1st lecture
23/7/19

Page No.:
Date:
YOUVA

System and Network Security

3-0-2-4

	Sessional I	15
	Sessional II	15
	End-sem	50
(5-6)	Lab Assignments	20
		100

Providing and understanding technological solution to security.

Information age

Where information is an asset and has a value like any other asset

Hence, information needs to be secure from attacks

Page No.:
Date:
YOUVA

Confidentiality - privacy, secrecy
securing the data

nsmitting data from one point to another
sic security element
& one other than receiver should read it.

Availability - service should be available
at all times

Denial of Service - DoS attacks

Non repudiation - refusal / denial of sending
or receiving data.

2nd lecture

24/7/19

Why internet security ?
Why Information security ?

Cyber attacks in News.

Phishing
Identity theft
Distributed denial of service (DDoS).
Malware - worms, viruses, spyware botnets
Information Warfare

1) understand goals of hacker / attacker / adversary.
2) try to understand types of attacks possible
3) Identify vulnerabilities
   — weaknesses / lacuna in the policies / procedures / protocols, H/W, S/W within an organisation that has a potential to cause damage / loss.

Two types of defenses

1) Prevention — level of access based on transaction

What kind of services / security you want. — controlled access.

through access controls, authentication, encryption etc.

DDoS prevention — Captcha. (Humans - not M/Cs. M/Cs can generate many requests).

Detection

Intrusion detection system
- N/W based
- (solo) based host
- could be signature based
- anomally based.

Traceback, forensics

Security vs Adversary.

Policy - confidentiality, integrity, availability
Threat Model - assumption @ adversary
Mechanism - S/W, H/W

CIA

any process designed to protect / prevent / recover from attack — mechanism

entity authentication (connection oriented)
data origin authentication (connectionless)

services — putting things in place for prevention

flaw in design of protocol — information system can be exploited.

3rd lecture
30/7/19.

OSI Security Architecture

- Security Attacks
  - Passive
    - Unauthorized reading of a message / file and traffic analysis (no movement to get noticed).
  - Active
    - modification of msgs / files and DoS attack.
- Mechanisms
  - any process designed to detect, prevent & recover from security attacks.
  - Eg: encryption algs, digital signature, authentication protocol.
  - design mechanisms based on type of security attack.
- Services
  - includes authentication, access control, data confidentiality, data integrity, non-repudiation and availability.

Level of security — low, moderate or high which depends on requirement of application

Page No.:
Date:
YOUVA

Course.

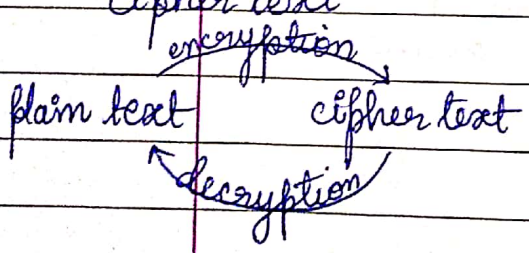
Cryptographic algos and protocols - have large range of applications
- symmetric encryption
- asymmetric encryption
- data integrity algos
- authentication protocol

Network and internet security
→ rely heavily on cryptographic techniques
→ consists of measures to deter, prevent, detect and correct security violations involved in transmission of information

Key Objectives

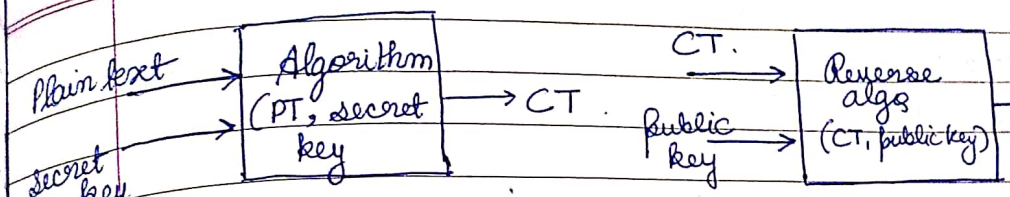
Confidentiality

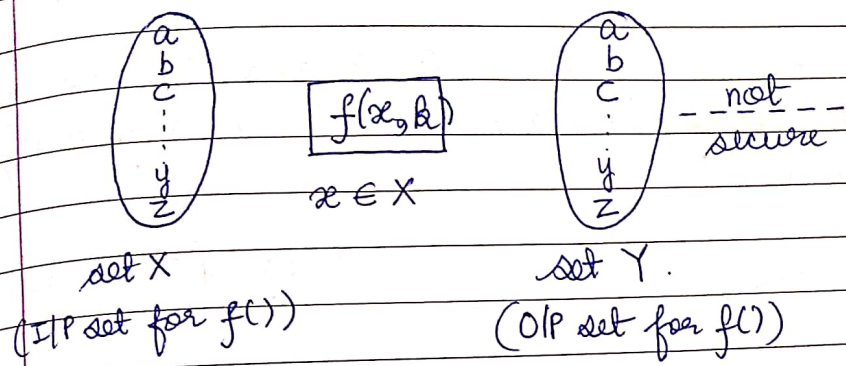
Intellectual msg transferred as unintellectual.
- conversion technique known to receiver
- plain text
- cipher text.



