

UNIT-I

①

INTRODUCTION & NUMBER THEORY :-

Introduction - ②
Services - ⑦

Mechanisms - ⑧

Attacks - ④

OSI security architecture - ③

Network security model - ⑨

classical Encryption techniques - ⑪

> Symmetric cipher model - ⑪

> Substitution techniques - ⑯

> Transposition techniques - ⑯

> Steganograph - ⑯

Finite fields and Number theory - ⑯

Groups - ⑯

Rings - ⑯

Fields - ⑯

modular arithmetic - ⑯

Euclid's algorithm - ⑯

Finite fields - ⑯

Polynomial Arithmetic - ⑯

Prime numbers - ⑯

Fermat's & Euler's theorem - ⑯

Testing for primality - ⑯

The Chinese remainder theorem - ⑯

Basic terminology:Cryptology :-

* Cryptology is the study of techniques for ensuring secrecy & authentication of information.

> Cryptography - Study of design of techniques.

> Crypt analysis - This deals with the concept of defeating cryptography.

Network security :-

It covers the use of cryptographic algorithms in network protocols and it applies.

* Computer security: Refers to the security of computers against intruders & malicious software.

Information security:-

Information needs to be secured. The security of info needs to be against physical damage & administrative damage.

*. Computer Security :-

*. It is the collection of tools to protect data & thwart hacker is called computer security.

*. Network Security :-

Used to protect the data during the transmission across the n/w.

*. Internet Security :-

Security against the data when it transmitted across the In.

*. OSI Security Architecture :-

*. OSI architecture provides a way to organize the security.

> Security Attack

> Security Mechanism

> Security Service

Threat:- It is a possible danger that exploit vulnerability.

Attack:- It is an intelligent act (eff) deliberate to evade security & violate the security policy of a system.

* Security Attack :- (A)

* Attack is defined as an action that compromises the security of info. owned by the org.

* It can be classified as,

> passive attack

> Active attack

* Passive attack :-

* The opponent wants to obtain the info (i) being transmitted across the net & involves no alteration.

Characteristics :-

> Difficult to detect

> Possible to prevent by encryption.

Classification :-

* Release of message contents

* The msg to be transmitted

should be prevented from eaves-dropping.

> Traffic Analysis

* Here, the intruder watches

the frequency, length of msg exchanged
b/w the two principals.

* Active Attacks :-

* Involves alteration to the

Characteristics :-

(5)

- > Difficult to prevent.
- > Detection is feasible & can be recovered from the causes.

Classification :-

> Masquerade

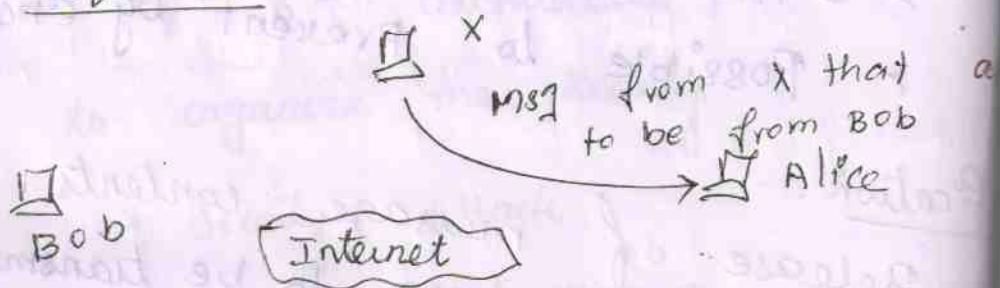
> Replay

> Modification of msgs

> Denial of service

> D/W attack.

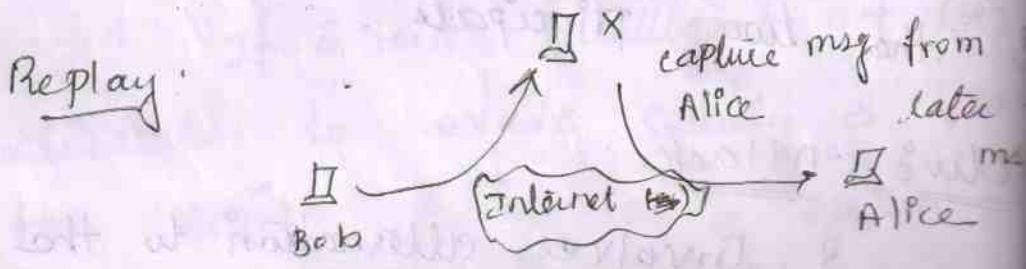
* Masquerade :-



*. when one entity pretends to be a different entity.

