Chapter 3

Cryptography & Public Key Infrastructure

- **Cryptography**
  - It is derived from greek words: “Crypto” means “hidden” and “graphy” means “writing”.
  - So we can say cryptography is hidden writing or secret writing.

- **Plain text (Clear text):**
  - Plaintext is original message or normal information that can be understood by reading it. This message is confidential.

- **Cipher text:**
  - Plain text converted into unreadable form is called cipher text.
  - Cipher text is secure message that can’t be understood by attacker.

- **Encryption:**
  - Encryption is the process by which plaintext is converted into cipher text.

- **Secret key:**
  - The secret key is also input to the encryption algorithm.
  - Key is a set of numbers used for converting plain text to cipher text and cipher text to plain text.

- **Decryption:**
  - It is a reverse process of encryption at receiver end.
  - In it cipher text is converted into plain text using decryption algorithm.

- **Encryption and decryption algorithm combined known as cipher or cryptography system.**

- **Cryptanalysis:**
  - It is the process of trying to break the cipher text to get the original plain text.

3.1 Classification of Cryptography

- We can classify all cryptography algorithms into two groups:

- **Symmetric key (Private key Or Secret key) algorithm**

- **Asymmetric key (Public key) algorithm**

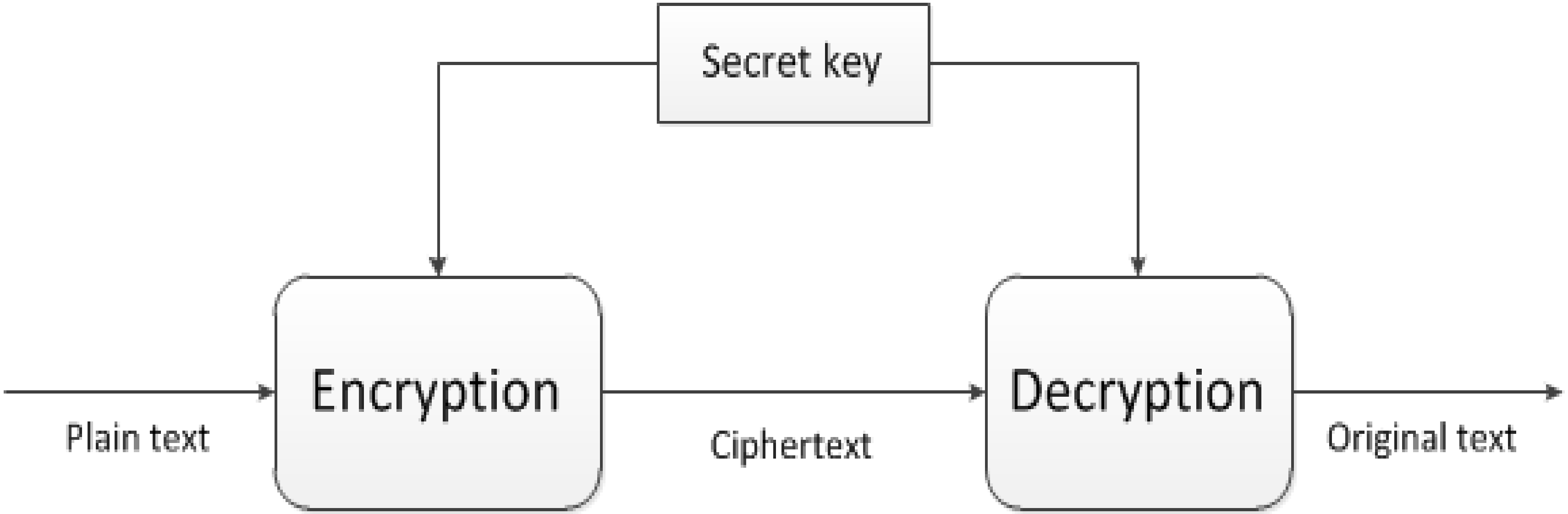
- Two basic requirements of encryption are:

  1) Encryption algorithm should be strong.

  2) The key shared by the sender and the receiver should be secret.

Symmetric Key Encryption

- Symmetric encryption is called as **private key** or **secret key** encryption.
- It is also referred to as conventional encryption or single-key encryption.
- In this one key is used for both encryption and decryption.
- Sender use same key for encrypting data and receiver use same key for decrypting data.



- Let us assume **X as plaintext** , **K as key** and **Y as cipher text** produced, Then we can write

Y = E(K, X)

Here **E** represents the **encryption algorithm** and is a function of plaintext X and key K.

- The receiver at the other ends decrypts the cipher text using the key.

X=D(K,Y)

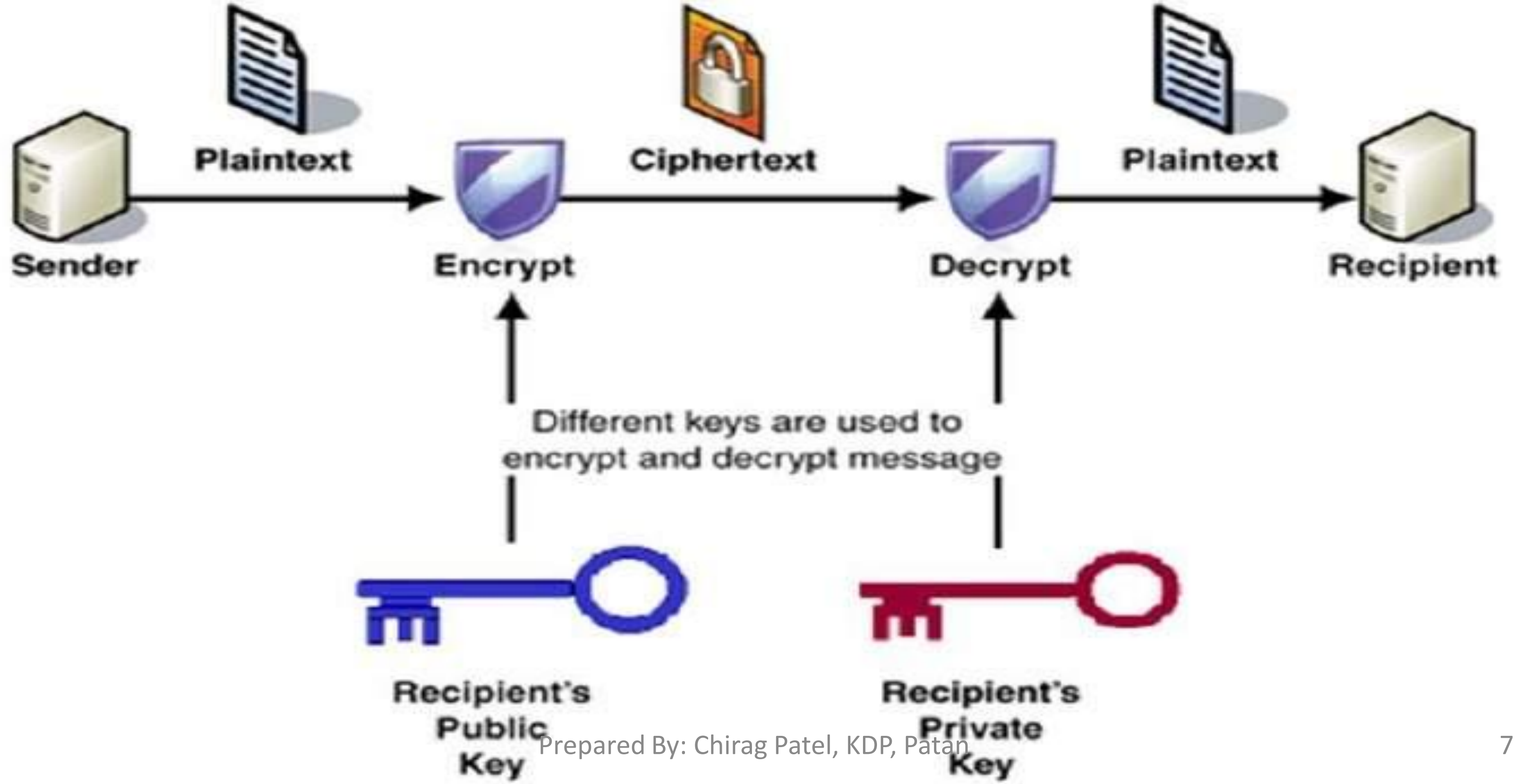
Here D represents the decryption algorithm and it reverse the process of encryption algorithm.