Integrity

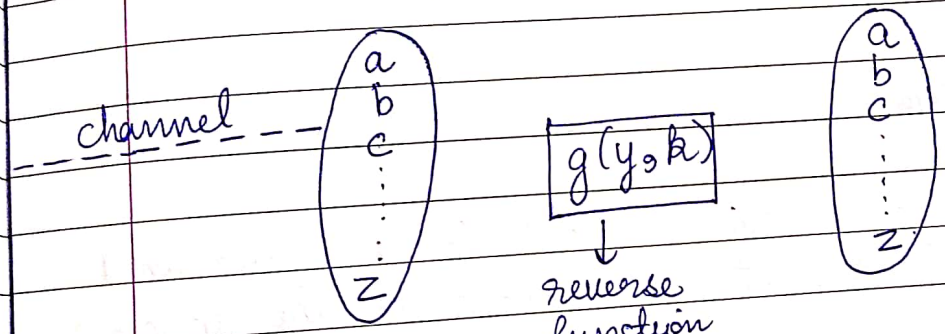
Availability





cardinality for both is 26. one-one mapping required.

* f() should be reversible



If we consider binary conversions, with 'n' bits for each character in msg,
cardinality of I/P and O/P space = 2^n.

Typically in cryptography, I/P and O/P spaces are same because crypto algos are just mathematical computations or mapping.

Costs might be associated with the conversions as well.

Domain codomain

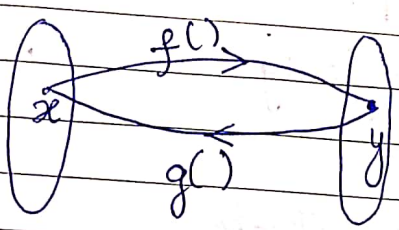
Types of functions

$x \Rightarrow y = f(x)$ ✓

$y \Rightarrow f(x) = y$ ×

if $f(x)$ is easy to compute for all $x \in X$ but for essentially all elements $y \in Im(f)$, it is computationally infeasible to find any $x \in X$ such that $f(x) = y$

— One way functions.



$f: X \to Y$

$g: Y \to X$

g: inverse of f.

↓

needed in cryptography

$X = \{1, 2, \ldots 16\}$

$Y \Rightarrow f(x) = 3^x \% 17$

since $|X|$ is small, we can maintain a lookup table but for large $|X|$, it becomes infeasible.

Trapdoor one-way functions

(Asymmetric Key cipher)

Given : 2 primes p and q.

$n = p \times q$

Given : n

find p and q.

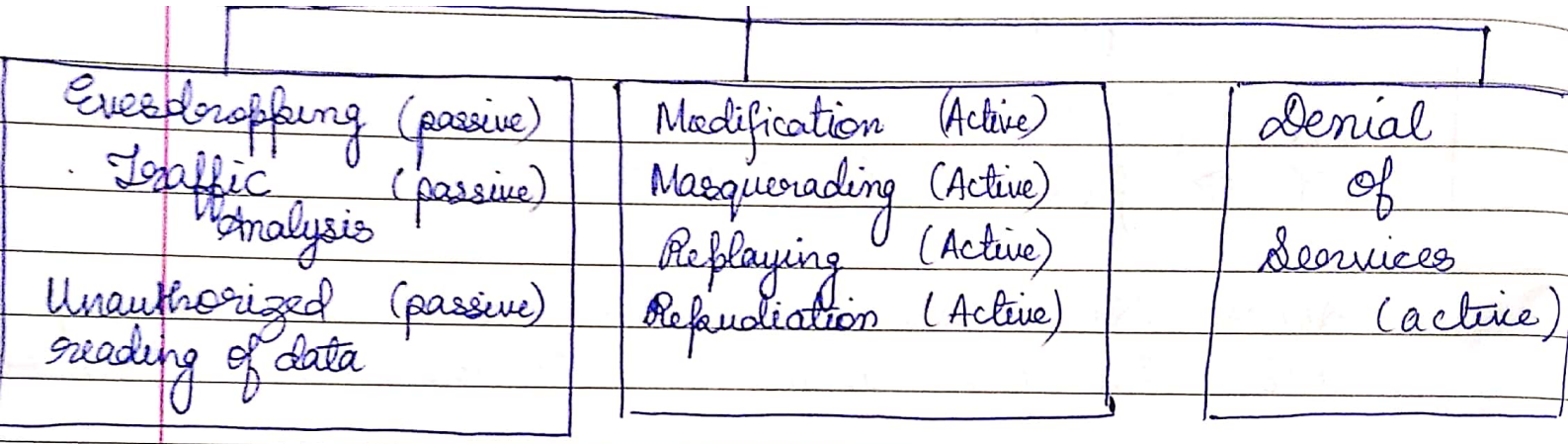
n bits to represent a number.

Find p and q such that pq = number.

(factorization)

Find complexity in terms of 'n'.