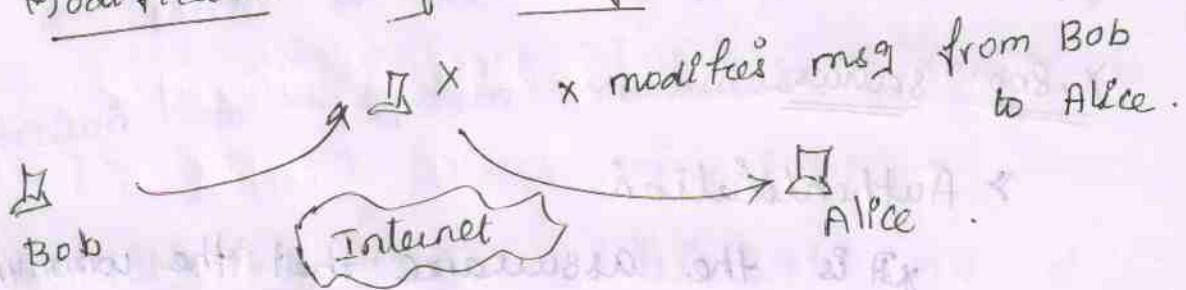
*. the attacker captures the message & impersonifies the sender.

* Replay :-



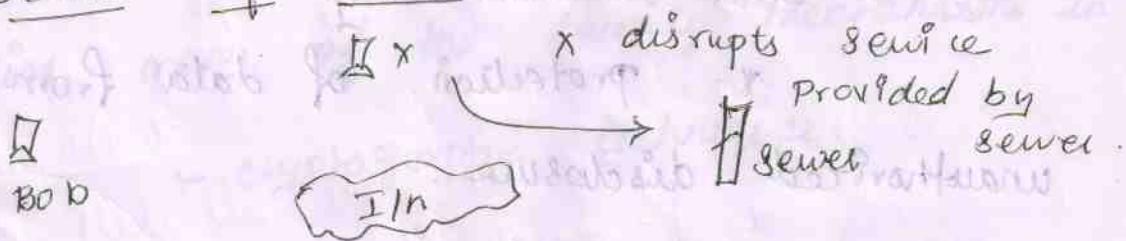
* The attacker captures the msg & retransmits the msg without any modification to produce unauthorized effect. (6)

* Modification of messages :-



* The attacker captures the msg & retransmits the msg with modification (or) delays (or) reorders the msg to produce unauthorized effect.

* Denial of service :-



Attack has specific target like suppress all the msgs directed to a user (or) disable the n/w, degrade the performance.

* Slow Attack :-

* Slow attacks are those which can be introduced into the systems (or) n/w's.

Ex: worms, viruses.

Security Services :-

* Security service is a service provided by the protocol layer, which ensures security of the systems for data transfer.

X.800 Services :-

> Authentication

* It is the assurance that the communicating entity is the one that it claims to be.
↳ Access control

* the access control is the protection of unauthorized use of a resource.

> Data confidentiality

* protection of data from unauthorized disclosure.

> Data Integrity

* This gives the assurance that data received are not modified / replicated / deleted / updated.

> Non-Repudiation

* This provides the protection against the denial by one of the principals involving in the communication.

A vailability

(8)

- * Resource accessible / usable.

RFC 2828:-

- * A Processing (or) comm Service provided by a system to give a specific kind of protection to system resources.

Security Mechanism:-

- * Feature designed to detect, prevent (or) recover from a security attack.
- * No single mechanism that will support all services required.
- * however one particular element underlies many of the security mechanisms in use.
 - cryptographic techniques.

X.800:-

- > specific security mechanisms
- > very pervasive " "

Specific Security mechanisms:-

- * May be incorporated into the appropriate protocol layer in-order to provide some of the OSI security services.

> Encipherment

> Authentication

> Digital signature

> Traffic padding

> Access ctrl

> Routing ctrl

> Data integrity

> Notarization

* Pervasive Security Mechanism:-

* Mechanisms that are not specific

to any particular OSI security service

(or) protocol layer.

> Trusted functionality

> Security label

> Event Detection

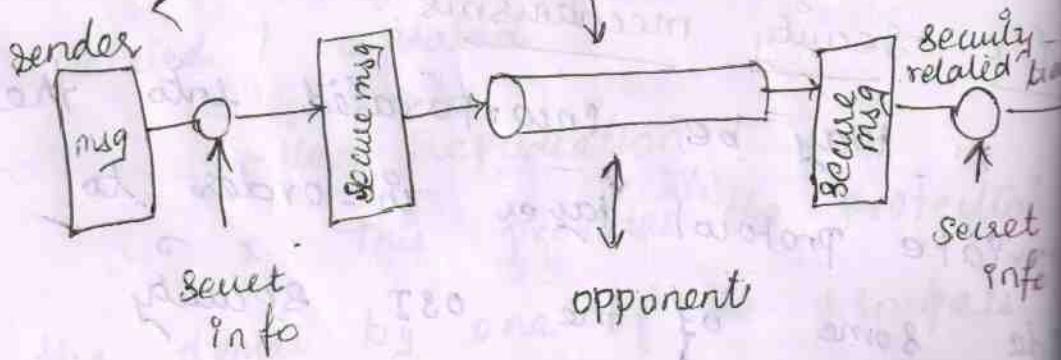
> Security Audit trail

> Security Recovery.