Example: Data Encryption Standard (DES)

- **Advantages:**
  - It takes less time compare to public key cryptography.
  - The key is smaller.

Asymmetric Key Encryption

- Asymmetric encryption also referred to as **public key encryption**.
- It uses two keys: **a public key** and a **private key**.
- **Public key is known by all** and **private key is for individual (receiver).**



- THE ESSENTIAL STEPS ARE THE FOLLOWING.

1. Each **user generates a pair of keys** to be used for the encryption and decryption of messages.
2. Each user **places public key in a public register**. The **other key is kept private** with user.
3. If A wishes to send a confidential message to B, A encrypts the message using B’s public key.
4. When B receives the message, it decrypts it using the private key. No other recipient can decrypt the message because only B knows B’s private key.
5. As long as a user’s private key remains protected and secret, incoming communication is secure.

- Suppose there is some **source A** that produces a message in **plaintext**, **X** and **sends it to B**.
- **B generates a related pair of keys**: **a public key, PUb**, and **a private key, PRb**. **PUb is publicly available** and therefore accessible by A.
- With the **message X** and the **encryption key PUb as input**, A forms the **cipher text Y** :

$$Y = E(PUb, X)$$

- The intended receiver, having the **matching private key**, is **able to decrypt the message:**

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

- Example: RSA algorithm, Digital Signature

Symmetric Cryptography	Asymmetric Cryptography
It uses same key(private key) for encryption and decryption.	It uses public key and private key for encryption and decryption.
It is also called as secret key or private key encryption.	It is also called as public key or two key encryption.
In it key must be known by sender and receiver.	In it only public key must be known by sender , private key kept with receiver only.
It cannot be used with digital signature.	It can be used with digital signature.
It is faster than Asymmetric cryptography.	It is slower than Symmetric cryptography.
Basic operation used in encryption, decryption are transposition and substitution.	It uses mathematical operation for encryption and decryption.
Example: DES	Example: RSA

Substitution Technique
3.2 (Encryption Algorithm)

- **Substitution Technique:**

A substitution technique is one in which the **letters of plaintext are replaced by other letters or by numbers or symbols**.

1. **Caesar Cipher**
2. **Playfair Cipher**
3. **Hill Cipher**
4. **Vigenere Cipher (Polyalphabetic Cipher)**
5. **Vernam Cipher**
6. **One Time Pad Cipher (Vermin Cipher)**

Caesar Cipher

- It is the **simplest technique found by Julius Caesar**.
- It is a **substitution cipher technique**.
- In this cipher, **each letter in the plaintext** is **replaced by a letter some fixed number position (Key) down the alphabet.**

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

- For Example with shift 3, A would be replaced by D & The alphabet is wrapped around so that Z follows A.
- Example:

  Plaintext: COMPUTER

  Ciphertext: FRPSXWHU

Caesar Cipher

- Here, the key is 3. If different key is used, different substitution will be obtained.
- Mathematically, starting from a=0, b=1 and so on, Caesar cipher can be written as:

$$E(P) = (P+ K) \text{ Mod } 26$$

$$D(C) = (C - k) \text{ Mod } 26$$

- Advantages:
  - It is easy to use.
  - It works fast
- Disadvantages:
  - There are only 26 possible keys.
  - Its too simple.
  - Brute force attack can be done easily on it.

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = kdpolytechnic KEY = 4
2. PT = computerdepartment KEY = 5
3. PT = digitalindia KEY = 6

Playfair Cipher

- It is also called as Playfair Square.
- It is a type of block cipher.
- It is best known method of multiple-letter encryption cipher.
- It uses two main processes:
- Step-1: Creation and Population of matrix:
- The playfair cipher

- The plaintext is encrypted **two letters at a time:**

  1) Break the plaintext into pairs of two consecutive letters.

  2) If a pair is a repeated letter, insert a filler like ‘X‘in the plaintext, eg. "balloon" is treated as "ba lx lo on“

  3) If in the last there is only one letter then insert X after it to make a pair.

  4) If both letters fall in the same row of the key matrix, replace each with the letter to its right (wrapping back to start from end), eg. “AR" encrypts as "RM"

  5) If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. “MU" encrypts to "CM“

  6) Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “HS" encrypts to "BP", and “EA" to "IM" or "JM" (as desired)

- If the plain text is YAGNIK then Cipher text is BNQYKE.
- If there is pair of XX then pad it Y.

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = Tall trees KEY = occurrence
2. PT = greet KEY = moonmission
3. PT = come to the window KEY = keyword
4. PT = cryptography KEY = security

Hill Cipher

- This cipher is based on linear algebra, Each letter is represented by numbers from 0 to 25 and calculations are done modulo 26.
- This encryption algorithm takes m successive plaintext letters and substitutes them with m cipher text letters.
- The substitution is determined by m linear equations. For m = 3, the system can be described as:

$$c1 = (k11p1 + k12p2 + k13p3)\text{mod } 26$$

$$c2 = (k21p1 + k22p2 + k23p3)\text{mod } 26$$

$$c3 = (k31p1 + k32p2 + k33p3)\text{mod } 26$$

- This can also be expressed in terms of row vectors and matrices, where C and P are row vectors of length 3 representing the plaintext and cipher text, and K is a3 X 3 matrix representing the encryption key.

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \text{ Mod } 26$$

- For example: If the PT= PAYMOREMONEY and if the key is given below ;

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

- Step :1 (CT for PAY)

  C = K (15 0 24) Mod 26

  = (11 13 18)

  = LNS

- Do the same for all pair that is MOR, EMO, NEY hence,

  CT = LNSHDLEWMTRW.

- Encryption and decryption can be given by the following formula,

  Encryption: C=P K Mod 26

  Decryption: P=C K^{-1} Mod 26

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = SUMMER KEY =

17	17	5
21	18	21
2	2	19

2. PT = WINTER KEY =

2	1	3
4	2	1
3	6	7

Polyalphabetic (Vigenere) Cipher

- This is a type of polyalphabetic substitution cipher which includes multiple substitutions depending on the key, In this the key determines which particular substitution is to be used.
- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.
- For Example if the PT = ATTACKATDAWN and Key = LEMON, but here the key is no long enough compare with PT so we repeat the key as depicted below;

PT = ATTACKATDAWN

KEY = LEMONLEMONLE

- For example, the first letter of the plaintext A is paired with L the first letter of the key, So use row L and column A of the Vigenère square, namely L. Similarly, The rest of the plaintext is enciphered in a similar fashion.