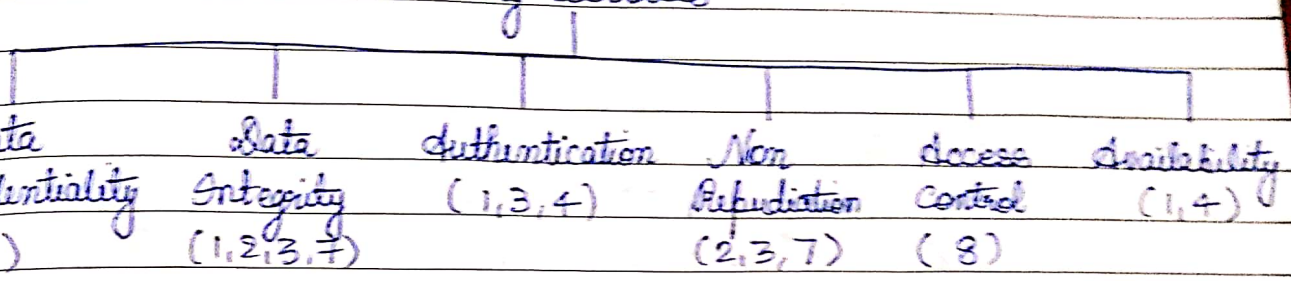
Most of modern ciphers are based on assumption that there is no efficient algo for factorisation.



4 types of attacks

Security Services

Derived in X.800 and RFC 2828
Download document and read 2-3 initial pages.



Security Mechanisms

1. Encipherment
2. Data Integrity
3. Digital Signature
4. Authentication Exchange
5. Traffic Padding
6. Routing Control
7. Notarization
8. Access control mechanism

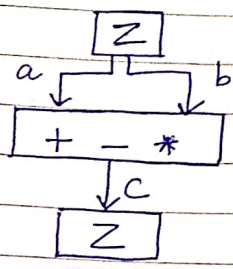
Cryptography - Transformation of message under control of secret key

Integer Arithmetic

* set of integers

$$Z = \{ \ldots -2, -1, 0, 1, 2, 3 \ldots \}$$

* Binary operations



* Integer Division

$a = q * n + r$

with 2 restrictions

$n > 0$

$r \geq 0$

* Divisibility

$a = q * n \Rightarrow n | a.$

$a = q * n + r$ where $r > 0$, $n \nmid a.$

* GCD

Facts 1) $GCD(a, 0) = a$

$GCD(a, b) = GCD(b, r)$

Euler's algo

$gcd(a, b) = p$ where $p > 1$

$gcd(a, b) = 1$

then a and b are coprime or relatively prime

Additive Cipher

encryption : $C = (P + K) \bmod 26$

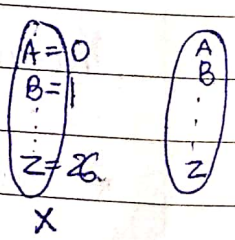
C → cipher text, P → plain text, K → key

decryption : $K' = 26 - K$

$P = (C + K') \bmod 26$

↓

Symmetric Cipher



two forms of cryptography

(i) symmetric / private
— single key shared by sender and receiver

(ii) Asymmetric / public
— separate keys for sender and receiver

$K = \{ K_e , K_d \}$
K_e → public key, K_d → private key

Symmetric key cryptography

* Plain text (P)
* Cipher text (C)
* Secret key (K)
* Encryption algo uses P, K
* Decryption algo uses C, K

L-6
06/08/19

Extended Euclidean Algorithm (a, b)

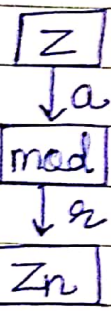
```
{
    r1 = a ;
    r2 = b ;
    s1 = 1 ;
    s2 = 0 ;
    t1 = 0 ;
    t2 = 1 ;
    while ( r2 > 0)
    {
        q = r1/r2 ;
```

```
    r = r1 - q * r2;
    r1 = r2;
    r2 = r;
    s = s1 - q * s2;
    s1 = s2;
    s2 = s;
    t = t1 - q * t2;
    t1 = t2;
    t2 = t;
  }
  gcd(a,b) = r1;
  s = s1;
  t = t1;
}
```

Scanned by CamScanner

Modular Arithmetic

Mod operation



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

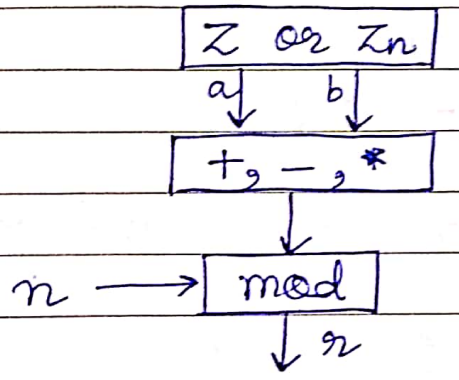
↓

set of residues

Residue class : set of integers congruent to modulo n.

Mapping of Z to Z_n is many to one mapping.

