n < 7 = \{1, 2, 3, 4, 5, 6\}$

Yes 3 is A primitive Root of 7

Multiplicative - Inverse

under mod n

$A \times A^{-1} \equiv 1 \bmod n$

$3 \times ? \equiv 1 \bmod 5$

$3 \times 2 \equiv 1 \bmod 5$

? = 2 is a multiplicative inverse under mod 5

$2 \times ? = 1 \bmod 11$

$2 \times 6 \equiv 1 \bmod 11$

$12 \equiv 1 \bmod 11$

6 is a multiplicative inverse under mod 6

Finding Multiplicative Inverse using Extended - Euclidian Algorithm

Q	A	B	T_1	T_2	T
			11		

A > B

Q

B | A

R

$T_1 = 0 \quad T_2 = 1$

For first column

$T = T_1 - T_2 \times Q$

T_1 is the multiplicative inverse

What is MI of 3 mod 5

A > B

Q	A	B	R	T1	T2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	2	-5	X

$$3 \overline{)5}\ 1 \quad 3 \quad 2$$

$T = (T_1 - T_2) \times Q$

$(0-9)\times 1$

-1

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

$(1-(-1)\times 1$

$= 2 \times 1$

$T = 2$

MI of 3 mod 5 is 2

$-1-2$

$-3x$

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

$-1-4$

$-1-2$

$= -3x$

Note that GCD(A,B) A,B should be Relatively Prime

The Chinese Remainder Theorem

The Chinese Remainder theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown :

$$X \equiv a_1 \pmod{m_1}$$
$$X = a_2 \pmod{m_2}$$
$$\vdots$$
$$X = a_n \pmod{m_n}$$

CRT states that the above equations have a unique solution of the moduli are relatively prime

$$X = (a_1 MM^{-1} + a_2 MM^{-1} + \dots + a M_n M_n^{-1}) \bmod M$$

solve using CRT

$$X = 2 \pmod 3$$
$$X = 3 \pmod 5$$
$$X = 2 \pmod 7$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

Given		To Find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	M
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

$$M = m_1 \times m_2 \times m_3$$
$$M = 3 \times 5 \times 7$$
$$\boxed{M = 105}$$

$M_1 = \frac{M}{m_1}$ $M_2 = \frac{M}{m_2}$ $M_3 = \frac{M}{m_3}$

$M_1 = \frac{105}{3} = 35$ $M_2 = \frac{105}{5} = 21$ $M_3 = \frac{105}{15} = 15$

finding inverse

$M \times M_1^{-1} \equiv 1 \bmod m_1$

$35 \times M_1^{-1} \equiv 1 \bmod 3$

$35 \times 2 \equiv 1 \bmod 3$

$\boxed{M_1^{-1} = 2}$

$M \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} \equiv 1 \bmod 5$

$\boxed{M_2^{-1} = 1}$

$M \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

$15 \times 1 = 1 \bmod 7$

$\boxed{M_3^{-1} = 1}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M M_3^{-1}) \bmod M$

$(2 \times 2 \times 35 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod (105)$

$X = 233 \bmod 105$

$\boxed{X = 23}$

The Chinese Remainder Theorem

Solve the following equations using CRT

$4x = 5 \pmod 9$

$2x = 6 \pmod{20}$

$4x = 5 \pmod 9$

$4^{-1} \times 4x = 4^{-1} \times 5 \pmod 9$

$x = 4^{-1} \times 5 \pmod 9$

$= 4^{-1} \pmod 9 \times 5 \pmod 9$

$= 7 \pmod 9 \times 5 \pmod 9$

$7 \times 5 \pmod 9$

$x = 35 \bmod 9$

$x = 8 \bmod 9$

$9 \overline{)35}\ 3$, 27

$2x = 6 \pmod{20}$

$2x \times 2^{-1} = 2^{-1} \times 6 \pmod{20}$

$x = 2^{-1} \pmod{20} \times 6 \pmod{20}$

6 R

$x = \frac{2x}{2} = \frac{6 \pmod{20}}{2}$

$x = 3 \bmod 20$

$x = 8 \bmod 9$

~~$m_1 = 8$~~ Given

$a_1 = 8$	$m_1 = 9$	To Find	
$a_2 = 3$	$m_2 = 20$	M_1 M_1^{-1}	$M = 180$
		M_2 M_2^{-1}	