CT = LXFOPVEFRNHR

	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	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
b	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
c	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	B
d	D	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = Tall trees KEY = gtu
2. PT = moonmission KEY = greet

Vernam Cipher

- This cipher works on binary data (bits) rather than letters, The technique can be expressed as follows:

$$c_i = p_i \oplus k_i$$

where

pi = ith binary digit of plaintext

ci = ith binary digit of ciphertext

ki = ith binary digit of key

$\oplus$= XOR operation

- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

- Here the conversion from alphabets to binary is done with the reference of their ASCII Code. (for A=65,B=66,… & for a=97,b=98,….)

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = gtu KEY = otg
2. PT= computer KEY = you

One Time Pad (OTP) Cipher

- This cipher is implemented using random key that is as long as the message, the key is random so that cipher text is too random.
- The key is used to encrypt and decrypt a single message, and then is discarded (here in this method key is never be reused).
- Only two copies of key are generated, one for sender and one for receiver.
- Each new message requires a new key of the same length as the new message.
- The one-time pad is the only cryptosystem that exhibits **perfect secrecy**
- Encryption Process:
  - Add each corresponding letter of PT to the corresponding alphabets of OTP.
  - If the sum produced is greater than or equals to 26 then subtract 26 from it.
  - Translate each number of the sum back to corresponding alphabets ,this gives the output CT.

- Example:

PT = HOWAREYOU & OTP = NCBTZQARX

PT	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
+									
OTP	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
INTIAL TOTAL	20	16	23	19	42	20	24	31	43
SUBTRACT 26, IF <= 26	20	16	23	19	16	20	24	5	17
CT	**U**	**Q**	**X**	**T**	**Q**	**U**	**Y**	**F**	**R**

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = YAGNIK OTP = USGNIK
2. PT= computer OTP = departme

Transposition Techniques 3.3 (Encryption Algorithm)

- **Transposition Technique:**

  A Transposition technique is one in which perform some sort of permutation on the plain text letters.

1. Rail Fence.

Rail Fence

- In this technique encryption involves writing plaintext letters diagonally over a number of rows, then read off cipher row by row.
- For example, the text “meet me after the toga party” with a rail fence of depth 2, we write the following:

```
m   e   m   a   t   r   h   t   g   p   r   y
  e   t   e   f   e   t   e   o   a   a   t
```

- The Encrypted Message:

  MEMATRHTGPRYETEFETEOAAT
- This scheme is very easy to cryptanalyze as no key is involved.

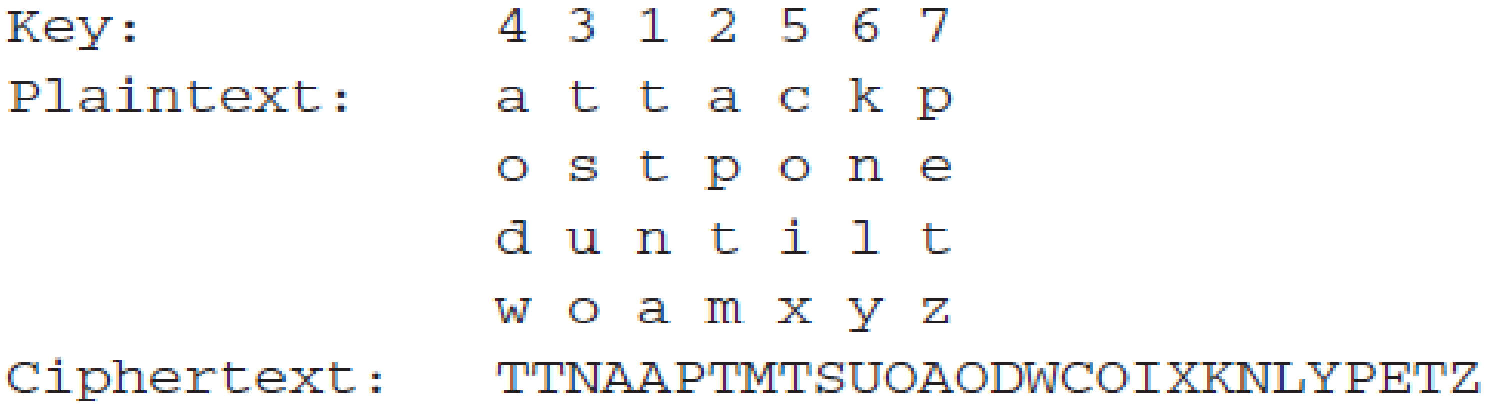
Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = gpcomuterdepartment
2. PT = porbandargujaratindia
3. PT= digitalindia

Rail Fence (Column cipher)