Network Security Model :-

Trusted 3rd party

[ex: Arbiters, distributor, of secret info]



Model for new security:-

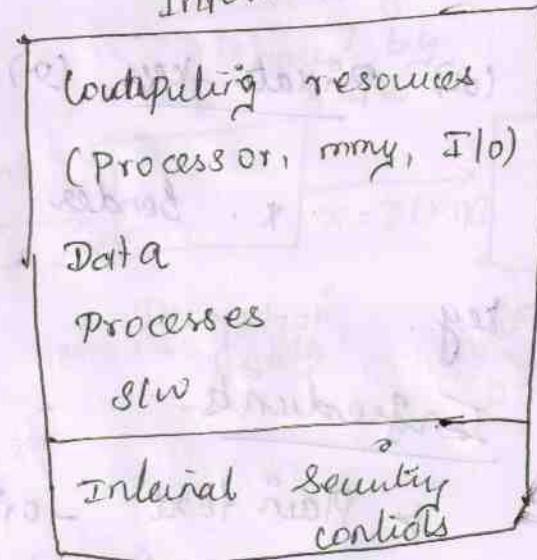
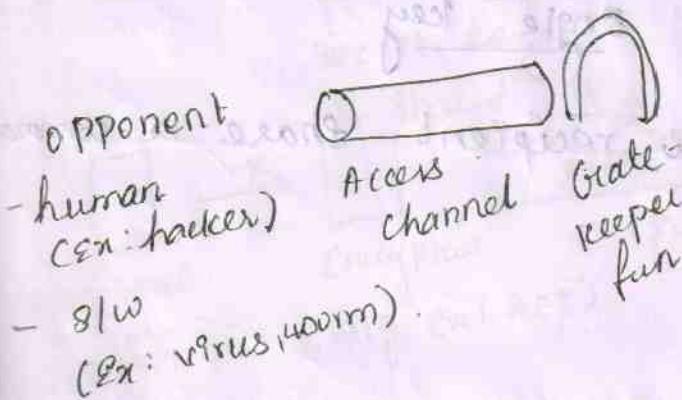
(c)

- It requires us to do the following,
- > Design a suitable algm for the security transformation.
- > Generate the secret info (keys) used by the algm.
- > Develop methods to distribute & share the secret info
- > Specify a protocol enabling the principals to use the transformation & secret info for a security service.

Model for Network Access

security :-

Information System



- * Using network Access security model requires,
 - > Select appropriate gatekeeper func to identify users.
 - > Implement security clets to ensure only authorised users access designated info (ex)

Classical Encryption Techniques

Symmetric Encryption :- [Symmetric cipher m

* Symmetric encryption is a form of crypto system in which encryption & decryption are performed using the same key.

* Symmetric encryption transforms plaintext into cipher text using a secret & an encryption algm. Using the same & a decryption algm, the plaintext is recovered from the cipher text.

* It is also named as conver-

(a) Private-key (b) Single key

* Sender & recipient share a key.

Ingredients:-

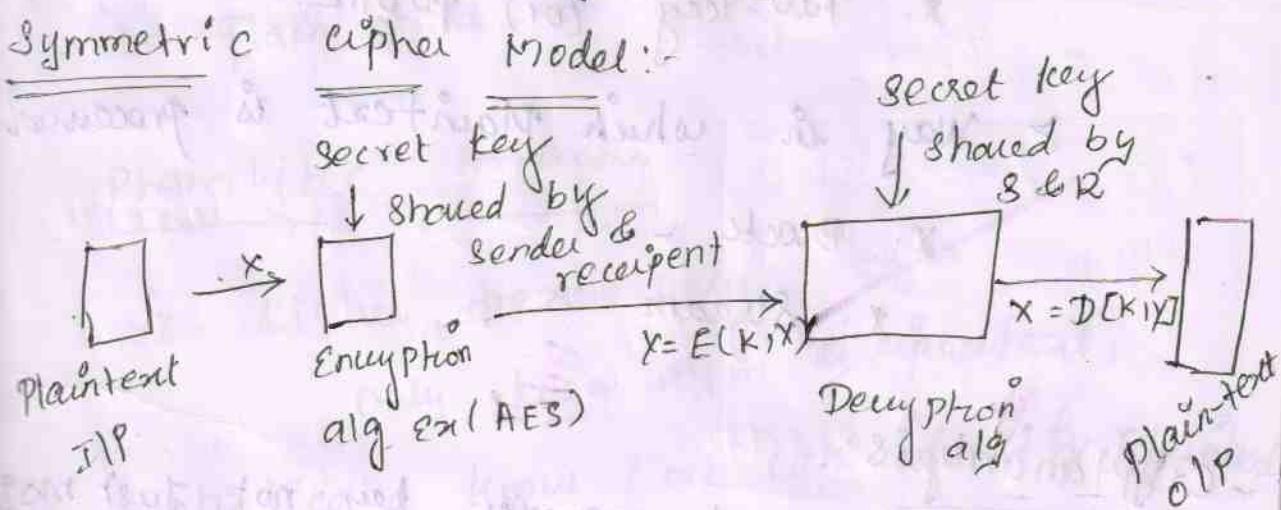
> Plain text - original msg

> cipher text - coded msg

> cipher - algm for transforming plaintext to cipher

> key - Info used in cipher known only to sender / receiver

- > **Encrypt** (Encrypt) - Converting plaintext to cipher text. (12)
- > **decrypt** (Decrypt) - recovering ciphertext from plaintext.
- > **Cryptography** - study of encryption principles & methods.
- > **Cryptanalysis** (code breaking) - Study of principles / methods of deciphering ciphertext without knowing key.
- > **Cryptology** - Field of both Cryptograph & Cryptanalysis.