Operations on Z_n



$$\begin{cases} C = (P+K) \bmod n \\ C = (P*K) \bmod n \end{cases}$$

encryption

For decryption, we need to know inverse of key K^{-1}. and it should exist.

Multiplicative Inverse

If $(a * b) \bmod n \equiv 1 \bmod n$, a and b are multiplicative inverses of each other.

Elements of Z_n that are relatively prime to n have multiplicative inverse.
Z_n^* is a subset of Z_n with elements belonging to Z_n that have multiplicative inverse.

If n is prime, all elements of Z_n except 0 will be coprime with n

$\therefore \quad Z_n^* = Z_n - \{0\}$

Else $Z_n^* = \{ z' \text{ where } z' \in Z_n \text{ and } \gcd(z', n) = 1 \}$

Eg: $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

$Z_8^* = \{1, 3, 5, 7\}$.

Page No.:
Date:

Assume $\gcd(a, n) = d$.
If $d \mid b$, there are d solutions
If $d \nmid b$, there are no solutions.

$5x \equiv 12 \bmod 17$ $\quad a = 5 \quad b = 12 \quad n = 17$

Find multiplicative inverse of 5 for $n = 17 \Rightarrow 7$.

$\underbrace{5 * 7}_{1} * x \equiv 7 * 12 \bmod 17$

$x \equiv 84 \bmod 17$

$x = 16.$

$(5 \times 16) \bmod 17 = 80 \bmod 17$

$= \underline{\underline{12}}$

We can solve a set of linear equations with same modulo if the matrix formed from coefficients of the variables is invertible.

$M \in Z_9$

$M = k$

All matrices defined over Z_n might not have multiplicative inverse - only if Δ is coprime with n.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & & & \vdots \\ \vdots & & & \vdots \\ a_{k1} & \cdots & \cdots & a_{kk} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}$$

7th lecture
07/08/19

Page No.:
Date:

Cryptology

Cryptanalysis

↓

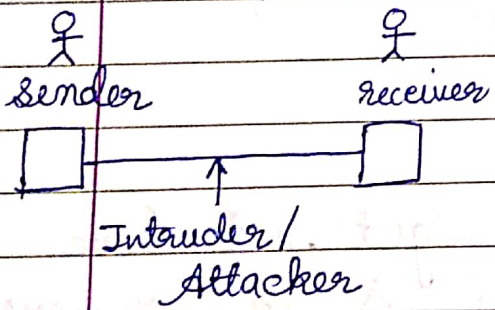
is the science and art of breaking those codes without the knowledge of secret information

Cryptography

Cryptanalysis attacks

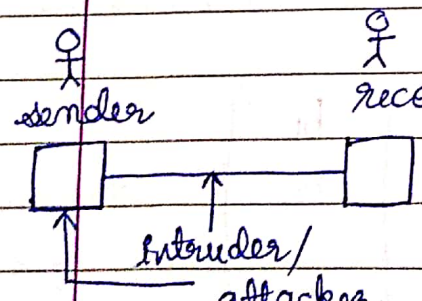
1. Cipher text only
2. Known plain text attack
3. chosen plain text attack
4. Chosen cipher text attack

1)



Given : C only cipher text
Find : K key
algorithm is open - assumption

2)

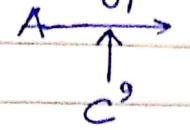


Given : C, P
Find : K

→ if sender does not secure plain text
→ if attacker knows the part of cipher text which is plain text
→ knowledge based
→ no extra efforts needed.

3) attacker designs the plain text such that when sender encrypts it, cipher text exposes some information about key i.e. getting key becomes easier. Attacker should have access to sender's machine.

4) attacker has tapped cipher text and somehow gets it decrypted from sender.