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm.
- For example,



```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Do It Your Self

- Find out the Cipher Text of the following Plain Text and keys.

1. PT = gpcomuterdepartment KEY = 34125
2. PT = prbandargujaratindia KEY = 6734512

Steganography

- The art and science of hiding information (it can be Plain Text, Cipher Text, Images , etc) by embedding messages within other is called Steganography.
- It is used when encryption is not permitted.
- It has three types (Ex. for Images)

1.LSB (Least Significant Bit)

It embeds data in the photo by replacing the least significant bit in BMP type picture.

2.DCT (Discrete Cosine Transform)

It works by Calculating the frequencies of the images and then replace some of them.

3.Append Algorithm

It appends the data to the end of the file as padding rather then hide the data in the photo by manipulating the picture.

3.4 Hashing

- Hashing is technique of obtain hash function which provides digital signature to the content.
- Some of the Application of the hash function are listed below,
  - Digital signature
  - Password hashing
  - Time Stamping
- Hash Function is one of the techniques that is used for Message authentication, Message Authentication verifies that received messages come from the legal source and have not been altered.
- Hash function maps a message of any length into a fixed-length hash value, which serves as the authenticator.

General Structure of Hash Function

- Generally, hash functions have a structure where a compression function (It produces output of size less than the input data) is repeated and such functions are referred to as iterated hash functions.
- In This Hash Function;

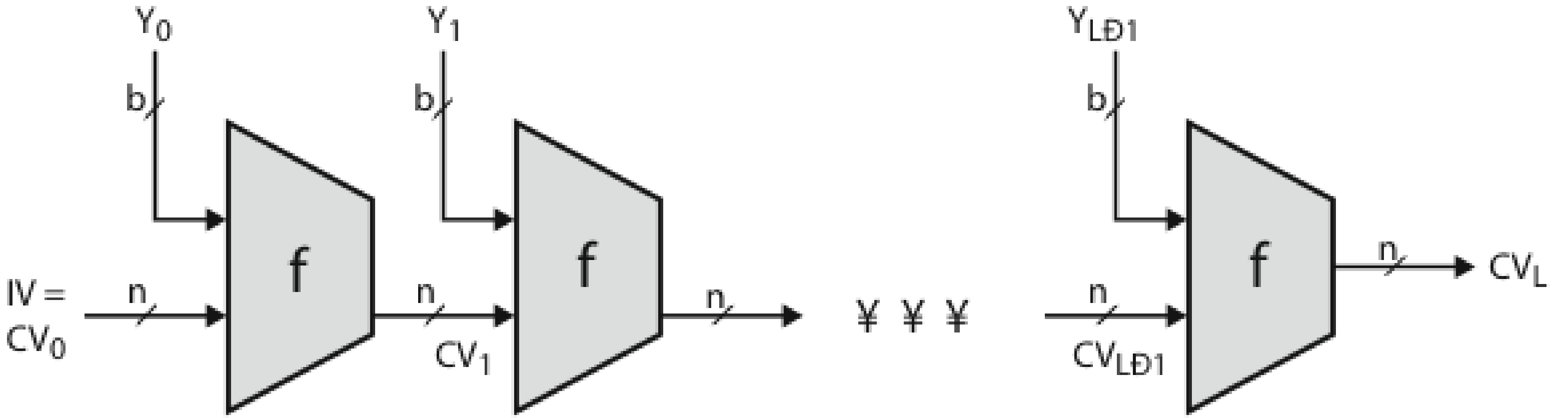
1.The input message is partitioned into L fixed-sized blocks of b bits each, If necessary, the final block is padded to b bits. The final block also includes the value of the total length of the input message.

2.The hash algorithm involves repeated use of a compression function, f, that takes two inputs And produces an n-bit output

3. At the start of hashing, the chaining variable has an initial value that is specified as part of the algorithm, The final value of the chaining variable is the hash value.

- The basic structure of Secure hash algorithm are depicted below,

- The basic structure of Secure hash algorithm are depicted below,



IV	=	Initial value	L	=	number of input blocks
CV_i	=	chaining variable	n	=	length of hash code
Y_i	=	ith input block	b	=	length of input block
f	=	compression algorithm			

SHA-1

- The algorithm takes as input a message of maximum length of less than 2^64 bits and produces a 160-bit message digest, The input is processed in 512-bit blocks.
- The Algorithm Step are listed below

1. Initialize variables

h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0
ml = message length in bits.

& Also initialize A 160-bit buffer is used to hold intermediate and final results of the hash function, The buffer can be represented as eight 32-bit registers (a, b, c, d, e).

2. Append padding bits.

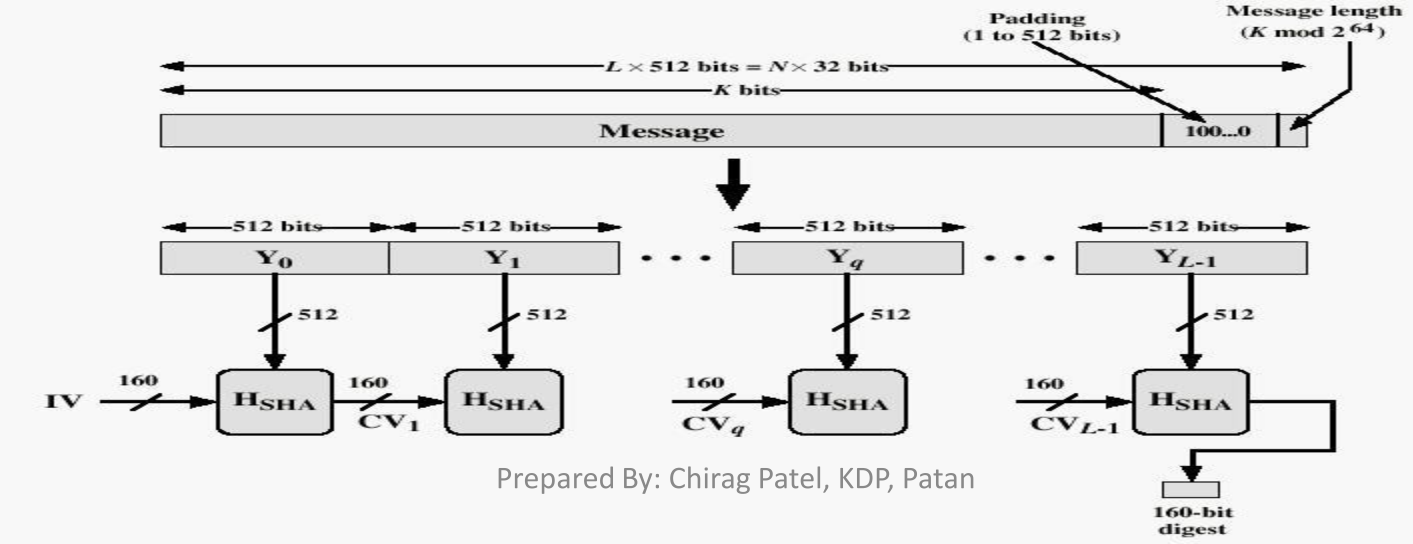
The message is padded so that its length is congruent to 448 (modulo 512) (length = 448 mod 512).

Pad the message with a single one followed by zeroes until the final block has 448 bits.

3. Append length.

A block of 64 bits is appended to the message. This block contains the length of the original message in binary (before the padding).The message is now an integer multiple of 512 bits in length.

In the figure below, expanded message is represented as the sequence of 512-bit blocks M1, M2,..., MN and the total length of the expanded message is N x 512 bits.



4. Process message in 512-bit (16-word) blocks.

➢ break message into 512-bit chunks

➢ **for** each chunk

```
        break chunk into sixteen 32-bit  words w[i], 0 ≤ i ≤ 15
```

➢ Extend the sixteen 32-bit words into eighty 32-bit words

```
    for i from 16 to 79
    w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) left rotate 1
```

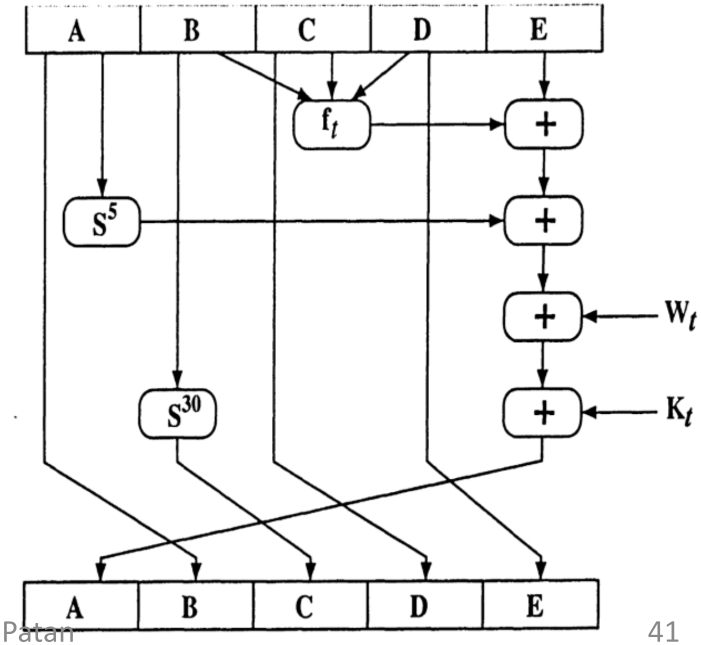
➢ Initialize hash value for this chunk

```
    a = h0
    b = h1
    c = h2
    d = h3
    e = h4
```

- Main Loop:

