Scheme Of Evaluation
Internal Assessment Test 1 – March.2019

Sub:	Cryptography,Network Security & Cyber law							Code:	15CS61
Date:	05 / 03 / 2019	Duration:	90mins	Max Marks:	50	Sem:	VI	Branch:	ISE

Note: Answer Any Five Questions

Question #		Description	Marks Distribution		Max Marks
1	a)	**Find the gcd of 421 and 111 using Euclidean Algorithm.** • Finding the gcd of 421 and 111 using Euclidean Algorithm.	3M	3M	10 M
	b)	**Decrypt the given cipher text into plain text using transposition cipher.** **Cipher text: wtnoeesrckpyctrtiuyrnahdyaropg** **Note: Consider 6x5 matrix The key used for encryption is as follows: Row :1->3, 2->6, 3->5, 4->1, 6->4, 5->2 Column: 1->3,2->5,3->2,4->1,5->4** • Column wise transposition • Row wise transposition	3M 4M	7M	
2	a)	**Calculate the modulo inverse of 3458mod4864 using extended Euclid's Algorithm[b=4864, c=3458]** • Extended Euclid's Algorithm steps • Finding inverse modulo.	4M 6M	10M	10 M
3	a)	**Discuss how encryption is done using DES construction.** • DES algorithm	10M	10M	10 M
4	a)	**Perform encryption & decryption for the plaintext M= 2 using RSA algorithm(Note: Select p=7, q=11,e=13)** • Finding d value • Encryption • Decryption	1M 4M 1M	6M	10 M
	b)	**Describe common vulnerabilities in any computer system or network.** • Vulnerabilities	4M	4M	

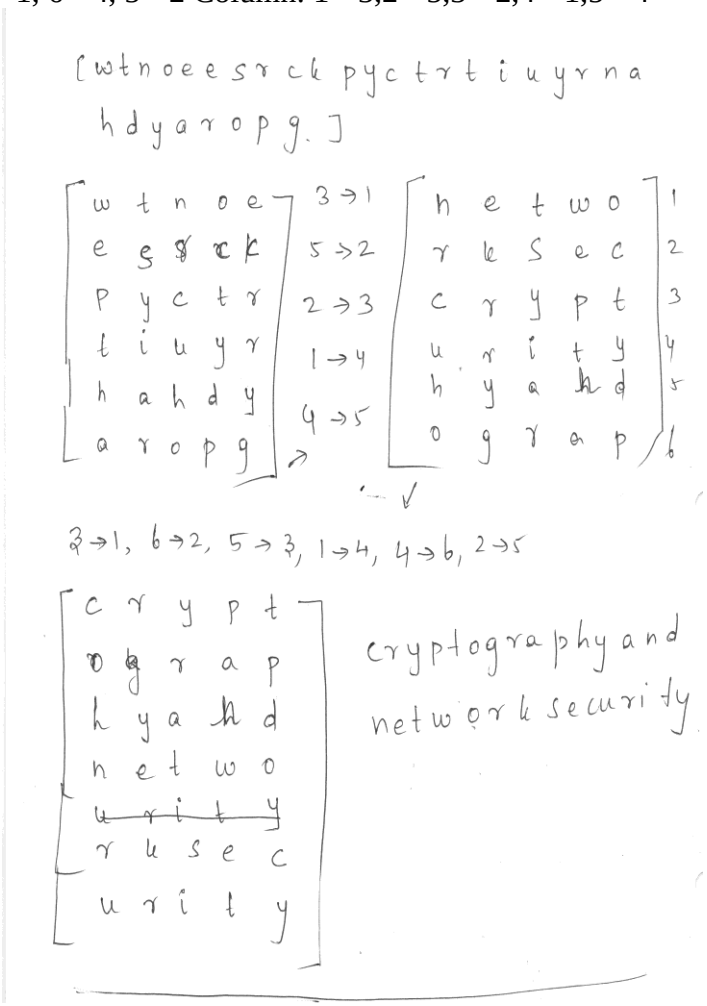
5	a)	**Explain the guiding principles for security.** • Guiding principles	5M	5M	10 M
	b)	**List defense strategies and techniques.** • Defense strategies and techniques. (4 techniques)	5M	5M	
6	a)	**Explain in brief about public key cryptographic standard.** • Public key cryptographic standard (diagram) • Theory	3M 2M	5M	10 M
	b)	**Solve the following equations using Chinese remainder theorem.** **$x \equiv 3 \bmod 5$, $x \equiv 5 \bmod 6$, $x \equiv 2 \bmod 7$** • Finding M • Finding M1,M2,M3 • Finding $M1^{-1}, M2^{-1}, M3^{-1}$ • Finding x	0.5M 0.5M 2M 2M	5M	
7	a)	**Discuss substitution cipher and its types with suitable examples.** • Mono alphabetic cipher (Ceaser cipher) • Poly alphabetic cipher:Vignere cipher • Hill cipher • One-time pad	2M 3M 3M 2M	10M	10 M
8	a)	**Whether Whatsapp chat is secured? If yes, explain how it is achieved.** • Whether Whatsapp chat is secured? • Explanation	1M 9M	10M	10 M