Requirements:

- * Two requirements for secure use of symmetric encryption:
 - > a strong encryption algm.
 - > a secret key known only to sender / receiver.

$$* \quad Y = E(K, X)$$

(13)

$$X = D(K, Y)$$

Cryptography:-

* It can characterize cryptographic

> type of encryption opns used

* Substitution

* transposition

* Product

> Number of keys used

* Single-key (or) private

* Two-key (or) public.

> Way in which plaintext is p

* Block -

* Stream -

Cryptanalysis:-

* Objective to recover key not p

* It have general approaches

> cryptanalytic attack

> brute-force attack

* If either succeed all key

compromised.

Crypt Analysis:

* the crypt analytic attack depends upon the nature of the algm & little knowledge abt the general characteristics of the plain text (or) plain & cipher text pair.

Brute-force Attacks:-

* Here, the attacker tries to find out the key used for the transformation.
 (or) Attack tries every possible key until an intelligible translation of cipher text into plain text is obtained.

Cryptanalytic Attacks:-

- * cipher-text only
only know algm & ciphertext,
is statistical, know (or) can identify plaintext
- * Known Plaintext
know) suspect plaintext & ciphertext,
- * chosen plaintext
select plaintext & obtain ciphertext
- * chosen ciphertext
select ciphertext & obtain plaintext

* Chosen text

* Select plaintext (or) ciphertext

to encrypt / decrypt

Requirements of encryption algm.

① Unconditional security -

* No matter how much computer

(or) time is available, the cipher

be broken since the ciphertext pro-

insufficient info to uniquely determine

the corresponding plaintext.

② Computational security :-

* Given limited computing resource

(Ex: time needed for calculations is greater than age of universe), the cipher cannot be broken.

Brute force search :-

Ex: Book b2 & PPT also.

* Always possible to simply try on

* most basic attack: proportionate key size

* Assume either know / recognise

plaintext.

Substitution higher techniques:-

16

- * Where letters of Plaintext are replaced by other letters (or) by numbers (or) symbols.
 - * (or) if Plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

→ caesar cipher

↳ monoalphabetic "

> play fair "

> polyalphabetic " " who

> Autolcay

> Vietnam "

→ one-line pad

Caesar cipher :- (by Julius Caesar).

- * first allotted use in military affairs.
 - * Replaces each letter by 3rd letter on.

Ex:

Computer

FRPS x WHU

* It can define transformation as,

a	b	c	d	e	f	g	h	i	j	k	l	..
D	E	F	G	H	I	J	K	L	M	N	O	..
0	1	2	3	4	5	6	7	8	9	W

* then,

$$C = E(k, P) = (P + k) \bmod (26)$$

$$P = D(k, C) = (C - k) \bmod (26)$$

Types of Attacks:

> Brute-force attack.

Cryptanalysis of Caesar cipher:-

* only have 26 possible ciphers

- A maps to A, B, ..., Z.

* a brute-force search - attack

* Given cipher text, just try all

of letters.

* Do need to recognize when the

plaintext

Monoalphabetic cipher:-

* Rather than just shifting the

* Could shuffle (Jumble) the

arbitrarily.

- * Each Plaintext letter maps to a different random ciphertext letter
- * hence key is 26 letters long.

Security

- * Total of $26! = 4 \times 10^{26}$ keys.
with so many keys, might think is secure
but would be wrong. Here, the problem
is language characteristics.

Language Redundancy & Cryptanalysis:-

- * Human lang is redundant
- * ex: "the red sun shined..."
letters not equally commonly used.
- * In English E is by far the most common letter → followed by T, R, N, I, O, A, S.
- * other letters like Z, J, K, Q, X are fairly rare.
- * Have tables of single, double & triple letter frequencies for various lang.

Table in book 66 & PPT

Use in cryptanalysis:-

(19)

- * Key concept - monoalphabetic Substitution ciphers do not change relative letter frequency
- * calculate letter frequencies for ciphertext
- * compare counts / plots against known values
- * If caesar cipher look for common Peaks / troughs
 - * Peaks at : A-E-I triple, NO pair, RST triple.
 - troughs at F-J-K, X-Z.
- * For monoalphabetic must identify each letter
 - tables of common double / triple letters help.

Playfair cipher:-

- * Not even the large no. of keys in a monoalphabetic cipher provides security
- * one approach to improving security was to encrypt multiple letters.

The Playfair cipher is an example.
invented by Charles Cochrane in 1854.

Rules of Encryption:

* When

Playfair Key Matrix:

* A 5×5 matrix of letters based on a keyword.

* Fill in letters of keyword.

* Fill rest of matrix with other letters.