```
for i from 0 to 79
if 0 ≤ i ≤ 19
            then f = (b and c) or ((not b) and d)
            k = 0x5A827999
else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d) or (c and d)
            k = 0x8F1BBCDC
else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

a = (a leftrotate 5) + f + e + k + w[i]
b = a
c = b leftrotate 30
d = c
e = d
```



5. Add this chunk's hash to result so far.

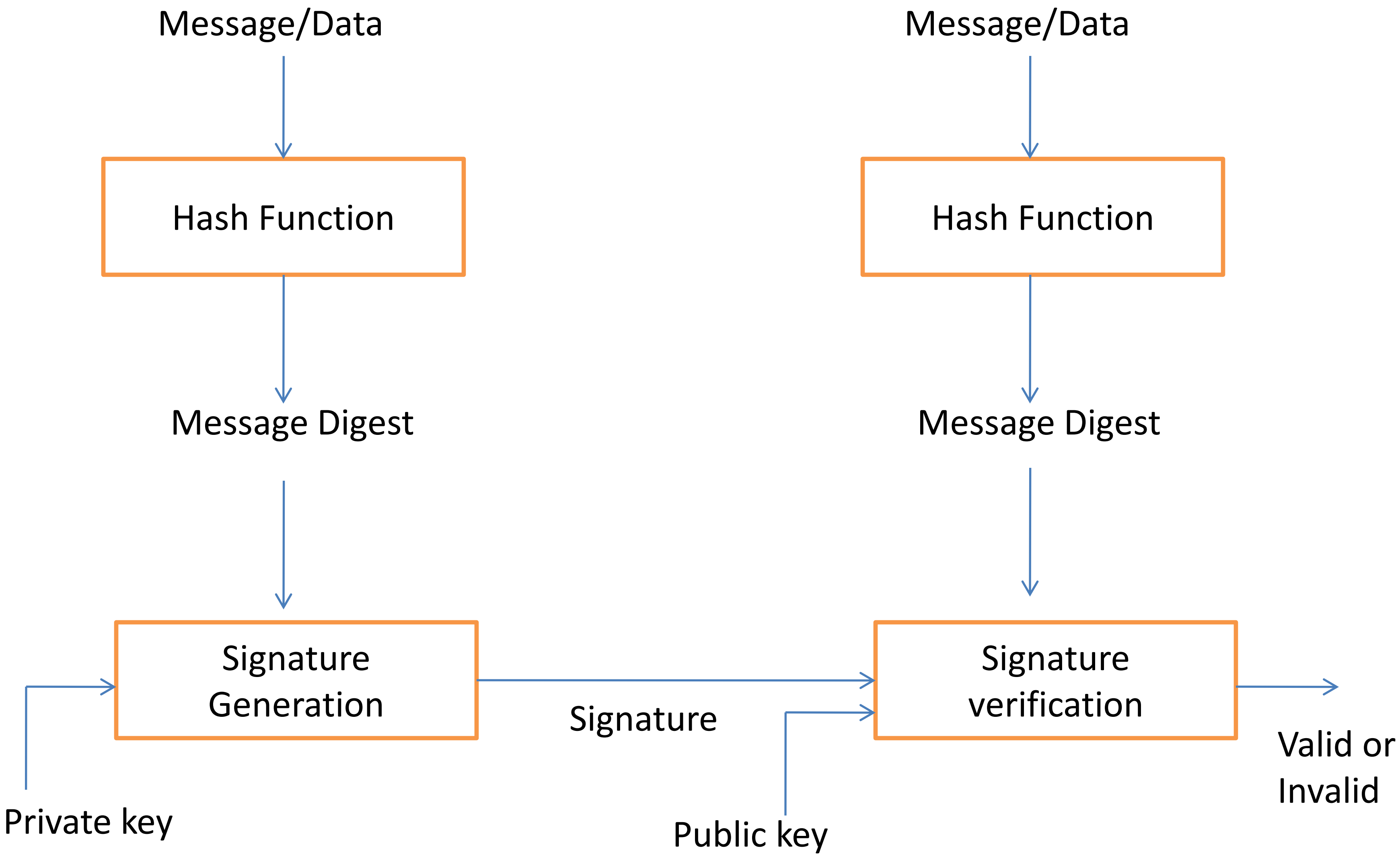
h0 = h0 + a
h1 = h1 + b
h2 = h2 + c
h3 = h3 + d
h4 = h4 + e

6.Produce the final hash value as a 160 bit number.

hh = (h0 left shift 128) or (h1 left shift 96) or (h2 left shift 64) or (h3 left shift 32) or h4

3.5 Digital Signature

- It is an electronic signature that can be used to authenticate the identity of a sender of a message or the signer of a document and possibly ensure that the original content of a message or document that has been sent is unchanged.
- The use of digital signature usually involves two processes, one performed by the signer (Digital Signature Creation) and the other by the receiver (digital Signature Verification) of the digital signature.
- This all Process is depicted below.



Message/Data
Hash Function
Message Digest
Signature Generation
Private key
Signature
Message/Data
Hash Function
Message Digest
Signature verification
Public key
Valid or Invalid

Key Escrow

- Key Escrow is a cryptographic key exchange process in which a key is held in a escrow (vault) or stored by the third party.
- It provide a backup source for cryptographic keys, but this system is somewhat risky because a third party is involved.
- The purpose of it is to serve as a backup if the parties with access to the cryptographic key loss the data.
- Example :

  Company A supplies software that Company B sells embedded in its hardware.

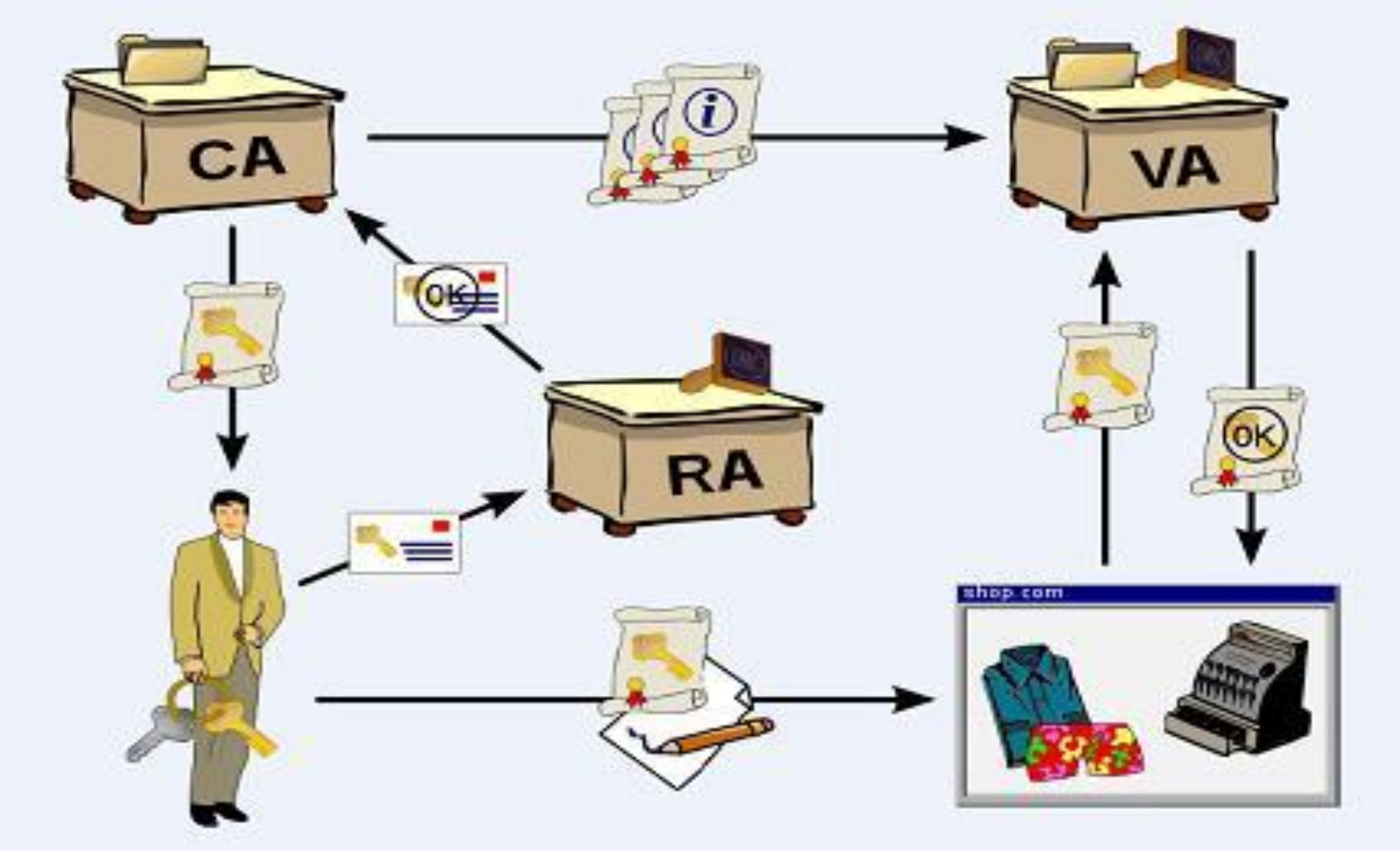
  Company B, worried that Company A may go out of business, So B requests that Company A place the source code for the software in Escrow.

  So as a authorized user of a software source code, company B can access that source code even if company A goes out of Business.

3.6 Public Key Infrastructure

- A **public key infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
- A public key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity.
- A **digital certificate (Public key certificate)** is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI)

- The figure is depicted below,



- A PKI consists of:

1. **Certificate Authority (CA)**

CA binds public keys with respective user identities, The user identity must be unique within each CA domain.

CA is an entity that issues digital certificates.

2. Registration Authority(RA)

It verifies the identity of users according to requesting information from the CA.

A **registration authority (RA)** is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.

3. **Central Directory**

A secure location in which to store and index keys.

4. **Certificate Management System**

which manage certificate.

5. **Certificate Policy**

Steps for Obtaining Digital Certificate

1. Application Phase

- In the application phase, the applicant will access the CA website to select customer type and class of certificate needed.
- After that, the applicant will be taken to online registration form.