Answers

1. A . Find the gcd of 421 and 111 using Euclidean Algorithm. (3)

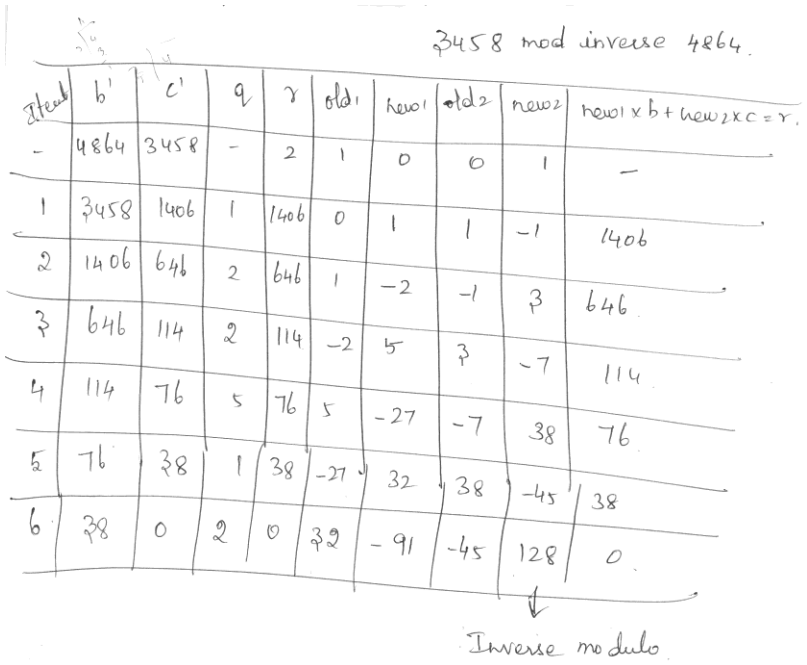
```
421 = 111 x 3 + 88   (larger number on left)
111 = 88 x 1 + 23    (shift left)
88 = 23 x 3 + 19     (note how 19 moves down the "diagonal")
23 = 19 x 1 + 4
19 = 4 x 4 + 3
4 = 3 x 1 + 1        (last non-zero remainder is 1)
3 = 1 x 3 + 0
```

b. Decrypt the given cipher text into plain text using transposition cipher.
Cipher text: **wtnoeesrckpyctrtiuyrnahdyaropg**
Note: Consider 6x5 matrix The key used for encryption is as follows: Row :1->3, 2->6, 3->5, 4->1, 6->4, 5->2 Column: 1->3,2->5,3->2,4->1,5->4 (6)



2. A .Calculate the modulo inverse of 3458mod4864 using extended Euclid's Algorithm[b=4864, c=3458] (10)

Algorithm: (inverse of c mod b)
computeinverse(b,c)
{
old=1 new1=0
old2=0 new2=1
b′=b c′=c
r=2
while(r>1){
q=b′/c′
r=b′%c′
temp1=old1-new1*q
old1-new1 new1=temp1
temp2=old2-new2*q
old2=new2 new2=temp2
b′=c′ c′=r
new1*b+new2*c=r
}
return new2 //new2 is the modulo inverse
}