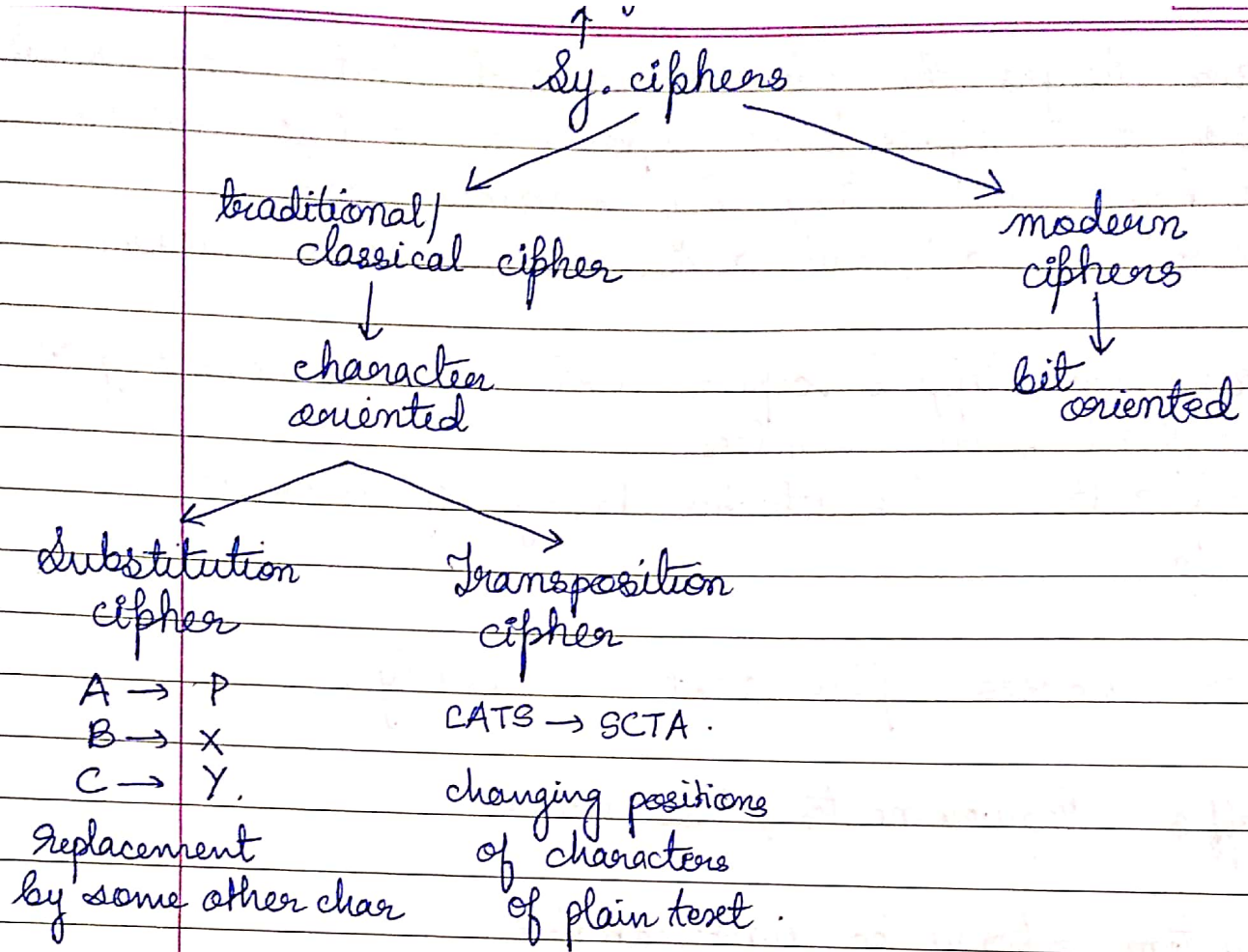


C' is attacker having cipher text.

Attacker chooses cipher text consciously.

Kerchoff's Requirements / Essentials

⇒ the system should be unbreakable
⇒ compromise of system details should not cause inconvinience to correspondents.
⇒ The key should be easy to remember and change.
⇒ Cryptogram should be transmissible by the telegraph.
⇒ should be portable and operable by a single person
⇒ should be easy
⇒ user of encryption algorithm can strive for an algo that meets one or both of the following
(i) the cost of breaking the cipher should exceed the value of encrypted information
(ii) the time required to break the ciphers should exceed the useful life ~~terms~~ time of the encrypted information.



Substitution Cipher

1. Monoalphabetic substitution
2. Polyalphabetic substitution

1) Irrespective of position and context, one alphabet is replaced by another alphabet for every occurrence. (the same)

2) The alphabet to replace any alphabet depends on position and context of every occurrence. Hence, can be different.

1) Caesar / Shift / Additive Ciphers

$C = P + K$

Depending on cardinality of plain text space, modulo is defined.
↓ depends on user.

What different values can K take? [1 - 25] (ignore 0)

A - 0
B - 1
C - 2
⋮
Z - 25

Key space $- Z_n$.

$P = \frac{C - K}{n - k}$

Is break cipher: (1) (2) (3)
only ciphertext attack
Brute force.
try each transformation
key domain small.

2) Product Cipher

$C = (P * K) \bmod n.$

$P = (C * K^{-1}) \bmod n$
↓ multiplicative inverse.

$n = 26$
∴ only 12 elements of Z_n can be key.

$|\text{Keyspace}| = |Z_{26}^*|$.

∴ $|\text{Key space}| = |Z_{26}^*|$

3) Affine cipher

$C = ((P * K_1) + K_2) \bmod n.$

09/08/19.

Substitution Cipher — frequency distribution analysis; cypher text only attack possible

⇒ A can be replaced with any letter from same domain

⇒ B can be replaced with any letter from same domain except the one used for A

One key – one substitution table.

A	B	C	D	.....	X	Y	Z
25	24	23	22		.....		

A not replaced with A

∴ No. of substitution tables = $25! - 1$

|Key space| = $25! - 1$.

Brute force – not feasible

Letter statistic analysis – to break this cipher (frequency etc).

Polyalphabetic Substitution Cipher

It preserves the frequency of letter → Monoalphabetic drawback.

∴ To break this cipher, frequency distribution can be used.