$M = m_1 \times m_2 = 9 \times 20 = 180$

$M_1 = \frac{M}{m_1} = \frac{180}{9} = 20$ $\quad M_1^{-1}$

$M_2 = \frac{M}{m_2} = \frac{189}{20} = 9$

finding inverse

$M_1 M_1^{-1} = 1 \bmod m_1$

~~180~~ $M_1^{-1} = 1 \bmod 9$

$20\ M_1^{-1} = 1 \bmod 9$

$\boxed{M_1^{-1} = 5}$

$M_2 M_2^{-1} = 1 \bmod m_2$

$9 \times M_2^{-1} = 1 \bmod 20$

$9 \times 9 = 1 \bmod 20$

$\boxed{M_2^{-1} = 9}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$X = (8 \times 20 \times 5 + 3 \times 9 \times 9) \bmod 180$

$X = (800 + 243) \bmod 180$

$X = 1043 \bmod 180$

$\boxed{X = 143}$ Ans

Homework Question

solve the following using CRT

$X = 5 \pmod 3$ —(i)

$X = 2 \pmod 5$ —(ii)

$X = 1 \pmod{11}$ —(iii)

$a_1 = 5 \quad a_2 = 2 \quad a_3 = 1$

$\boxed{m_1 = 3 \quad m_2 = 5 \quad m_3 = 11}$

$M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 11$

$= 15 \times 11$

$\boxed{M = 165}$

$M_1 = \frac{M}{m_1} = \frac{165}{3} = 55$

$M_2 = \frac{M}{m_2} = \frac{165}{5} = 33$

$M_3 = \frac{M}{M_3} = \frac{165}{11} = 15$

$M_1 M_1^{-1} = 1 \bmod m_1$

$55\ M_1^{-1} = 1 \bmod 3$

$55 \times 4 = 1 \bmod 3$

$\boxed{M_1^{-1} = 4}$

$55 \times 4 + 3$

3 | 220

3 | 214

1

$M_2 M_2^{-1} \equiv 1 \bmod m_2$

$33 \times M_2^{-1} \equiv 1 \bmod 5$

$33 \times M_2^{-1} \equiv 1 \bmod 5$

$33 \times 2 \equiv 1 \bmod 5$

$66 \equiv 1 \bmod 5$

$M_2^{-1} = 2$

$M_3 M_3^{-1} \equiv 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 11$

$15 \times 3 = 1 \bmod 11$

$M_3^{-1} = 3$

$$\therefore x = \sum_{i=0}^{n} M_i M_i^{-1} a_i$$

$$x = [(55 \times 4 \times 5) + (33 \times 3 \times 2) + (1 \times 3 \times 15)] \bmod M$$

$$= (1100 + 198 + 45) \bmod 165$$

$$x = (1343) \bmod 165$$

~~23 mod~~

$x = 23$

Chapter 3: SYMMETRIC CIPHERS

Classical Encryption Techniques

1.1

- Substitution Technique
- Transposition Techniques

Example 1.1

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

a → M
b → X
X → Z
g → A

Plaintext: bag

Ciphertext: XMA

Transposition Technique

Example: NESO

Ciphertext: ESON, SONE, ONES, ENOS

Applying some sort of permutation on the plaintext letters.

classical Encryption Techniques

- Substitution
  1. caesar cipher
  2. Monoalphabetic cipher
  3. playfair cipher
  4. Hill cipher
  5. polyalphabetic cipher
  6. One-Time Pad
- Transposition
  1. Rail Fence
  2. Row Column Transposition.