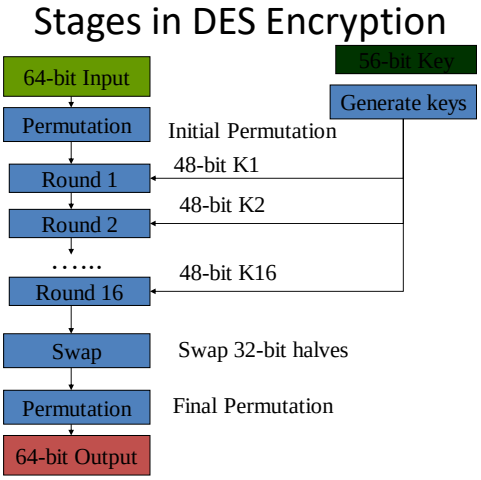
3. Discuss how encryption is done using DES construction. (10)

DES (Data Encryption Standard)

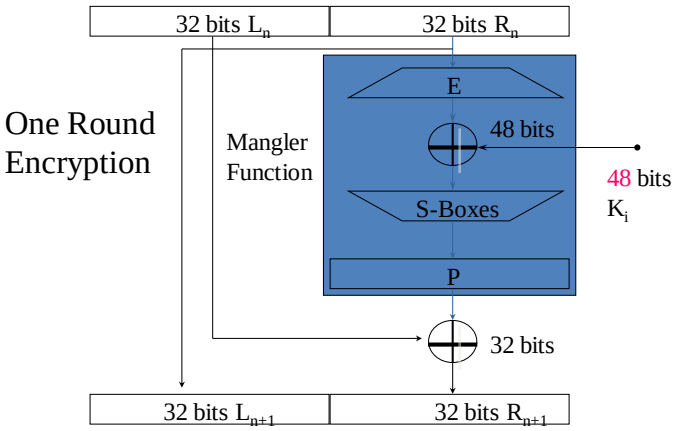
Published as standard cipher for symmetric key cryptography by NIST(National Institute of Standards and Technology)

Fiestel Structure

- Block size-64 bits • Key size-56/128 bits
- Stages:
- Initial Permutation
- 16 rounds of a given function
- 32 bit left-right swap
- Final permutation



Single round of DES



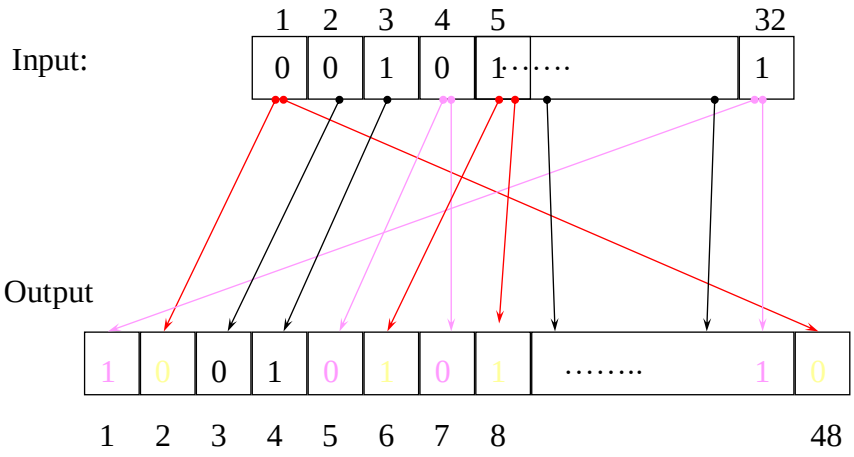
In encryption

- Li=Ri-1
- Ri=Li-1 xor f(Ri-1,Ki)
- In Decryption
- Ri-1=Li
- Li-1=Ri xor f(Li,Ki)

Round function f(Ri-1,Ki)