- After verification of mandatory fields, the applicant will be given an opportunity to confirm the given details. The applicant will also print the displayed form to hand sign and send it across to the CA.
- The applicant will be shown the list of documents required with reference to category and the class of certificate chosen with payment details and also time period.

2. Authentication Phase

- In authentication phase, RA verifies and validates the information you provide in the online application and identification form.
- Upon approval of your application, RA will send you an email on the email address provided in the application form with a link for email id verification.

3. Retrieval Phase

- After email verification, receipt of documents and payment of fees, Reference Number will be sent through email whereas Authorization Code will be sent through registered A.D. on the postal address provided in the application form, Once you have received your retrieval email, you will be able to access your Digital Certificate.

3.7 Centralized &Decentralized Infrastructure

- The key pairs used in a PKI are generated using the two basic methods that are depicted below.
- In a Centralized Infrastructure, The key are generated and stored on a central server and are transmitted to the individual systems as needed.
  - ADVANTAGES : If a company uses a resource intensive algorithm to generate the public/private key pair and if the key sizes that are needed are large and resource intensive ,then the individual computers may not have the necessary processing power to produce the key on that case this infrastructure is useful.
- In a Decentralized Infrastructure, software's on individual computers generates and stores cryptographic keys local to the systems themselves.
  - DISADVANTAGES : Here all keys are stored in one place which is prime target for an attacker.

Private Key Protection

- When managing code(signing private keys),The following is recommended for the user.

1.Minimize Access to Private Keys

Computers with private keys should have minimal external connections. Minimize the number of users who have access to the private keys.

2.Use Physical Security to Protect Keys

Protect private keys with cryptographic hardware products that meet the minimum of Level 2 certified. Cryptographic hardware does not allow export of the private key to software where it could be attacked.

3.Test-Signing versus Release-Signing

This precaution helps ensure that test certificates are trusted only within the intended test environment.

3.8 Trust Model

- **Trust Model**

  A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

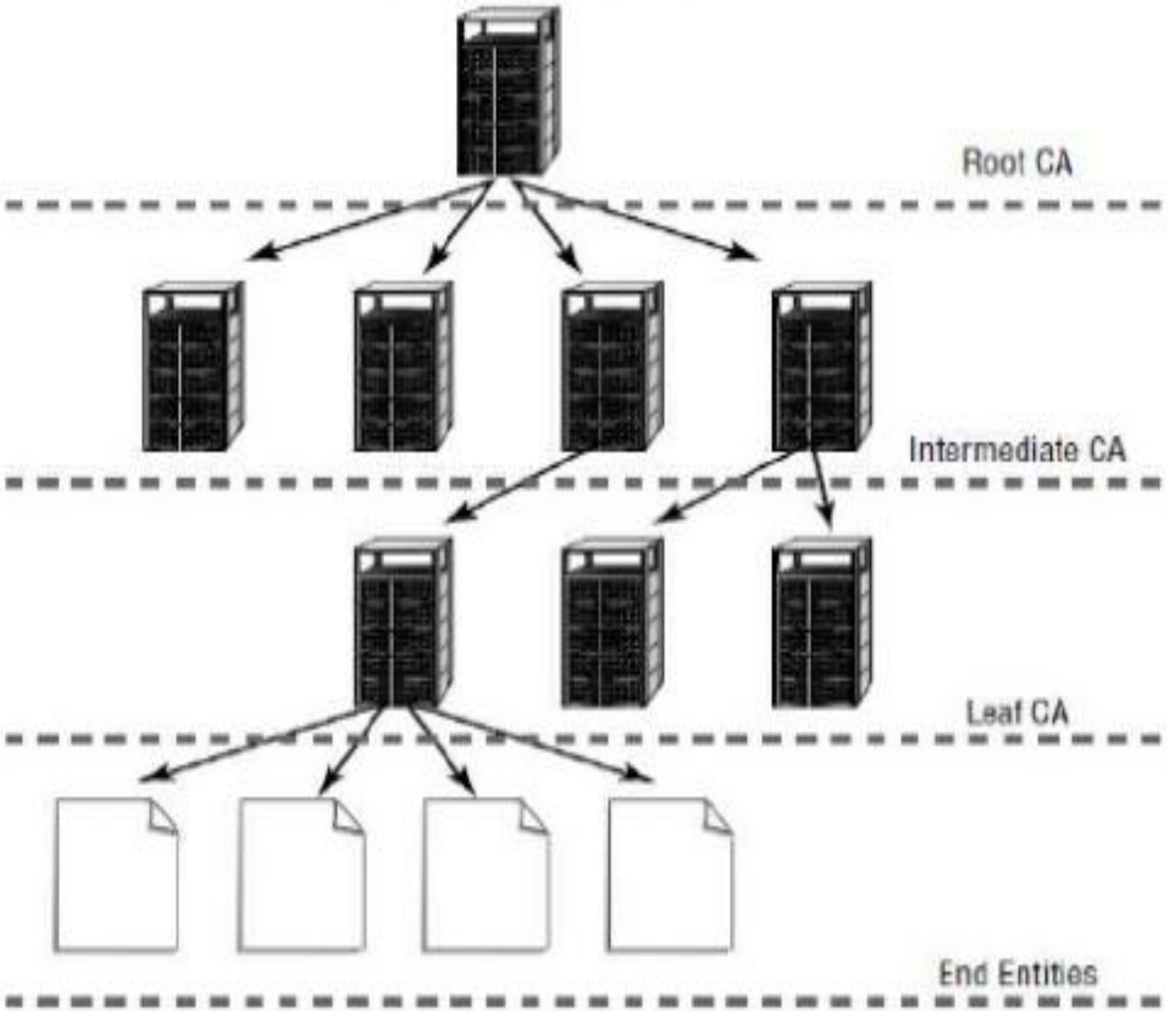
Three types of Trust Model

1. Hierarchical Model
2. Peer to Peer Model(Bridge Model)
3. Hybrid Model

Hierarchical Trust Model

- In a hierarchical trust model a root CA at the top provides all the information.
- The intermediate CAs are next in the hierarchy, and they only trust information provided by the root CA.
- The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren’t. This arrangement allows a high level of control at all levels of the hierarchical tree.

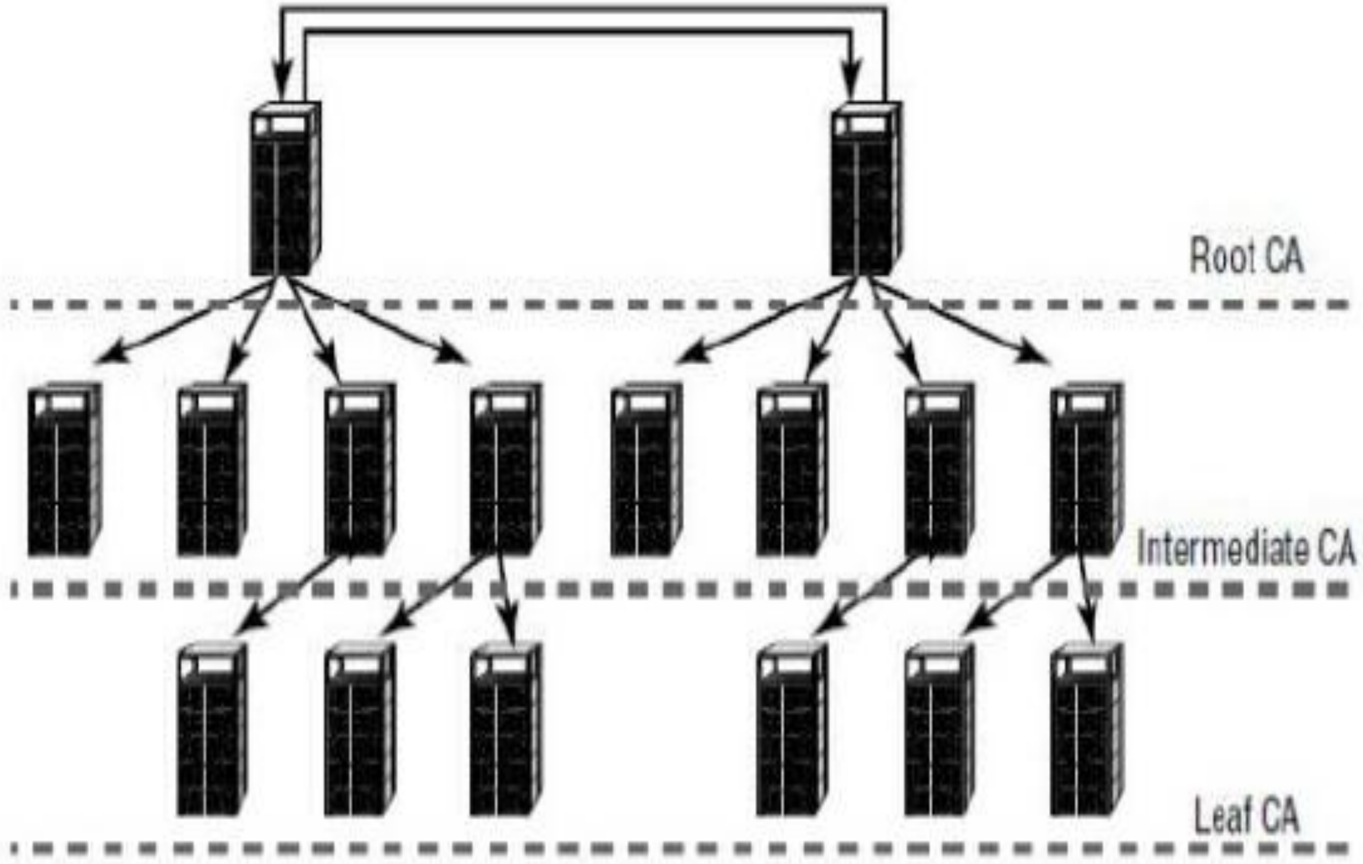
Hierarchical Trust Model



Bridge Model(Peer to Peer)

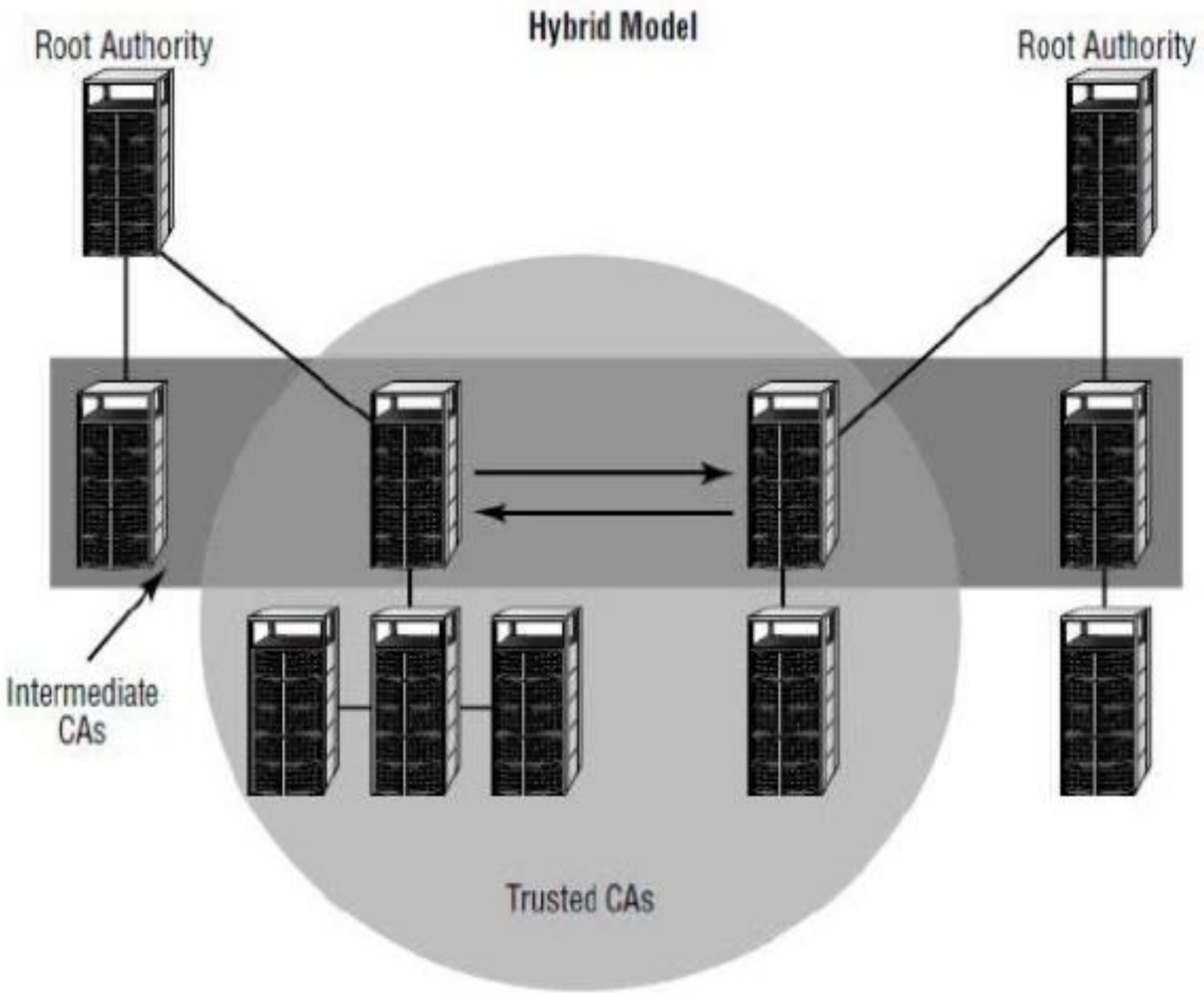
- In a bridge trust model, a peer-to-peer relationship exists between the root CAs, The root CAs can communicate with each other, allowing cross certification.
- This arrangement allows a certification process to be established between organizations or departments.
- Each intermediate CA trusts only the CAs above and below it, but the CA structure can be expanded without creating additional layers of CAs.
- This model may be useful if you’re dealing with a large, geographically dispersed organization or you have two organizations that are working together.
- In figure, the intermediate CAs communicate only with their respective root CA.
- Advantages:
  - Additional flexibility and interoperability between organizations.

Bridge Model



Hybrid Model

- A Hybrid Trust Model can use the capabilities of any or all of the trust model, hence you can be extremely flexible when you build a hybrid trust structure.
- Notice that in this structure, the single intermediate CA server on the right side of the illustration is the only server that is known by the CA below it.
- The subordinates of the middle-left CA are linked to the two CAs on its sides.
- These two CAs don’t know about the other CAs, because they are linked only to the CA that provides them a connection.
- The two intermediate servers in the middle of the illustration and their subordinates trust each other; they don’t trust others that aren’t in the link
- In our example, a user could accidentally be assigned to one of the CAs in the middle circle, As a member of that circle, the user could access certificate information that should be available only from their root CA.



Hybrid Model
Root Authority
Root Authority
Intermediate CAs
Trusted CAs

NO.	QUESTIONS	MARKS	YEAR					REMARKS
1	Define: Key Escrow.	2			2016			
	Write short note on: Key Escrow.	3				2017		
2	What is Cipher text?	2			2016			
3	Define: Ciphertext and Encryption.	2			2016			
4	Write a simple example for conversation of plain text in to cipher text using Caesar cipher.	2	2014		2016		2018	
	Explain Caesar cipher with example.	3		2015	2016		2018	
	Explain Caesar cipher Algorithm with example.	4		2015				
5	Write short note on one time pad with example. Or Write a short note on OTP. Or Explain vermin cipher(one time pad). Or Explain Vermin Cipher with Example.	3		2015	2016			
6	Convert given plain text in to cipher text using “one time pad cipher”. Plain Text = COMPUTER and Key is = MCDTZQBP.	3				2017		

7	To convert given plain text in to cipher text using vigenere cipher. Plain text is "GUJARAT UNIVERSITY" Key is " TECHNOLOGICAL".	3	2014				
8	Explain Public Key Infrastructure. Or Write a short note on PKI.	4			2016		2018
	Explain PKI briefly.	3				2017	
9	What is centralized infrastructure ? Write a limitation of it.	4	2014	2015			
10	List out different trust models. Explain any one model.	3				2017	
	Explain Trust models.	4			2016		
11	Explain Bridge trust model. Or Write a short note on bridge trust model.	3	2014		2016		
12	Explain Hierarchical Trust model.	4		2015			2018
13	Explain rail fence technique. Or Explain Rail Fence cipher with example. Or Explain Rail Fence Technique with Example	3		2015			