* ex: MONARCHY

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

Encrypting & Decoding:

* Plaintext is encrypted two letters at a time.

(*) if a pair is a repeated letter,

insert letter like 'x'

② If both letters fall in the same row, replace each with letter to right [wrapping back to start from end].

③ If both letters fall in the same column, replace each with letter to right below it (wrapping to top from bottom).

④ otherwise each letter is replaced by the letter in the same row & in the column of the other letter of the

Pau

Ex: Balloon

Ba || oo = n [not accepted.]

ba Ix lo on [replaced replaced by -]

B a
l x
d o
on

elp ü

11

I/J B
8 U
P M
N A

Adv:

> Matrix combination

$$26 \times 26 = \underline{\underline{676}}$$

(22)

> Relative frequency is not the same.

Hence, frequency analysis is difficult.

Dis-adv:-

> Easy to break because it has the structure & the resemblance of the plain text lang.

Hill cipher:-

*. The Hill cipher is a multi-letter cipher. Developed by Lester Hill.

*. The algm takes 'm' successive plain text letters & substitutes for 'm' cipher text letters.

Here, $m=3$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \text{ mod } 26$$

$$c = kp \text{ mod } 26$$

P = Pay $\frac{1}{25}$ to

$$\text{Ex: } \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 14 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \text{ mod } 26$$

$$\rightarrow \begin{pmatrix} 255 + 120 \\ 315 + 504 \\ 30 + 456 \end{pmatrix} \bmod 26 \Rightarrow \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix}$$

$$= \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \Rightarrow \underline{L \ N \ S}.$$

Decryption: $P = k^{-1} C \bmod 26$

Adv & disadv:

- > Completely hides single letter & frequency info.
- > Easiliy attacked with known plain attack.

Polyalphabetic ciphers

- * It is substitution cipher. It increases security using multiple cipher alphabets.
- * It makes cryptanalysis harder because more alphabets to guess & flatten frequency distribution.
- * Use a key to select which alphabet is used for each letter of message.
- * Use each alphabet in turn.
- * Repeat from start after end.

23

mod
26Ex: Auto-key cipher
key: d e c e p t i o n

24

Plain: computer

Cipher text: F S O T J M M M W

one Time Pad:

* If a truly random key as long as the msg is used, the cipher will be secure called a one-time pad.

* It is unbreakable since ciphertext

has no statistical relationship to the plaintext.

* Since for any plaintext &

any ciphertext there exists a key mapping

one to other. It can only use the key

once though.

Adv:

> Random op is produced for each msg

> Not easy to break.

Disadv:

> Practically impossible to generate a random key as to the length of the msg.

> Pblm is key distribution &

key protection.

Transposition techniques

- * It is one cipher that is for the permutation of plain text letters.
- * These hide the msg by rearranging the letter order.

Rail Fence cipher :-

Write msg letters out diagonally a number of rows. Then read off row by row.

Ex: Computer Science

C m u e s i n
o p t r c e

Adv: Cryptanalysis is difficult

Row Transposition cipher :-

- * Row Transposition cipher is more complex.
- * It specifies the order in which the scrambling to be done.

Ex: key : 4 3 1 2

plain text computer science

4	3	1	2
c	o	m	p
u	t	e	r
s	c	p	e
n	c	e	a

1st, 2nd, 3rd, 4th column written in sequence

Ciphertext: me e p r e a o t c c c u s n.

Adv & Disadv:-

- > Early recognized bcoz the freq is same in both plain text & cipher text.
- > Can be made secure by more number of transposition.

Rotor Machines :-

- * The machine has independently rotating cylinders, through which electrical pulses can flow. Each cylinder has 26 pins & 26 pins with internal wiring. The 26 pin wire is connected to an unique 26 pin.

- * If we associate each i/p & o/p with a letter of the alphabet, a single cylinder is a mono-alphabetic substitution.

when each ilp key is depressed, the 27 cylinder rotates one position. The internal connections are shifted. the wrap around is followed after 26th letter.

* the rotor machine is advantageous only when we have multiple cylinders. the o/p pins of one cylinder is connected to the i/p pins of the next.

* The cylinder which is closer to the opr is the ilp cylinder. The ilp rotates one pin position for each key stroke.

* the inner cylinder gives the ip to the middle cylinder which is rotated by one position. The middle cylinder rotates the outer cylinder by one pin position. The DES is uses the concept of rotor machine.

Steganography :-

* In steganograph the plain-text is hidden. The existence of the msg is concealed.

Methods:-

* The text is to be stegged is read in a msg. for ex the sequence of

(27)

187 letters of each word of the over all msg in the hidden msg.

(28)

Character marking :-

selected letters of printed (or) typed text is overwritten with pencil. These marks are not visible. They can be seen when the paper is held at an angle to bright light.

> Invisible Ink

> Pin punchers

> Type writer correction Ribbons.

Adv:
* It can obscure encryption use.

Dis-adv:
* High overhead to hide relatively few info bits.

FINITE FIELDS & Number theory:-

* Will now introduce finite fields of increasing importance in cryptograph.
- AES, elliptic curve, IDEA, public key

* It concern opns on "numbers".