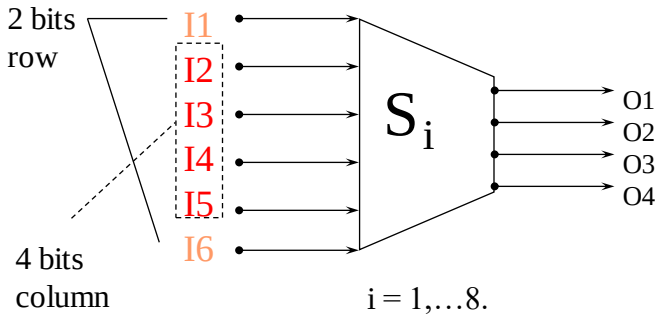
- Expansion-32 bit to 48 bit
- Xor with the round key- 48 bit key
- Substitution
- Permutation

Bits Expansion (1-to-m)

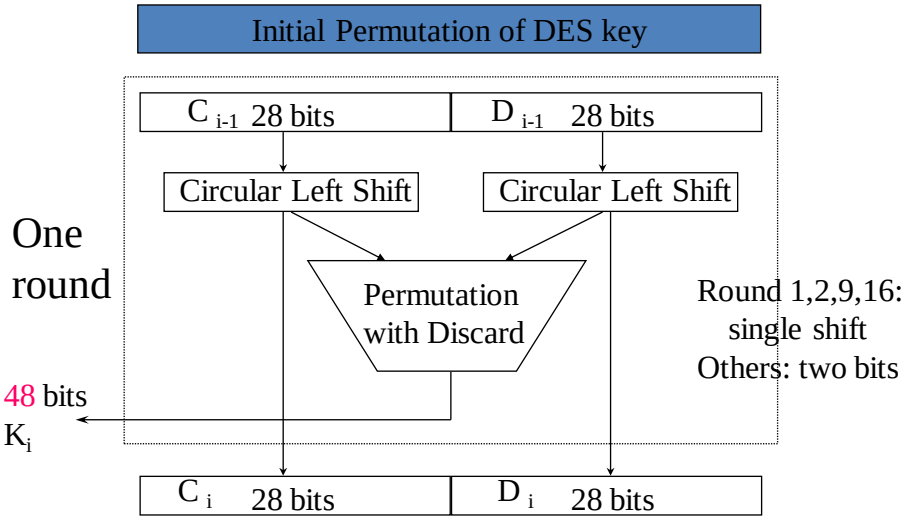


S-Box (Substitute and Shrink)

- 48 bits ==> 32 bits. (8*6 ==> 8*4)
- 2 bits used to select amongst 4 substitutions for the rest of the 4-bit quantity



Per-Round Key Generation



4 a. Perform encryption & decryption for the plaintext M= 2 using RSA algorithm (6)

Choose n:

Start with two prime numbers, ***p*** and ***q***. This time we try: p = 7 & q = 11. Then n = p * q = 7 * 1 = 77.

Calculate Φ(n):

Φ(n): = (p-1)(q-1) = 6 * 10 = 60.

Choose e & d:

Try e = 13. Then, d = 37, since 13 * 37 = 481 and 481 mod 60 = 1.

Now test it out:

We know that

if $C = P^e \bmod n$, then $P = C^d \bmod n$.

Let P = 2.

Then

$C = 2^{13} \bmod 77 = 8192 \bmod 77 = 30.$

and we obtain P back again thus:

$P = 30^{37} \bmod 77 =$

$450283905890997363000000000000000000000000000000000 \bmod 77 = 2.$

4. b Describe common vulnerabilities in any computer system or network. (5)

Weakness in a procedure, protocol, h/w or s/w within an organization that has the potential to cause damage.

Vulnerability classes:

1. Human Vulnerabilities
   - Induced by human behavior or action
   - eg. clicking a link may leads to phishing or cross site scripting attack, e-mail virus
2. Protocol Vulnerabilities
   - Protocols in LAN such as TCP, IP, ARP can be easily attacked
   - Pharming attacks: ARP protocol to get passwords from LAN, man in the middle attack, replay attack
3. Software vulnerabilities
   - In app' s/w
   - eg
   - Without validation of limit of user input may lead to buffer overflow
   - in text field if some java script is given then validation is stopped eg of cross site scripting vulnerability
   - in text field if SQL query is given then validation is stopped eg SQL injection vulnerability
4. configuration vulnerability
   - configuration settings in newly installed s/w can be given wrongly e.g read, write & execute privileges

5.a. Explain the guiding principles for security. (5)

1. Security is as much a human problem than a technological problem & must be addressed at different levels

It should be addressed by top level mgmt

- Chief Information Security Officer (CISO)

Robust security policies should be formulated

- Security Engineers
- key role to play in designing technique and products to protect organizations from the various cyber attacks

- System administrators
- Handle day-to-day operations
- Configure systems & applications

- Employees
- should be educated on various do's and don'ts through periodically updated security awareness programs.