		4		2015	2016		2018
	How transposition techniques differ from substitution techniques? Give example of rail fence technique.	3				2017	
14	In Digital Signature which key is use for creation and verification process?	2		2015			
	Explain Digital signature. Or Explain Digital Signature.	3			2016		2018
		4		2015			2018
15	List out steps for obtaining Digital Signature.	4		2015			
16	Name four key steps in the creation of a digital certificate.	2				2017	
	Explain Steps to obtain Digital certificate.	3		2015			

17	How to use digital certificate?	3	2014				
18	Explain the role of a RA in creation of digital certificate.	3				2017	
19	Define Encryption. List out Symmetric Encryption Algorithm.	2		2015			
20	**Define Symmetric Encryption.**	**2**		**2015**			
21	Which key is use for encryption and decryption in Symmetric encryption Technique?	2		2015			
22	Draw and Explain Symmentric Encryption model.	3		2015			
23	Define symmetric and asymmetric encryption with neat figure. Or What is Cryptography? Explain Symmetric and Asymmetric cryptography with figure.	3			2016		
		7			**2016**		
24	Explain Asymmetric Encryption.	4		2015			2018
25	Difference between Symmetric encryption and Asymmetric encryption. Or Compare symmetric encryption with asymmetric encryption.	4	2014				
		2				2017	
26	Write a short note on conventional encryption model.	4			2016		
27	**Explain Play fare cipher with example.**	**7**	**2014**				**2018**
28	Find cipher text using Playfair cipher for given Plain text is “UNIVERSITY” and Key is “HELLO”.	4			2016		
29	Solve using Playfair cipher: Key: “PRIMROSE”, plaintext is: “hike the foothills”.	3			2016		
30	If Key = “computer”. Write playfair cipher key matrix.	3		2015			

31	If Key=COLGATE, Write Playfair Cipher Key Matrix.	3		2015			
32	**For given plain text=CRYPTOGRAPHY & Key=SECURITY find cipher text using Playfair cipher.**	**7**				**2017**	
33	Define Steganography.	2		2015			
34	Write a short note on steganography. Or Explain Steganography technique. Or Write a Short note on steganography.	3	2014	2015			
		4			2016		2018
35	Explain SHA-1 function in short. Or Give the brief explanation of SHA-1 function. Or Explain SHA-1 algorithm in short with block diagram.	4	2014		2016	2017	
36	What is Hashing?	2				2017	
37	Write down application of hash function.	2		2015			
38	Define: hash function. Draw block diagram of hash function.	3		2015			2018
39	Write Hill cipher algorithm and give example of it.	4				2017	

40	**Define poly alphabetic ciphers. List out its different methods. Find the ciphertext for the following using Hill cipher. For given plaintext is: ATT and Key is: 2 4 5 9 2 1 3 17 7**	**7**			**2016**		
41	**For given Plaintext=SUMMER, Key= 17 17 5 21 18 21 2 2 19 Find cipher text using hill cipher.**	**7**		**2015**			
42	**For Given Plaintext= WINTER, Key=2 1 3 4 2 1 3 6 7 Find Cipher Text using Hill Cipher.**	**7**		**2015**			
43	Explain private key protection.	3	2014				2018
		4		2015			
44	Define Cryptanalysis. List out various cryptanalysis attacks.	2			2016		2018
45	Which Algorithm is use for encrypt two character at time.	2		2015			
46	Define Decryption.	2		2015			2018
47	Define: Encryption and Decryption.	2	2014				2018
48	Explain Transposition technique	4	2014				2018