* Group:-

- * Group is a set of elements (or) numbers denoted by $\{G\}$ * } \hookrightarrow binary opns.
- * It may be finite (or) infinite with some open whose result is also in the set (closure).

Axioms are obeyed:-

$$\Rightarrow \text{Associative law: } (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

> Identity element e : $e \cdot a = a \cdot e = a$

> Inverse element a^{-1} : $a \cdot a^{-1} = e$

& commutative $a \cdot b = b \cdot a$.

* Then forms an abelian group

Cyclic Group:-

* Define exponentiation as repeated

appln of opx

$$\text{ex: } a^3 = a \cdot a \cdot a$$

* Identity be: $e = a^0$

* A group is cyclic if every elem

is a power of some fixed element.

$$(i) b = a^n \text{ for some } a \text{ & every } n$$

be a generator of the

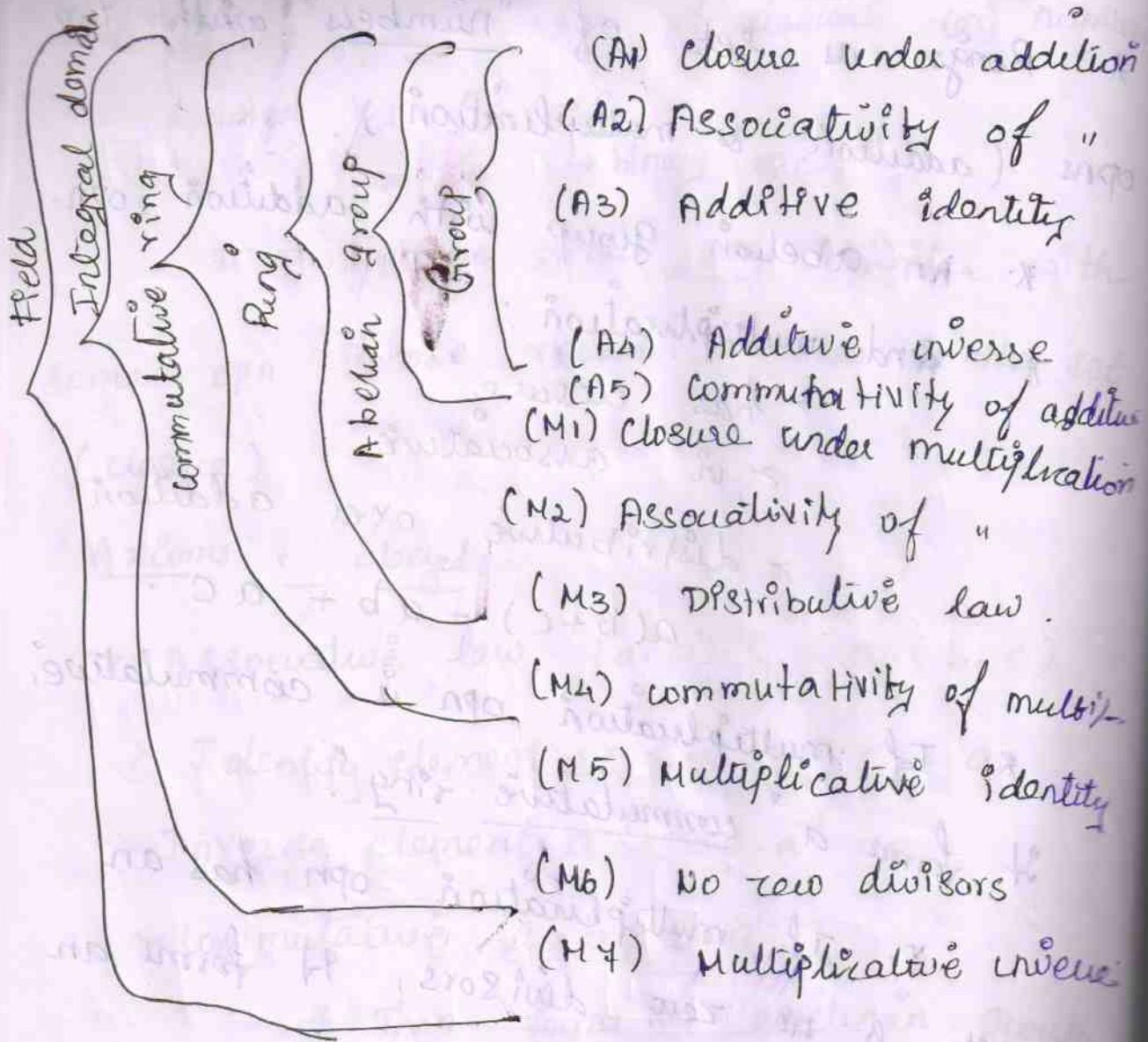
Rings:-

(30)

- * Rings as set of "numbers". with two ops (addition & multiplication).
- * An abelian group with addition opn.
- * And multiplication:
 - > has closure.
 - > is associative
 - > distributive over addition.
$$a(b+c) = ab + ac.$$
- * If multiplication opn is commutative, it forms a "commutative ring".
- * If multiplication opn has an identity & no zero divisors, it forms an "integral domain".