2. Security should be factored in at inception, not as an afterthought

- Application s/w is often vulnerable to attack
- Soln: Integrating secure coding practices into the s/w curriculum in the colleges
- 3. Security by obscurity- unknown(or by complexity) is often bogus- not genuine or true
- New security protocols may also have serious vulnerabilities
- They should be properly deployed in hacker perspective

4. Always consider the "Default Deny" policy for adoption in access control

- Default Permit- unless subject(people, n/w packets.,,) is in Blacklist
- Default Deny – unless subject is in Whitelist
- Disadvantages:
- Mistakenly some legitimate subject whose name has been excluded from the whitelist
- Mistakenly some attacker subject whose name has been excluded from the blacklist

- 5. An entity should be given the least amount/level of permissions/privileges to accomplish a given task
- Role based access control: principle idea in RBAC is that mapping between roles and permissions
- 6. Use 'Defense in depth' to enhance security of an architectural design
- 2 firewalls configured by 2 different s/m administrators

7. Identify vulnerabilities & respond appropriately

- Risk assessment
- Risk=Assests X Vulnerabilities X Threat
- If the assests impacted by a vulnerability are of low value and /or the threat perception(probability that a vulnerabilty is successfully exploited) is small, then the associated is low.
- In such case it may not make economic sense to address such vulnerabilities

8. Carefully study the tradeoffs involving security before making any

- Engg design often involves making tradeoffs- cost versus performance.
- E.g Many airports requires passengers to check in several hours before flight departure, where human convenience is being sacrificed same as this cyber security also have same issue like..
- The s/m will not allow you to log in today unless u change ur pwd.(The s/m expects u to do so at least once in 3months)

b. List the defense strategies and techniques. (5)

1.Accesscontrol-Authentication and Authorization

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.

Authentication: assurance that the entity is the one that claims to be

E.g After login into system using password(Authentication) the job of the access controller is to answer authorization questions

Whether Kavya is allowed to write into the file CS1561

Access ctrl decision is based on:

the subject or principal , kavya

the object or resource CS1561

the access mode or operation write

Authentication/Authorization

ID card to enter into college

Hall ticket to enter into exam hall to write exam

- Firewall: to protect n/w from outside world

2. Data Protection

i) Confidentiality : assurance that the message is send and received only by authorized persons

ii) Integrity : The data is not changed during transit

Is achieved by Encryption, decryption and cryptographic checksum which is achieved by shared secret key

the sender computes the checksum using one way function and sends the checksum along with the message and the receiver computes the checksum and cross check with the received check sum

3. Prevention and Detection

Prevention strategies

access control, encryption

Detection strategies

cryptographic checksum

S/w security

Black box testing: when the source code of the pgm is not easily available

The goal is to determine whether the s/w has been carefully designed to handle unexpected or malicious i/p.

White box testing: the security engineer has access to source code

& can perform more elaborate testing

Intrusion prevention technique- false +ve false –ve

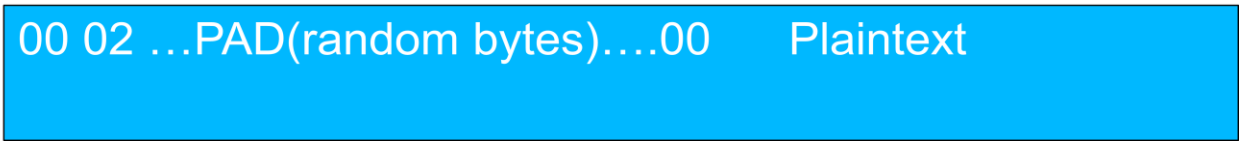
Intrusion detection technique- Anti virus products are signature based