Caesar cipher

Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Algorithm:

for each plaintext letter 'p' substitute the ciphertext letter 'c'

$$c = E(p, K) \bmod 26 = (p + K) \bmod 26$$

$$p = D(c, K) \bmod 26 = (c - K) \bmod 26$$

P : Plaintext
K : key
E : Encryption
D : Decryption
C : cipher text

0	1	2	3	4	5	6	7	8	9	10
A	B	C	D	E	F	G	H	I	J	K
11	12	13	14	15	16	17	18	19	20	21
L	M	N	O	P	Q	R	S	T	U	V
22	23	24	25							
W	X	Y	Z							

Q: ENCRYPT "NESO ACADEMY"

n	e	s	o	a	c	a	d	e	m	y	→ plain text
Q	H	V	R	D	F	D	G	H	P	B	→ cipher text

$$c = (p + K) \bmod 26$$

$$c = (13 + 3) \bmod 26$$

$$c = 16 \bmod 26$$

$$26 \overline{)\,16\,}\ 0$$

$$16$$

$c = 16$ Refer mapped

SHIFT CIPHER

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

key = 2, 3, 4, 5 - - -

A ceaser cipher is a special case of shift cipher

So ∴ A shift cipher with key = 3 is called a ceaser cipher

plain text : MANIPAL

KEY : 4

Cipher text : QEQMTMP — shift cipher with key = 4

caesar cipher :- pros and cons

Pros

1) Easy to implement
2) simple

Cons

1) The encryption and decryption algorithms are known
2) There are only 25 keys to try
3) The language of plaintext is known and easily recognizable.

BRUTE FORCE ATTACK

Brute force attack is a method where we Attempt all 25 possibilities of key's and shift until we get a Reodable text

SHIFT TABLE	SHIFT
	[25]
	[24]
	[23]

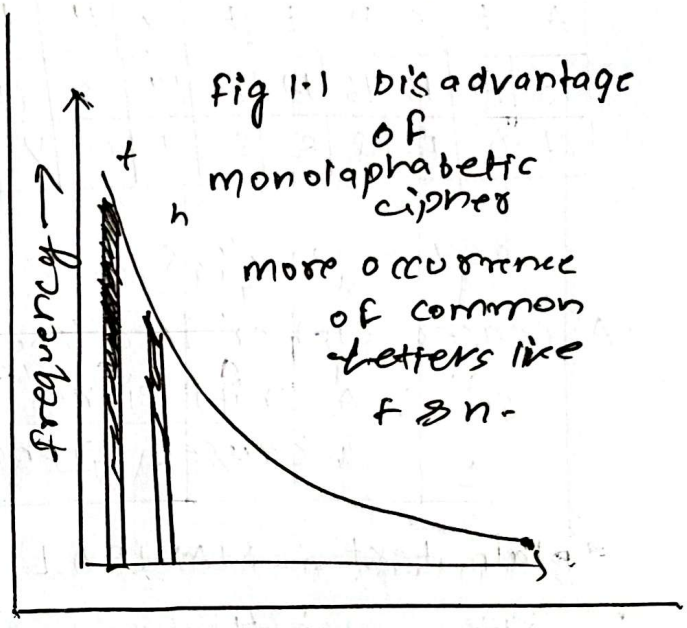


fig 1.1 Disadvantage of monoalphabetic cipher

more occurrence of common letters like t & h.

MONO-ALPHABETIC CIPHERS

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Example:- plain text — NESO } RANDOM MAPPED KEY

cipher text — DULA

4! possiblity for mapping key

ADVANTAGES

1. Better security than caesar cipher

Disadvantages

1. Monoalphabetic ciphers are easy to break because they reflect data of original alphabet
2. prone to guessing attack using English letter frequency of occurrence.

ceasey cipher (+3)

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
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

monoalphabetic cipher

$S = \{a, b, c\}$

{abc, bca, cab, bac, acb, cba}

Manipal

~~flag - fair~~ **PLAY - FAIR CIPHER**

5x5 word matrix

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

mo	sq	ue
ON	TS	ML

ONTSML → play fair cipher text

Note: key word is MONARCHY

Ex. attack

pt
ct

at	ta	ck	
RS	SR	DE	

Example

AT	TA	CK	– plain text
RS	SR	DE	– play fair cipher text

play fair

1) Diagram letter
2) Repeating letter - filling letter
3) same column (↓) wrap
4) same row (→) wrap
5) Rectangle (⇄) swap.

Homework problem (HW)

Decrypt the ciphertext "ODZFQSE2SONTSW" using playfair technique with the key word "Neso App"

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

← 5x5 key matrix →

OD ZF QS E2 SO NT SW

Hill cipher.

Multi-letter cipher

Developed by Lester Hill in 1929

Encrypts a group of letters: Digraph, Trigraph or polygraph.

The Hill Algorithm

$$C = E(K, P) = P \times K \bmod 26$$

$$P = D(K, C) = CK^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$$

$$(C_1 C_2 C_3) = (P_1 P_2 P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

Encryption

$$C_1 = (P_1 K_{11} + P_2 K_{21} + P_3 K_{31}) \bmod 26$$
$$C_2 = (P_1 K_{12} + P_2 K_{22} + P_3 K_{32}) \bmod 26$$
$$C_3 = (P_1 K_{13} + P_2 K_{23} + P_3 K_{33}) \bmod 26$$

Question :- Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution

plain text

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24
R	R	L	M	W	B	K	A	S	P	D	H

cipher text

key = 3 x 3 matrix

PT = pay mor emo ney

Encrypting : pay

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (15\ 0\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$(C_1\ C_2\ C_3) = (15 \times 17 + 0 \times 21 + 24 \times 2), (15 \times 17, 18 \times 0, 24 \times 2), (\sout{5 \times 24, 24 \times 2}\ (15 \times 5 + 0 \times 21 + 24 \times 19) \bmod 26$

$= (303\ 303\ 531) \bmod 26$

$= \begin{pmatrix} 17 & 17 & 11 \\ R & R & L \end{pmatrix}$

↓ continue

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{vmatrix}$$

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \\ 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{vmatrix} \quad \begin{bmatrix} 18 \times 19 - 21 \times 2 & - & - \\ | & & \\ | & & \end{bmatrix}$$

$$K^{-1} = \frac{1}{\det K} \times \text{Adj } K$$

$$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = 23^{-1} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

$$\boxed{K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}}$$

To find the determinant of $K \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

$$\text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= 17(18\times19 - 2\times21) - 17(19\times21 - 2\times21) + 5(21\times2 - 2\times18) \bmod 26$$

$$= 17(342 - 42) - 17(399 - 42) + 5(42 - 36) \bmod 26$$

$$= 17(300) - 17(357) + 5(6) \bmod 26$$

$$= 5100 - 6069 + 30 \bmod 26$$

$$-939 \bmod 26$$

$$-3 \bmod 26$$

$$= 23$$

Decryption requires K^{-1}, the inverse matrix K

$$\boxed{K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K}$$

$$P = D(K, C) = CK^{-1} \bmod 26$$

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \begin{matrix} 17 & 17 \\ 21 & 18 \\ 2 & 2 \end{matrix}$$

polyalphabetic cipher

Vigenere cipher: It consists of the 26 caesar cipher with shifts of 0 through 25

Encryption process:-

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

Decryption process:-

$$P_i = (C_i - K_i \bmod m) \bmod 26$$

Key : deceptive deceptive deceptive

Plain text : wearediscoveredsaveyourself

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2	21	19	22	12	13	6	17	25	6	21

$C_i = (P_i + K_i \bmod m) \bmod 26$

$(3 + 22) \bmod 26$

$= 25 \bmod 26 = 25$

$C_i = (4 + 4) \bmod 26$

$8 \bmod 26$

$= 8$

$(2 + 0) \bmod 26$

$2 \bmod 26$

$= 2$

Auto-key-system

The periodic nature of the keyword can be elpminated by using a non-repeating keyword that is as long as the message itself.

Vigenére proposed autokey system in which a keyword is concatenated with plaintext itself to provide a running key.

Example:-

Key : deceptivewearediscoveredsav

Plain text : wearediscoveredsaveyourself

Classical Encryption Techniques

TRANSPOSITION TECHNIQUE

Rail Fence Technique.

Rail Fence Technique: The plaintext is written down as a sequence of diagonals and then read off as a sequence of Rows.

Example:- Encipher the message "neso academy is the best" with a rail fence of depth 2

n		s		a		a		e		y		s		h
	e		o		c		d		m		i		t	

	b		s	
e		e		t

NSAAEYSHBSEOCDMITEET → cipher text

Ans

Homework:- neso academy is the best

Depth :- 3

n				a				e				s				b	
	e		o		c		d		m		i		t		e		e
		s				a				y				h			

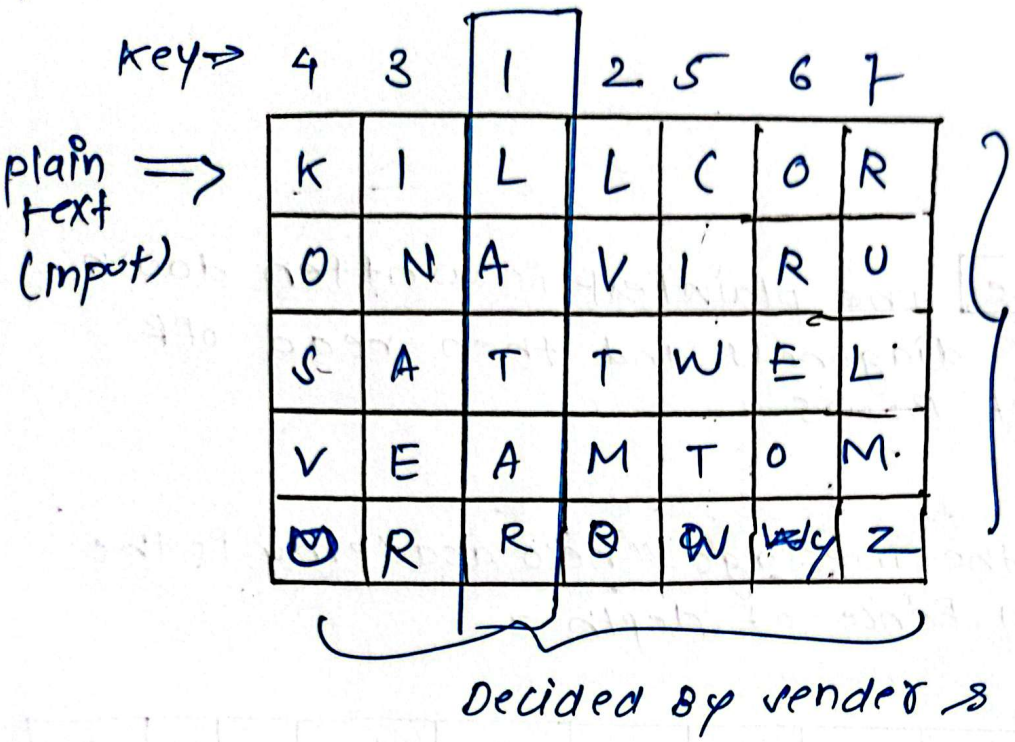
t

Cipher-text → NAESBEO CDMITEESAYHT

HW question solved

Row column Transposition

Plaintext: "KILL CORONA VIRUS AT TWELVE AM TOMORROW



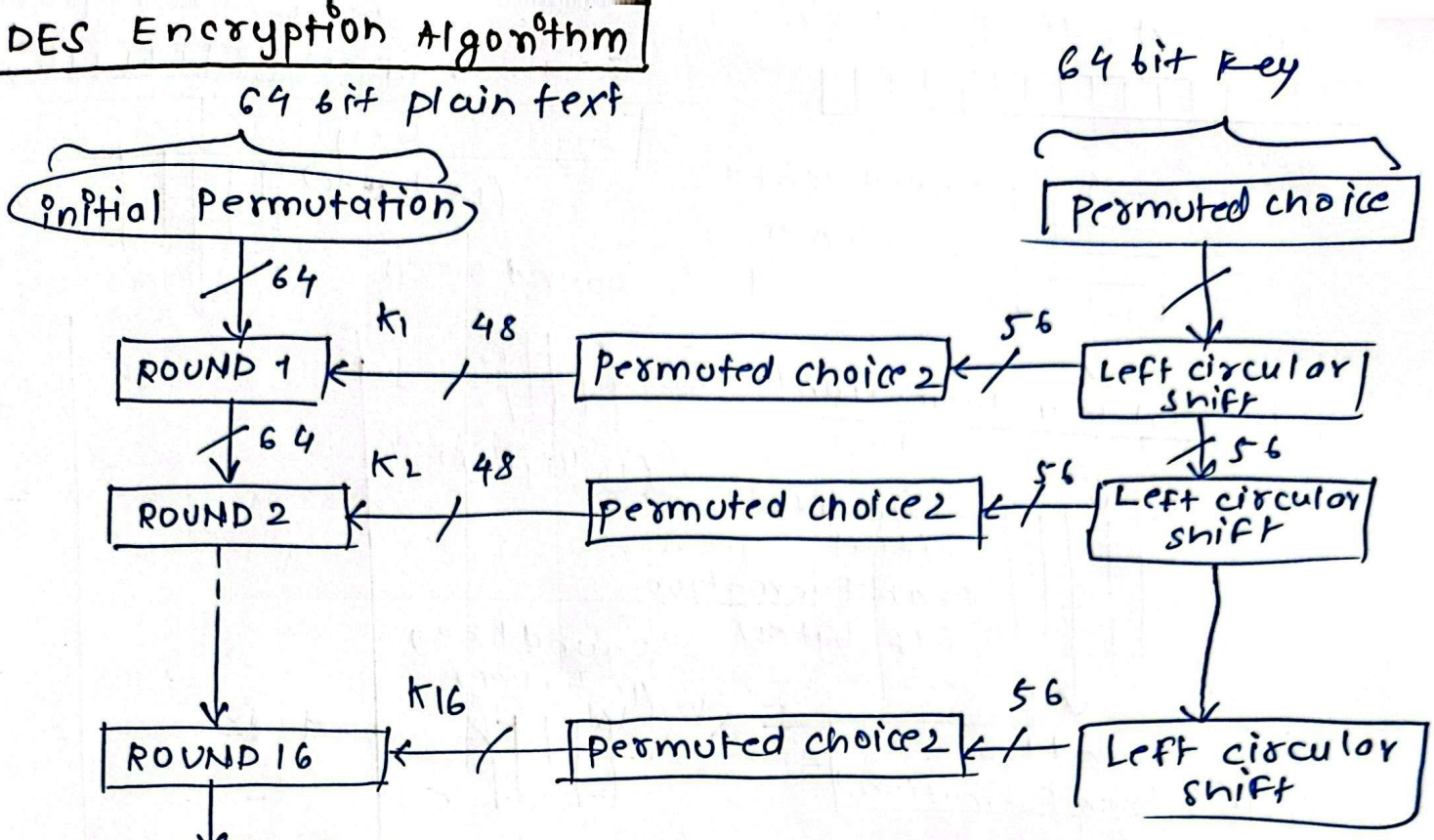
Decided by sender & Reciever

LATAR LVTMO INAER KOSVO CIWTW OREOY

RULMZ ↓

Ciphertext

DES Encryption Algorithm



1) Apply permutation
split IP(P) into two 32 bit L_0 and R_0

2) Bit parity drop

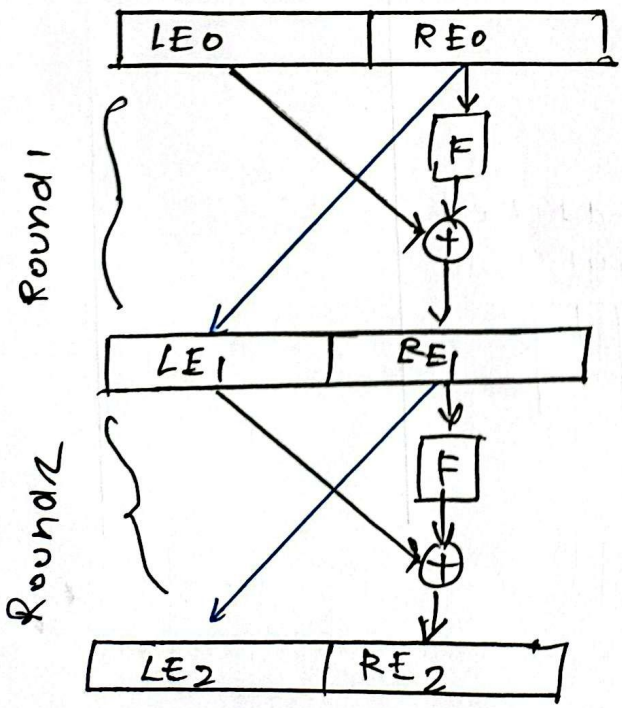
16 Rounds of feistel fn

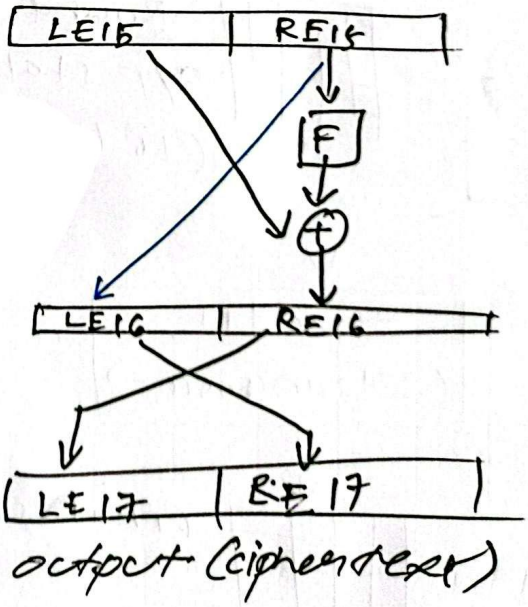
$L_i = R_{i-1}$

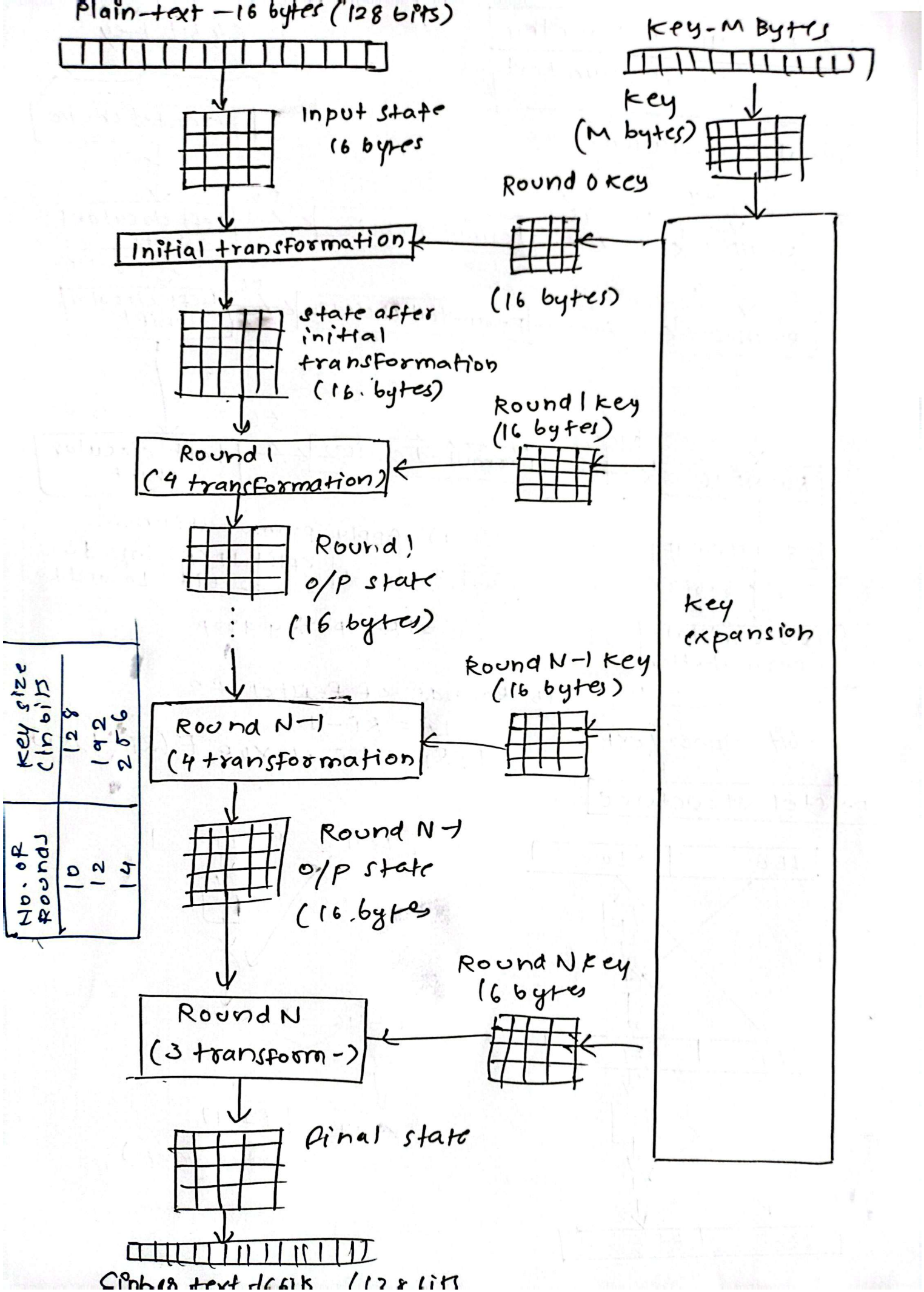
$R_i = L_{i-1}$ XOR $F(R_{i-1}, K_i)$

:

Feistel structure






Plain-text – 16 bytes (128 bits)
Key - M Bytes
Input state
16 bytes
Key
(M bytes)
Round 0 key
Initial transformation
(16 bytes)
state after
initial
transformation
(16 bytes)
Round 1 key
(16 bytes)
Round 1
(4 transformation)
Round 1
o/p state
(16 bytes)
key
expansion
Round N-1 key
(16 bytes)
Round N-1
(4 transformation
Round N-1
o/p state
(16 bytes
Round N key
16 bytes
Round N
(3 transform-)
Final state
Key size (in bits)
128
192
256
No. of Rounds
10
12
14