⇒ It hides the frequency distribution by making multiple substitutions

⇒ Always works on block of letters. — poly.

i) Playfair cipher

If two letters are same in a block of 2 letters,

No brute force
only ciphertext attack not possible – only for huge ciphertext
2 letter frequency distribution analysis – diagram
we replace one of them with a dummy letter

There is a keyword for every cipher.

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

P Q | R X | E B | E S | T S |
A Y | G M | R T | B L | B K |

search for PQ – both letters in same column, replace letter with letter below that in the matrix

if both letters fall in same row, each will get replaced with the letter on the right.

if both are not in same row or column,
first letter : first ka row, second ka column.
– common letter
second letter : first ka column, second ka row

I is substituted with L in one scenario and with K in another – depends on context
– polyalphabetic nature

Therefore, frequency is not preserved → statistic analysis not possible

Matrix – transformation function

Key space |K| – 25!. I and J occupies same cell – fixed

2) Vigenere Cipher

Plain text P
Key K.
Divide P into blocks each of size |K| → pre-processing required.

$$P = \underbrace{p_1 p_2 p_3 p_4}_{k_1 k_2 k_3 k_4} | \cdots | \underbrace{p_i p_{i+1} p_{i+2} p_{i+3}}_{k_1 k_2 k_3 k_4} |$$

$$C = c_1 c_2 c_3 c_4 \cdots c_i c_{i+1} c_{i+2} c_{i+3}.$$

Encryption : $c_i = p_i + k_i$

If same letter is in different positions — different substitutions.

Key space : ${}^{26}P_m$ if |key| = m.

What is cryptanalysis of this cipher ?

3) Hill Cipher.

Preprocessing required
Plain text divided into block of size n.

Key-matrix — $n \times n$

If $n = 2$, $\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \left(\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} * \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \right) \bmod n$

$K_{ij} \in Z_n$. $\forall$ i and j

What is key space size ?
- depends on which matrices Δ is coprime with n.

$P = K^{-1}C$.

context dependent and position dependent
(which letter in same block) (position in block).

$C_1 = k_{11}P_1 + k_{12}P_2$
$C_2 = k_{21}P_1 + k_{22}P_2$.

Key space : 26^{n^2}. $\begin{bmatrix} 26 & 26 \\ 26 & 26 \end{bmatrix}$

↓
No, because all keys are not possible.

Brute force : not feasible.
Only cipher text attack not possible
Known plain text - atleast 4 blocks
↓
$n \times n$.

Atleast n pairs of C and P are needed :

One problem from this - in sessional.

Distributed Attack on Hill cipher

15/8/19.

Page No.:
Date:

Autokey cipher

$P = P_1 P_2 \ldots P_m$

$K = K_1 K_2 \ldots$ No. It is a shift cipher, additive

$$+\ \underset{C_1}{K} \nearrow\ +\ \underset{C_2}{C_1} \nearrow\ +\ \underset{C_3}{C_2} \ldots \nearrow\ +\ \underset{C_m}{C_{m-1}}$$

The previous block cipher is used as a key.

Enigma – HW.

Transposition Ciphers

Keyed, unkeyed.
Position of letters changes – frequency remains same

P = Hello World.
→ H l o W r d.
→ e l o l

C = HloWrdel ol.

These are keyless ciphers.

P = Hello World. C = HWeolrllod.

P =

H	l	o	d
e	o	r	x
l	W	l	x

dummy elements

C = HlodeorxlWlx.

If the frequency distribution does not change in cipher text — then it is transposition cipher

Keyed Transposition cipher

1 2 3 4 5 6 7 8 9 10

⇒ P = Hella World

⇒ Say n = 5. (Divide P in blocks of size n).

⇒ Key = 45132

4 5 1 3 2 | 4 5 1 3 2

C = | l | o | H | l | e | l | d | W | r | o |

∴ Key - one permutation of n.

∴ |Key space| = n!

Given encryption key, find out the decryption ke

Encryption key : 45132

key	4	5	1	3	2
index.	1	2	3	4	5

Sort the key, accordingly sort the indese.

key	1	2	3	4	5
index	3	5	4	1	2

∴ | key | 3 | 5 | 4 | 1 | 2 | → decryption key.
|---|---|---|---|---|---|---|
| index | 1 | 2 | 3 | 4 | 5 | |

Hence, if we know the encryption transposition key, we can get the decryption key as well.

Challenge here is finding size of block — appropriate 'n'.

Cryptanalysis — self study.

One-time Pad.

⇒ Theoretical cipher

⇒ $P = P_1 P_2 P_3 \ldots P_n$.

$K = K_1 K_2 \ldots K_n$

$+$

$C = C_1 C_2 C_3 \ldots C_n$.

Pattern String

Key String — random

↓

needs to be communicated to the receiver so that he/she can generate plain

Since it is random, receiver will not be able to recover the key.

Cryptography requires sets of integers and specific operations that are defined for those sets.

The combination of the set and the operations that are applied to the elements of the set is called algebraic structures

- Groups
- Rings
- Fields

Page No.
Date
YOUVA

Groups.

/ division
- not binary
- generates remainder

A group (G_1) is a set of elements with a binary operation $(*)$ that satisfies 4 properties

1) closure $G_1 = \{ \langle Z_n \rangle , * \}$.

$a, b \in Z_n$

If $c = a * b$ and $c \in Z_n$.

$\forall$ a, b — closure is satisfied

2) Associative

$(a * b) * c = a * (b * c)$ where $a, b, c \in Z_n$.

3) Commutativity (Commutative group / Abelian group).

$a * b = b * a$ where $a, b \in Z_n$.

4) Existence of Identity

$a * e = a$ where $a, e \in Z_n$.

5) Existence of Inverse

$a * b = e$ where $a, b, e \in Z_n$.

Let $G_1 = \langle \{ Z_8 \}, + \rangle$

$Z_8 = \{ 0, 1, 2, 3, 4, 5, 6, 7 \}$.

Since it is Z_n set, we have modulo arithmetic operations.

1. closure.

$(a+b)\%n = c$

$\downarrow$

$\mathbb{Z}_n$ }.

yes.

2. associative

$[(a+b)\%n]+c\%n$

$(a+[(b+c)\%n])\%n$

— are equal — yes.

3. Identity : 0. — yes

4. ~~multi~~ inverse : $(n-a)$ for a. — yes.

∴ This algebraic structure is a group.

Check for $*$ and $\langle \{\mathbb{Z}_8^*\}, * \rangle$

$G_1 = \langle \{(1,2,3), (1,3,2), (3,1,2), (3,2,1), (2,1,3), (2,3,1)\}, \square \rangle$

$\square$: composition operator.

(1,2,3)

abc Apply (3,2,1)

$\downarrow$

cba Apply (2,3,1). composition of 2 permutations.

$\downarrow$

bac

(2,1,3) → belongs to same set. → closure

$(P_1 \square P_2 \square P_3)$

$(P_1 \square P_2) \square P_3$ $\quad$ $P_1 \square (P_2 \square P_3)$.

14/0

(1,2,3)
abc
↓ (3,2,1).
cba
↓ (2,3,1)
bac

(1,2,3)
abc
↓ (2,3,1)
bca
↓ (3,2,1)
acb.

∴ Not associative

14/08/19

Groups
- finite
- order of group
- subgroup
- cyclic subgroup
- Lagrange's theorem.
- Order of an element

(1,2,3) abc
↓
(3,2,1) cba

(3,2,1) cba
↓
(1,2,3) abc.

⇒ It is ~~communicate~~ commutitive
⇒ If it is cascading, we can apply final o/p to string and get same mapping.
⇒ doesn't improve strength of cipher.

⇒ number of elements in group - order of group.
⇒ number of elements are finite - finite
⇒ subgroup - should satisfy all properties of a group.

cyclic subgroup :- if a subgroup of a group can be generated using the power of an element. Its subgroup is called a cyclic subgroup.

$a^n \Rightarrow \; a \circ a \circ a \ldots$ (n times)

$G_1 = \langle Z_8, + \rangle$ → modulo.

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

$H_0 = 0^0 = 0 \bmod 8$

$0^1 = (0+0) \bmod 8$

$0^2 = (0+0+0) \bmod 8$.

$H_1 = 1^{0+1} = 1 \bmod 8$ $\qquad 1^0 = 0 \bmod 8$.

$1^{1+1} = (1+1) \bmod 8$

Page No.:
Date:
YOUVA

⇒ Cyclic group :- a cyclic group is a group that is its own cyclic subgroup.

$\{ e, g^1, g^2, g^3 \ldots g^{n-1} \}$ where $g^n = e$.

$a = 3 = g$.

$3^0 = 0 = e$

$3^1 = 3 =$

$3^2 = 6$

$3^3 = 1$

$3^4 = 4$

$3^5 = 7$

$3^6 = 2$

$3^7 = 5$.

generator group
- generates all values of Z_n.

$\{ 0, 3, 6, 1, 4, 7, 2, 5 \}$.

↓

cyclic group.

$3^8 = 24 \cdot 1.8$
$= 0$
$= e$.

$G = \langle Z_{10}^*, \times \rangle$.

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

Some ciphers use generators because generators use both I/P and O/P space i.e it will not map plain text to a subset of O/P space - it maps to each and every element of O/P space i.e it covers the complete O/P space.

Lagrange's Theorem

If n is large - how many generators ? (which elements)
- which generator used in cipher ?

Assume that G is a group and H is a subgroup of G. If the order of G and H are |G| and |H| respectively, then based on this theorem,
|H| divides |G|.

$G = \langle Z_{10}^*, \times \rangle$

$Z_{10}^* = \{1, 3, 5, 7\}$.

$H_1 : a = 1$.

← cyclic subgroup.

$1^0 = 1 \bmod 10 = 1$
$1^1 = 1 \bmod 10 = 1$
$1^2 = 1 \bmod 10 = 1$

$|H| = 1$ 1 divides 4
$|G| = 4$.

$H_2 : a = 3$.

$|H_2| = 4$ $a = 3$ 4 divides 4
$|H_3| = 4$ $a = 7$ 4 divides 4
$|H_4| = 2$ $a = 9$. 2 divides 4.