4. Response, Recovery and Forensics

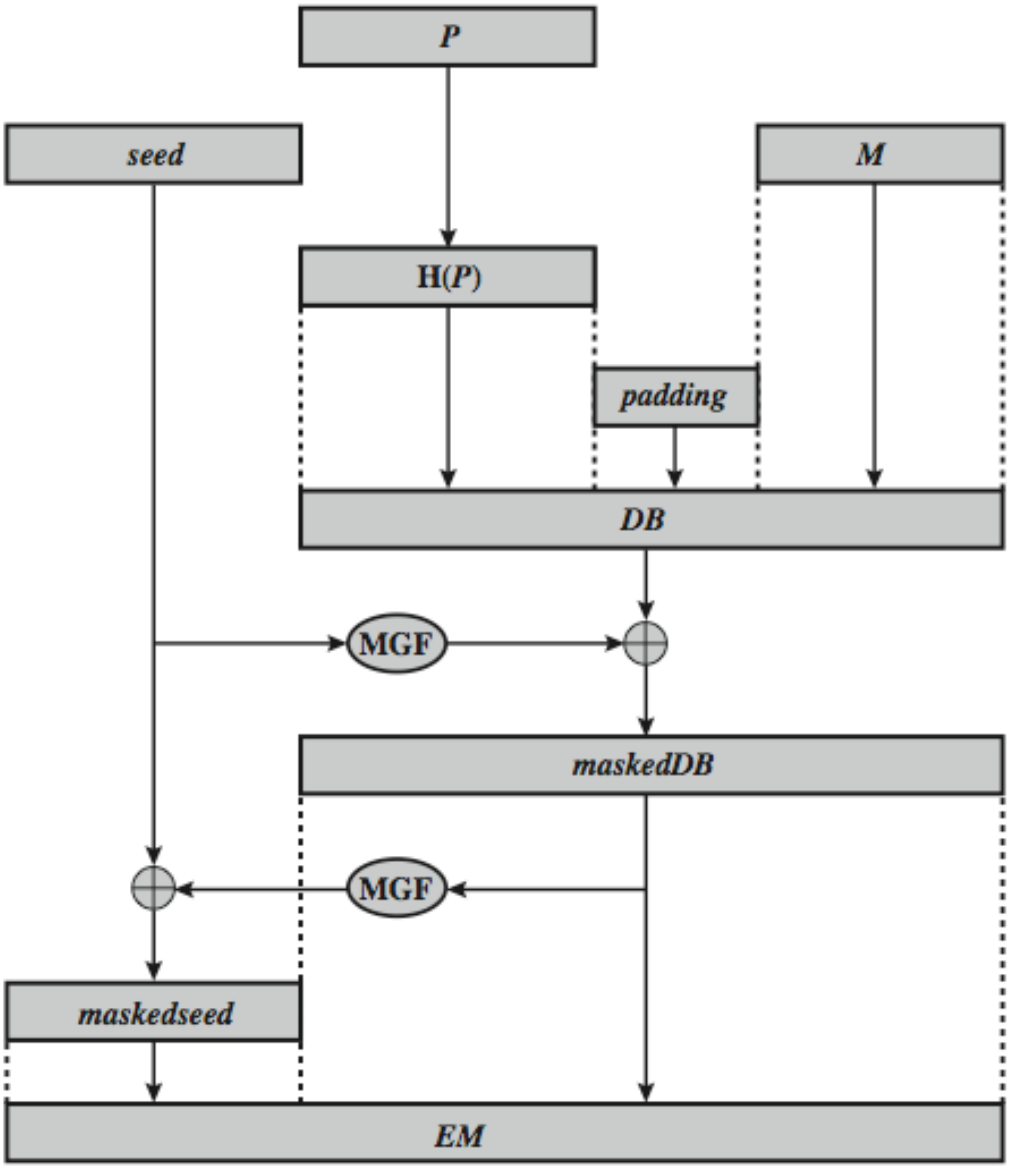
- Once an attack behavior is identified response measures should be taken and the system should be recovered to working state
- Cyber forensics is an emerging technique used to identify attacker using the fingerprint they left