Fields

- * A set of numbers with 2 opns,
- * A set of numbers with 2 opns,
 - > abelian group for addition
 - > " multiplication
 - > "
 - > (ignoring 0)
 - > ring.
- * Have hierarchy with more axioms/laws
- > group \rightarrow ring \rightarrow field



modular Arithmetic

* Define modulo opr "a mod n" to be remainder when a is divided by n

* r is called a residue

$$a = qn + r$$

$$\therefore r = a \bmod n$$

* modulo reduction $\because 0 < r \leq n - 1$

$$\underline{\text{Ex:}} \rightarrow -12 \bmod 7$$

$$\rightarrow -5 \bmod 7$$

$$\rightarrow 2 \bmod 7$$

* a & b are congruent if: 32

$$[a \bmod n = b \bmod n]$$

* when divided by n , a & b have same remainder.

* ex: $100 = 34 \bmod 11$.

Operations:-

* Can perform arithmetic with residues

* uses a finite no. of values, & loops back from either end

$$\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$$

* It is when do addition & multiplication & modulo reduce answer can do reduction at any point,

$$[a + b \bmod n = [a \bmod n + b \bmod n] \bmod n]$$

Properties:-

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$.

ex: $[(11 \bmod 8) + (15 \bmod 8)] \bmod 8$.

$$\begin{aligned} &\Rightarrow 10 \bmod 8 \Rightarrow 2 (11+15) \bmod 8 \\ &= 26 \bmod 8 = \underline{\underline{2}} \end{aligned}$$

$$2. [(a \bmod n) - (b \bmod n)] \bmod n \quad (33)$$

$$= (a - b) \bmod n.$$

$$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8$$

$$\Rightarrow -4 \bmod 8 \Rightarrow 4(11 - 15) \bmod 8$$

$$\Rightarrow -4 \bmod 8 \Rightarrow \underline{4}.$$

$$3. [(a \bmod n) \times (b \bmod n)] \bmod n$$

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

$$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8$$

$$\Rightarrow 81 \bmod 8 \Rightarrow 5(11 \times 15) \bmod 8$$

$$\Rightarrow 165 \bmod 8 \Rightarrow \underline{5}.$$

Ex seen in Book 134 & PPT
135

Euclid's algorithm

4. An efficient way to find the GCD

$$\text{GCD}(a, b) = \text{GCD}(b, a \bmod b)$$

\hookrightarrow Greatest common divisor

Alg'm: Euclidean Alg'm to compute $\text{GCD}(a, b)$

$\text{Euclid}(a, b)$

if ($b = 0$) then return a ;

else return $\text{Euclid}(b, a \bmod b)$;

33

Extended Euclidean Alg:-

34

- * Calculates not only GCD but x & y .

$$ax + by = d = \text{gcd}(a, b).$$

- * It useful for later crypto computations

- * follow sequence of divisions for GCD
but assume at each step i, can find x & y :

$$\boxed{x = ax + by}$$

- * at end find GCD value & also x & y .
- * if $\text{GCD}(a, b) = 1$ these values are inverse.

Finite Fields (Galois)

- * Finite fields play a key role in crypto.

- * It can show no of elements in a finite field must be a power of a prime p^n . It can be denoted $\text{GF}(p^n)$.

or

Ex:

1. $\text{GF}(P)$

2. $\text{GF}(2^n)$.

Galois fields $\text{GF}(P)$

- * $\text{GF}(P)$ is the set of integers $\{0, 1, \dots, P-1\}$ with arithmetic ops modulo prime P .

* Since have multiple cative inverses

& find inverse with extended Euclidean algm.

* Hence, arithmetic is "well-behaved" and can do addition, subtraction, multiplication & division without leaving the field $\text{GF}(p)$

GF(7) Multiplication

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Polynomial Arithmetic

* It can compute using polynomials,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \sum a_i x^i$$

* Several alternatives,

> ordinary polynomial arithmetic

> Poly arithmetic with coords mod p

> .. and polynomials mod m

ordinary Polynomial Arithmetic :-

(36)

- * Add (or) Subtract corresponding co-efficients
- * Multiply all terms by each other.

ex:-

$$f(x) = x^3 + x^2 + 2 \text{ and } g(x) = x^2 - x + 1$$

$$f(x) + g(x) = x^3 + 2x^2 - x + 3$$

$$f(x) - g(x) = x^3 + x + 1$$

$$f(x) \times g(x) = x^5 + 3x^3 - 2x + 2.$$

Polynomial Arithmetic with modulo co-efficients

- * when computing values of each coefficient do calculation modulo some value

- forms a polynomial ring.

co-efficients are 0 (or) 1.

$$f(x) = x^3 + x^2 \text{ & } g(x) = x^2 + x + 1$$

$$f(x) + g(x) = x^3 + x + 1$$

$$f(x) \times g(x) = x^5 + x^2.$$

Polynomial Division :-

- * In the form, $f(x) = q(x)g(x) + r(x)$.

- * can interpret $r(x)$ as being a remainder

$$r(x) = f(x) \bmod g(x).$$

- * If have no remainder say $g(x)$ divides $f(x)$.
- * If $g(x)$ has no divisors other than itself & I say it is irreducible (or prime) polynomial.

* Arithmetic modulo an irreducible polynomial forms a field.

Number theory

Prime Numbers:

- * prime nos only have divisors of 1 and self they cannot be written as a product of other numbers.
- * 1 is prime, but is generally not of interest.
- * prime nos r central to number theory.

Ex: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...

Prime Factorisation:

- * To factor a no 'n' is to write it as a product of other numbers.

$$n = a \times b \times c$$

- * Factoring a no is relatively hard compared to multiplying the factors together to

* the prime factorisation of a number n
 is when its written as a product of primes
 to n .

Ex: for $n=10$.
 complete set of residues is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Reduced set of residues is $\{1, 3, 7, 9\}$.

* No of elements in reduced set of residues is called the Euler Totient Fun $\varphi(n)$.

$$\text{Ex: } a = 7 \times 13 ; \quad 3600 = 2^4 \times 3^2 \times 5^2$$

$$\therefore a = \prod_{p \in P} p^{ap}$$

Fermat's Theorem

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

$$\because p - \text{prime} \quad \& \quad \gcd(a, p) = 1.$$

$$* a^p = a \pmod{p}$$

↳ useful in public key & primality testing.

Euler Totient Fun $\varphi(n)$

* When doing arithmetic modulo n .

* complete set of residues is $0, \dots, n-1$

* Reduced set of residues is those nos

* To compute $\varphi(n)$ need to count no of residues to be executed

(39)

* for p (prime) $\varphi(p) = p - 1$

* for $p \cdot q$ (p, q prime) $\varphi(p \cdot q) = (p-1)(q-1)$

Ex: $\varphi(37) = 36$

$$\varphi(21) = (3-1) \times (7-1) = 2 \times 6 = 12.$$

Euler's theorem:

* A generalization of Fermat's theorem

* $a^{\varphi(n)} = 1 \pmod{n}$

↳ for any a, n where $\gcd(a, n) = 1$.

Ex: $a = 3; n = 10; \varphi(10) = 4;$

hence $3^4 = 81 \equiv 1 \pmod{10}$

$a = 2; n = 11; \varphi(11) = 10;$

hence, $2^{10} = 1024 \equiv 1 \pmod{11}$

also have: $a^{\varphi(n)+1} \equiv a \pmod{n}$.

Primality Testing

Testing

to

- * often need to find large prime nos.
- * traditionally, sieve using trial division
 - > (e). divide by all nos (primes) in turn less than the square root of the no.
 - > only works for small nos.
- * Alternatively, can use statistical primality tests based on properties of primes.
 - > for which all primes nos satisfy property
 - > but some composite nos, called pseudo-primes, also satisfy the property.
 - > can use a slower deterministic primality test.
- In PPT:
 - > Miller Rabin algm
 - > probabilistic consideration
 - > prime distribution

Chinese

Remainder

Theorem

- * Used to speed up modulo computations
- * If working modulo a product of nos

$$\text{Ex: } \mod M = m_1 m_2 \cdots m_k$$

- * Chinese Remainder theorem lets us each moduli mi separately

* Since, this is faster than working in the full modulus M . (41)

Chinese Remainder theorem:-

- * Can implement CRT in several ways
- * To compute $A \pmod{M}$
 - > first compute all $a_i = A \pmod{m_i}$ separately
 - > determine constants c_i below, where $M_i = M/m_i$.
 - > then combine results to get answer,

$$A = \left(\sum_{i=1}^k a_i c_i \right) \pmod{M}$$

$$c_i = M_i \times (M_i^{-1} \pmod{m_i}) \text{ for } 1 \leq i \leq k.$$

Primitive Roots

- * From Euler's theorem have a $\varphi(n)$ mod $n-1$.
- * Consider $a^{m-1} \pmod{n}$, $\text{GCD}(a, n) = 1$.
 - > must exist for $m = \varphi(n)$ but may be smaller
 - > once powers reach m , cycle will repeat
- * If smallest $m = \varphi(n)$ then a is called a primitive root

* If P is prime, then successive power of a generate the group mod P , these are

Discrete Logarithms

A2

- * The "inverse" problem to exponentiation
is to find the discrete logarithm of a
no modulo P .
* (ii) to find i such that,
 $b = a^i \pmod{P}$
written as, $i = d \log_a b \pmod{P}$.
 - * If a is a primitive root then it
always exists, otherwise it may not,
ex: $x = \log_3 4 \pmod{13}$ has no answer
 $x = \log_2 3 \pmod{13} = \underline{\underline{4}}$ by trying
successive powers.
 - * Whilst exponentiation is relatively easy,
finding discrete logarithms is generally
a hard problem.

Discrete Logarithms mod 19 :-

base 2, modular 19 :-

base 3, modulo 19 :-

(43)

a	1	2	3	4	5	6	7	8
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3

9	10	11	12	13	14	15	16	17	18
2	11	12	15	17	13	5	10	16	9