★★★ Start from 1. 3^1
↓ 3^2
not zero. 3^3
3^4

Order of an element

order of an element, say a, in a group — ord(a) is the smallest integer r such that $a^r = e$.

$G_1 = \langle Z_{10}^*, \times \rangle$ $\quad Z_{10}^* = \{1,3,5,7\}$.

order(3) = 4.

$3^4 = 81 \bmod 10$

$= 1$

$= e$.

$G_1 = \langle Z_7, \times \rangle$ $\quad Z_7 = \{0,1,2,3,4,5,6\}$.

ord(1) =

ord(2) =

ord(3) =

Ring

It is an algebraic structure with two operations. An abelian group can be extended to form a ring.

All properties of a group + distributive property

$R = \langle Z_n, *, \square \rangle$

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

↓ distributive property.

* : first op.
□ : second operation

1) Distribution of □ over *
2) □ should satisfy closure and associativity
3) If it satisfies commutativity then it's a Commutative ring.

Eg) $R = \langle Z_n, +, * \rangle$.

+ → all 5 properties

* → 3 properties ← closure, associativity, commutativity (optional)

Field

$R = \langle Z_8, +, \times \rangle$ → It is a ring.

all 5 properties ✓ closure ✓ associativity ✓

It is not a field.

$Z_8 \to \times$ — does not have multiplicative inverse for 0, 2, 4, 6.

does not follow exception because $+_c = 0$.

$R = \langle Z_8^{**}, +, \times \rangle$ ✓

$R = \langle Z_p, +, \times \rangle$ ✓ where p is a prime no.

Galois showed that for a field to be finite, the number of elements should be p^n where p is prime and n is a positive integer.

A galois field $GF(p^n)$ is a finite field with p^n elements.

⇒ GF(p) - have a set $Z_p = \{0, 1, 2 \ldots (p-1)\}$ with two operations.

GF(2) - set has two elements which are binary digits (0 and 1)

(i) Addition is actually XOR operation
(ii) Multiplication is AND operation
(iii) Addition and subtraction are the same.
(iv) Multiplication and division are the same.

GF(2) :- $(0, 1), +, \times$

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$e = 1$ (multiplication)

$e = 0$ (addition).

Additive inverse

a	0	1
-a	0	1

$0 \oplus 0 = 0$
$1 \oplus 1 = 0$] identity.

Multiplicative inverse

a	0	1
a^{-1}	x	1

$0 \& 1 = 0$
$0 \& 0 = 0$] not identity.
$1 \& 0 = 0$
$1 \& 1 = 1$ – identity.

GF (5) = $\langle \{0,1,2,3,4\}, +, * \rangle$.

x	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

order of element
generaters.

Groups
Rings – commutative group, distributive group
Fields

⇒ For ciphers, functions need to be invertible
⇒ For cryptography, fields are preferred because all 5 properties are satisfied by both operators.

GF(2) field is very important for us – binary system.

Polynomial is a set of bits
For every polynomial, inverse for both operators will exist..

AES
Advanced Encryption Standard

$GF(2^2) = <\{00, 01, 10, 11\}, +, \times>$

↓
two bits can be handled.

2 ↑ how many positions
2 ↓ how many values.

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

11
11
1 10

↓
correct?

×	00	01	10	11
00	00	00	00	00
01	00	00	00	01
10	00	00	10	10
11	00	01	10	11

→ Incorrect because for a bit stream [not GF(2)] anding does not give correct product.

Polynomial

A polynomial of degree $(n-1)$ is an expression of the form $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots a_0 x^0$

where x^i – (i^{th} position) i^{th} term
a_i – i^{th} term coefficient

Rules need to be followed to represent n bit word by polynomial

a) The power of x defines position of x in n bit word

b) The coefficient of the term defines the value of the bit, as bit can have only a value of 0 or 1, polynomial coefficients can only be either 0 or 1.

8 bit word – 10011001

1	0	0	1	1	0	0	1
x^7			x^4	x^3			x^0

Simply : $x^7 + x^4 + x^3 + 1$.

Given : $x^6 + x^4 + x^2 + 1$. What is the word ?

01010101

Polynomial representing n-bit words use two fields
(i) GF(2)
(ii) GF(2^n)

$$x^7 + x^4 + x^3 + 1$$
$$\oplus \quad x^6 + x^4 + x^2 + x$$
$$x^7 + x^6 + x^3 + x^2 + x^1 + 1$$

$$10011001$$
$$\oplus \quad 01010110$$
$$11001111$$

This won't generate a polynomial of higher degree.
— like polynomial addition.

For multiplication,

$x^7 \cdot x^6 = x^{13}$ → but our system is 8 bit
∴ we do modulo operation

If a polynomial cannot be reduced by modulo,
— irreducible.

⇒ For the set of polynomials in $GF(2^n)$, a group of polynomials with degree n is defined as modulus. Such polynomials are referred as irreducible polynomials.

Degree	Irreducible polynomial
1	$(x+1)$, x
2	$x^2 + x + 1$