6.a . Explain in brief about public key cryptographic standard. (5)

- can counter the attacks with random pad of plaintext



- Right most 00 specifies the starting of data bit
- or use Optimal Asymmetric Encryption Padding (OASP)



P = encoding parameters
M = message to be encoded
H = hash function
DB = data block
MGF = mask generating function
EM = encoded message

(b) Solve the following equations using Chinese remainder theorem. (5)
$x \equiv 3 \bmod 5$, $x \equiv 5 \bmod 6$, $x \equiv 2 \bmod 7$

(b) $x \equiv 3 \bmod 5$

$x \equiv 5 \bmod 6$

$x \equiv 2 \bmod 7$

→ 5 marks

$a_1 \equiv 3,\ a_2 = 5,\ a_3 = 2$

$m_1 = 5,\ m_2 = 6,\ m_3 = 7$

Step1: $M = m_1 \times m_2 \times m_3$

$= 5 \times 6 \times 7 = 210.$

Step2: $M_1 = M/m_1 = 210/5 = 42$

$M_2 = M/m_2 = 210/6 = 35$

$M_3 = M/m_3 = 210/7 = 30.$

Step3: $M_1 M_1^{-1} \equiv 1 \bmod (5)$ $\therefore 42 \times M_1^{-1} = 1 \bmod 5$

$42 \times 3 M_1^{-1} \equiv 3 \bmod 5$

$\boxed{M_1^{-1} \equiv 3}$

$M_2 M_2^{-1} \equiv 1 \bmod 6$ $35 \times M_2^{-1} \equiv 1 \bmod 6$

$175 M_2^{-1} \equiv 5 \bmod 6$ $\boxed{M_2^{-1} = 5}$

$M_3 M_3^{-1} \equiv 1 \bmod (7)$ $30 M_3^{-1} \equiv 1 \bmod 7$ $M_3^{-1} = 4$

Step4:

$x = [(a_1 \times M_1 \times M_1^{-1}) + (a_2 \times M_2 \times M_2^{-1}) + (a_3 \times M_3 \times M_3^{-1})] \bmod M$

$= [3 \times 42 \times 3] + [5 \times 35 \times 5] + [7 \times 30 \times 4] \bmod 210$

$= 1493 \bmod 210.$

$\boxed{x = 23}$

7.a. Discuss substitution cipher and its types with suitable example. (10)

Types

- Mono alphabetic cipher
- Poly alphabetic cipher
- Caeser cipher

- earliest known substitution cipher
- by Julius Caesar
- It is a mono alphabetic cipher because each letter is always substituted for another unique letter
- first attested use in military affairs replaces each letter by 3rd letter on example:

meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB

- can define transformation as:

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

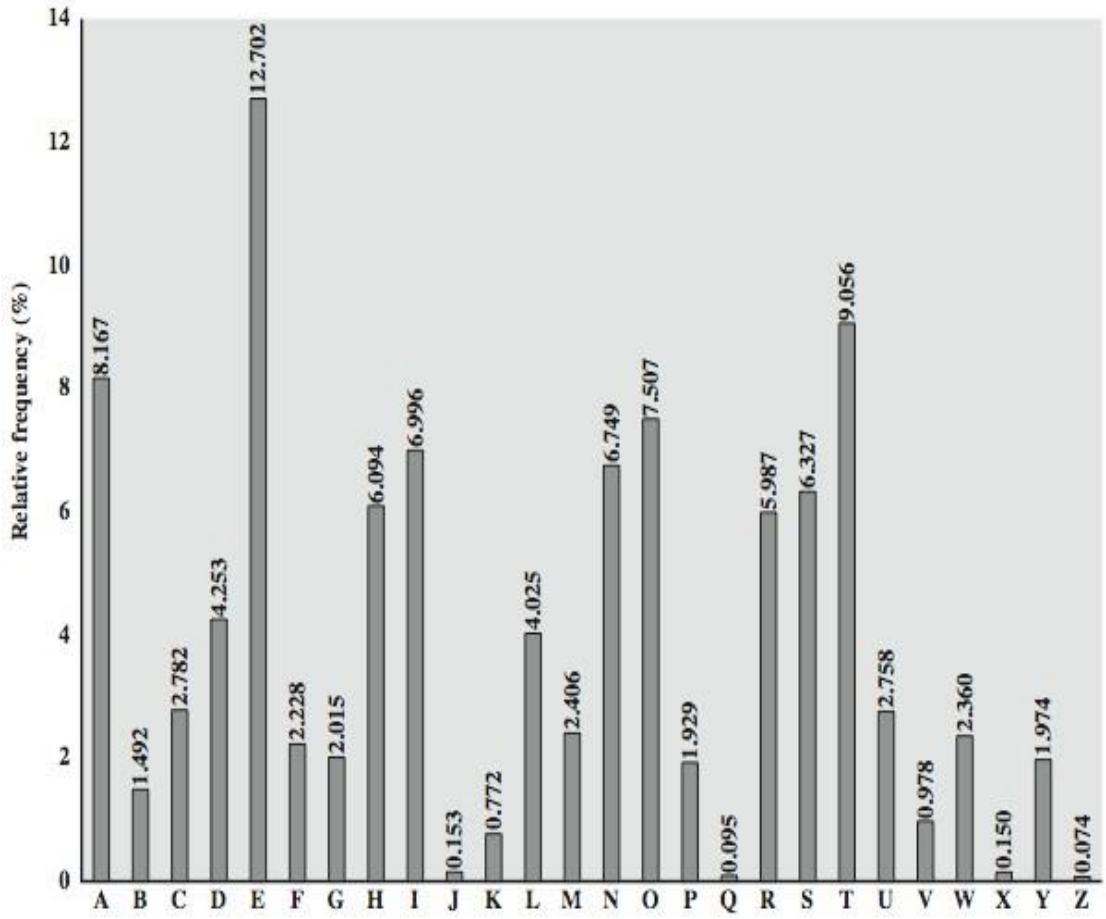
- mathematically give each letter a number

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 z0 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

- then have Caesar (rotation) cipher as: c = E(k, p) = (p + k) mod (26) p = D(k, c) = (c – k) mod (26)

Caesar and his army

English Letter Frequencies



- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- 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, N-O pair, R-S-T triple
troughs at: J-K, U-V-W-X-Y-Z

- for monoalphabetic must identify each letter
  - tables of common double/triple letters help (digrams and trigrams)

- amount of ciphertext is important – statistics!

- Example cryptanalysis

- given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies (see text)

- given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- guess P & Z are e and t

- guess ZW is th and hence ZWP is "the"

- proceeding with trial and error finally get:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Polyalbhabetic cipher

In a polyalphabetic cipher, the ciphertext corresponding to a particular character in the plaintext is not fixed.

Vignere Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1 k_2 ... k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse
- Attacker can deduce the key as it is repeated
- Example:
- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

key: deceptivedeceptivedeceptive

3 4 2 4 15 19 2 1 4

plaintext: wearediscoveredsaveyourself

ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Hint: shift w by 3 e by 4 a by 2....

Hill cipher

Invented by Lester Hill in 1929.

- Inputs : String of English letters, A,B,…,Z.
  An n□n matrix **K**, with entries drawn from 0,1,…,25.
  (The matrix **K** serves as the secret key.) □□Divide the input string into blocks of size n. □□Identify A=0, B=1, C=2, …, Z=25.
- Encryption: Multiply each block by **K** and then reduce mod 26.
- Decryption: multiply each block by the inverse of **K**, and reduce mod 26.
- c= p k
- $p=c_k-1$

  - **One-time pad**
  - Arbitrarily long, random and non-repeating sequence of character=key
  - called a One-Time pad (OTP)
  - In Vigenere cipher the same key is repeated which is susceptible to the attacker
  - But in one-time pad the key is not repeated
  - is unbreakable since ciphertext bears no statistical relationship to the plaintext
  - problems in key generation & safe distribution of key

8 (a) Whether Whatsapp chat is secured? If yes, explain how it is achieved. (10)
Yes, Whatsapp chat is secured.

WhatsApp's end-to-end encryption is available when you and the people you message use our app. Many messaging apps only encrypt messages between you and them, but WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages.