

Model For Network Security

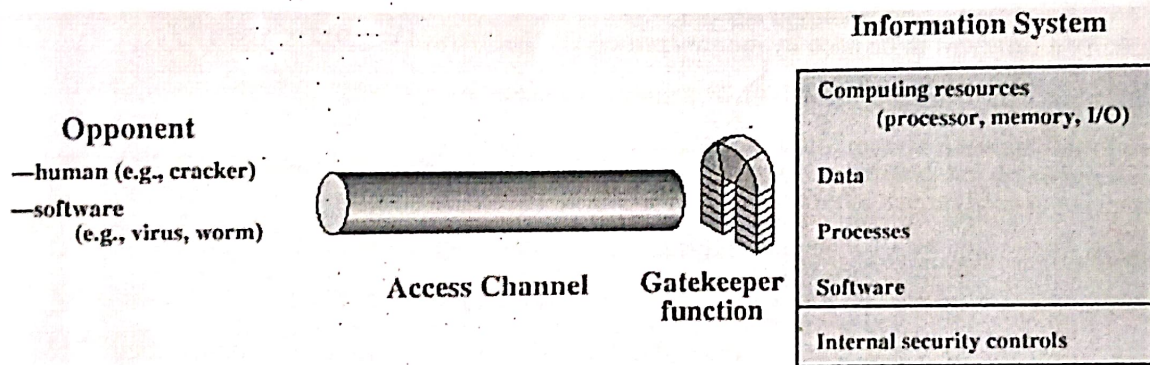
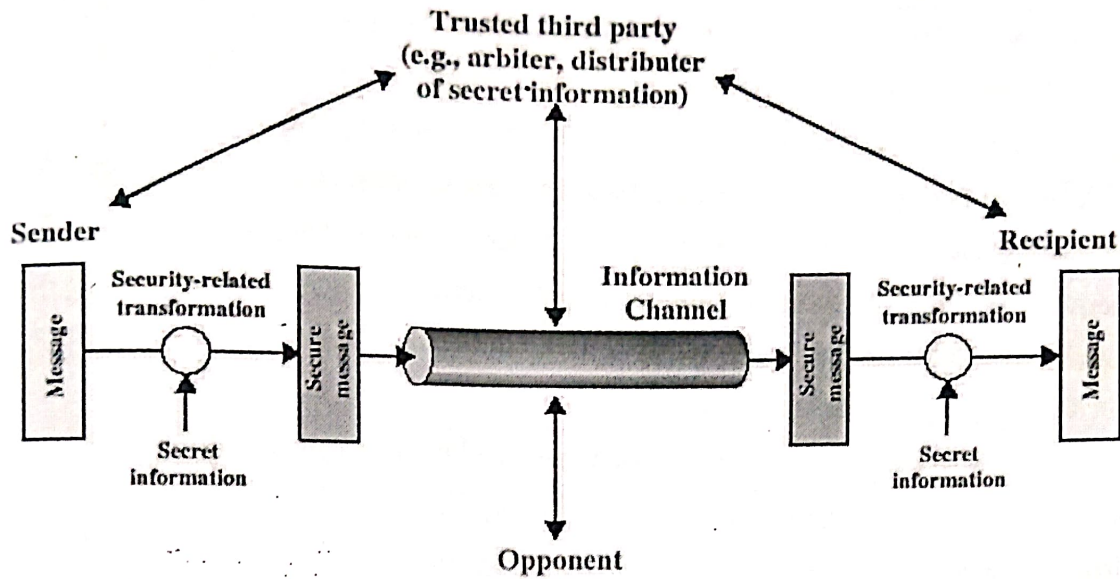


Figure 1.4 Network Access Security Model

(Data is transmitted over network between two communicating parties, who must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination by use of communication protocols by the two parties. Whenever an opponent presents a threat to confidentiality, authenticity of information, security aspects come into play. Two components are present in almost all the security providing techniques.

A security-related transformation on the information to be sent making it unreadable

①

by the opponent, and the addition of a code based on the contents of the message, used to verify the identity of sender.)

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. (An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception)

A trusted third party may be needed to achieve secure transmission. It is responsible for distributing the secret information to the two parties, while keeping it away from any opponent. It also may be needed to settle disputes between the two parties regarding authenticity of a message transmission. (The general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose

2. Generate the secret information to be used with the algorithm

3. Develop methods for the distribution and sharing of the secret information

4. Specify a protocol to be used by the two principals that makes use of the security

algorithm and the secret information) to achieve a particular security service various other threats to information system like unwanted access still exist.

~~and the application of a particular cryptographic system of authentication is not sufficient for the effective~~
Information access threats intercept or modify data on behalf of users who should not have

access to that data Service threats exploit service flaws in computers to inhibit use by legitimate users Viruses and worms are two examples of software attacks inserted into the system by means of a disk or also across the network. The security mechanisms needed to cope with unwanted access fall into two broad categories.

Some basic terminologies used

1. CIPHER TEXT - the coded message
2. CIPHER - algorithm for transforming plaintext to cipher text
3. KEY - info used in cipher known only to sender/receiver
4. ENCIPHER (ENCRYPT) - converting plaintext to cipher text
5. ECIPHER (DECRYPT) - recovering cipher text from plaintext
6. CRYPTOGRAPHY - study of encryption principles/methods
7. CRYPTANALYSIS (CODEBREAKING) - the study of principles/ methods of deciphering cipher text *without* knowing key
8. CRYPTOLOGY - the field of both cryptography and cryptanalysis)

Cryptography

Cryptographic systems are generally classified along 3 independent dimensions:

Type of operations used for transforming plain text to cipher text:

All the encryption algorithms are a based on two general principles: **substitution**, in which each element in the plaintext is mapped into another element, and **transposition**, in which elements in the plaintext are rearranged.

Classical Encryption Techniques

There are two basic building blocks of all encryption techniques: substitution and transposition.

Substitution Techniques

In which each element in the plaintext is mapped into another element.

1. Caesar Cipher
2. Monoalphabetic cipher
3. Playfair Cipher
4. Hill Cipher
5. Polyalphabetic Cipher
6. One Time Pad

Caesar Cipher

It is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the cipher text. It is a simplest form of substitution cipher scheme.

This cryptosystem is generally referred to as the **Shift Cipher**. The concept is to replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25.

For this type of scheme, both sender and receiver agree on a 'secret shift number' for shifting the alphabet. This number which is between 0 and 25 becomes the key of encryption.

The name 'Caesar Cipher' is occasionally used to describe the Shift Cipher when the 'shift of three' is used.

Process of Shift Cipher

- In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
- The plaintext letter is then encrypted to the cipher text letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext 'tutorial' is encrypted to the cipher text 'WXWRULDO'. Here is the cipher text alphabet for a Shift of 3 –

Plaintext Alphabet	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
Ciphertext Alphabet	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

- On receiving the cipher text, the receiver who also knows the secret shift, positions his sliding ruler underneath the cipher text alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
- He then replaces the cipher text letter by the plaintext letter on the sliding ruler underneath. Hence the cipher text 'WXWRULDO' is decrypted to 'tutorial'. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown below –

Ciphertext Alphabet	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
Plaintext Alphabet	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

Security Value

Caesar Cipher is **not** a secure cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

Simple Substitution Cipher

It is an improvement to the Caesar Cipher. Instead of shifting the alphabets by some number, this scheme uses some permutation of the letters in alphabet.

For example, A.B.....Y.Z and Z.Y.....B.A are two obvious permutation of all the letters in alphabet. Permutation is nothing but a jumbled up set of alphabets.

With 26 letters in alphabet, the possible permutations are $26!$ (Factorial of 26) which is equal to 4×10^{26} . The sender and the receiver may choose any one of these possible permutation as a cipher text alphabet. This permutation is the secret key of the scheme.

the Simple Substitution Cipher has a simple design and it is prone to design flaws, say choosing obvious permutation, this cryptosystem can be easily broken.

Monoalphabetic and Polyalphabetic Cipher

(Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalysis.

Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, **playfair** and **Vigenere Cipher** are **polyalphabetic ciphers**.)

(Playfair Cipher

In this scheme, pairs of letters are encrypted, instead of single letters) as in the case of simple substitution cipher.

(In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

The sender and the receiver decide on a particular key, say 'tutorials'. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be –

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

Process of Playfair Cipher

- First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message "hide money". It will be written as –

HI D E M O N E Y Z

- The rules of encryption are –
 - If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)

T U O R I

A L S B C

D E F G H 'H' and 'I' are in same column, hence take letter below them to replace.

HI → QC

K M N P Q

V W X Y Z

- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

T U O R I

A L S B C

D E F G H 'D' and 'E' are in same row, hence take letter to the right of them to replace. DE → EF

K M N P Q

V W X Y Z

- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

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

'M' and 'O' nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row
MO -> NU

Using these rules, the result of the encryption of 'hide money' with the key of 'tutorials' would be -

QC EF NU MF ZV

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Security Value

It is also a substitution cipher and is difficult to break compared to the simple substitution cipher. As in case of substitution cipher, cryptanalysis is possible on the Playfair cipher as well, however it would be against 625 possible pairs of letters (25x25 alphabets) instead of 26 different possible alphabets.

The Playfair cipher was used mainly to protect important, yet non-critical secrets, as it is quick to use and requires no special equipment.

Vigenere Cipher

which is then used for doing a



Steganography

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g., (i) the sequence of first letters of each word of the overall message spells out the real (hidden) message. (ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are:

- **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.
- **Invisible ink** – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures** – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.)
- ✱ **Typewritten correction ribbon** – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of Steganography

- Requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless.)

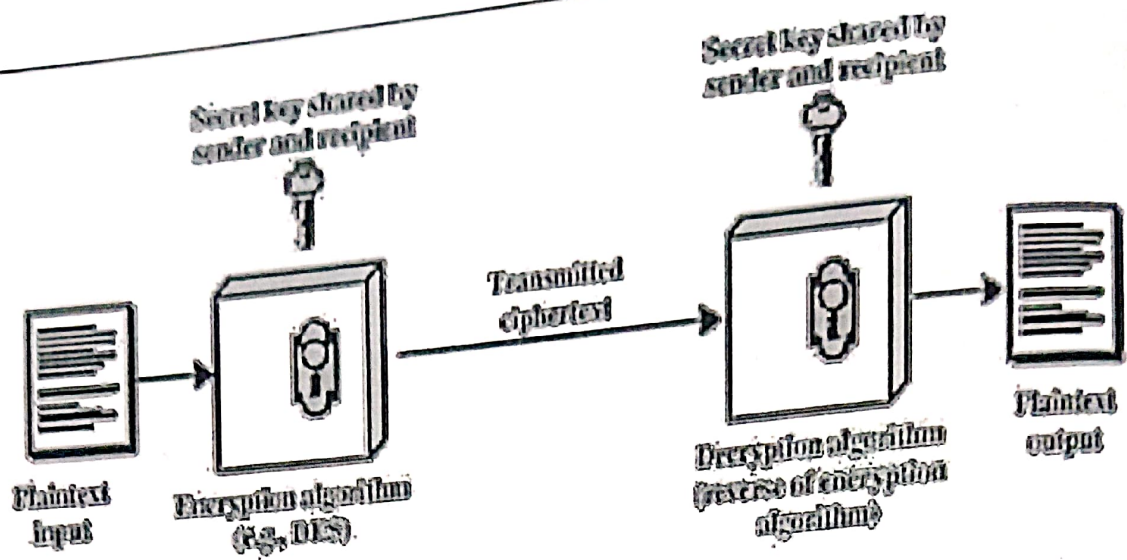
Asymmetric Key Ciphers: Principles of Public Key Cryptosystems, Algorithms (RSA, Diffie-Hellman, ECC), Key Distribution.

Conventional Encryption Principles

Key components of encryption

A Conventional/Symmetric encryption scheme has five ingredients:

1. **Plain Text:** This is the original message or data which is fed into the algorithm as input.
2. **Encryption Algorithm:** This encryption algorithm performs various substitutions and transformations on the plain text.
3. **Secret Key:** The key is another input to the algorithm. The substitutions and transformations performed by algorithm depend on the key.
4. **Cipher Text:** This is the scrambled (unreadable) message which is output of the encryption algorithm. This cipher text is dependent on plaintext and secret key. For a given plaintext, two different keys produce two different cipher texts.
5. **Decryption Algorithm:** This is the reverse of encryption algorithm. It takes the cipher text and secret key as inputs and outputs the plain text.



Simplified Model of Conventional Encryption

The important point is that the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm i.e. it is not necessary to keep the algorithm secret, but only the key is to be kept secret. This feature that algorithm need not be kept secret made it feasible for wide spread use and enabled manufacturers develop low cost chip implementation of data encryption algorithms. With the use of conventional algorithm, the principal security problem is maintaining the secrecy of the key.)

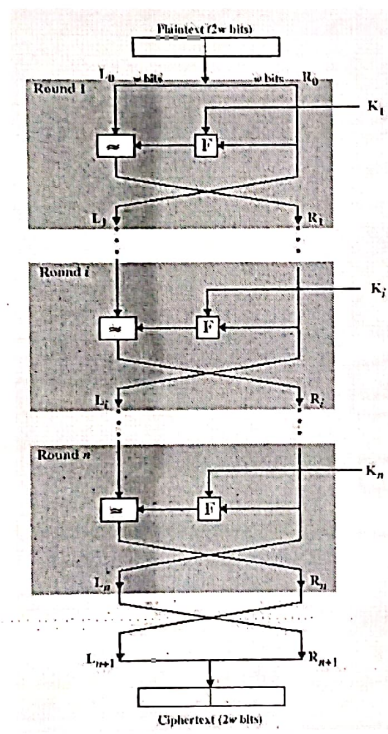
Feistel Cipher Structure

The input to the encryption algorithm are a plaintext block of length $2w$ bits and a key K . the plaintext block is divided into two halves L_0 and R_0 . The two halves of the data pass through „ n “ rounds of processing and then combine to produce the cipher text block. Each round „ i “ has inputs L_{i-1} and R_{i-1} , derived from the previous round, as well as the subkey K_i , derived from the overall key K . in general, the subkeys K_i are different from K and from each other.

All rounds have the same structure. A substitution is performed on the left half of the data (as similar to S-DES). This is done by applying a round function F to the right half

of the data and then taking the XOR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round subkey k_i . Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution-permutation network. The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- **Block size** - Increasing size improves security, but slows cipher
- **Key size** - Increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **Number of rounds** - Increasing number improves security, but slows cipher
- **Subkey generation** - Greater complexity can make analysis harder, but slows cipher
- **Round function** - Greater complexity can make analysis harder, but slows cipher
- **Fast software en/decryption & ease of analysis** - re more recent concerns for practical use and testing



Public Key Cryptography

(The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. It is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key.) Public key schemes are neither more nor less secure than private key (security depends on the key size for both). Public-key cryptography *complements rather than replaces* symmetric cryptography. Both also have issues with key distribution, requiring the use

of some suitable protocol. The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption:

1.) *key distribution* – how to have secure communications in general without having to trust a KDC with your key

2.) *digital signatures* – how to verify a message comes intact from the claimed sender

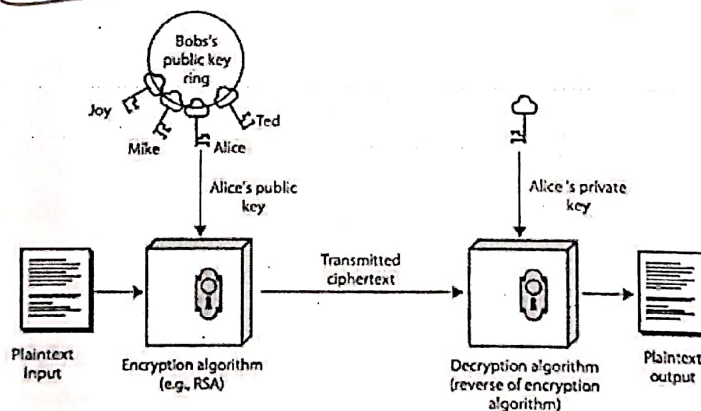
Public-key/two-key/asymmetric cryptography involves the use of two keys:

- a *public-key*, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
- a *private-key*, known only to the recipient, used to **decrypt messages**, and **sign (create) signatures**.
- is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Public-Key algorithms rely on one key for encryption and different but related key for decryption. These algorithms have the following important characteristics:

- it is computationally infeasible to find decryption key knowing only algorithm & encryption key
- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms like RSA)

The following figure illustrates public-key encryption process and shows that a public-key encryption scheme has six ingredients: plaintext, encryption algorithm, public & private keys, cipher text & decryption algorithm.



The essential steps involved in a public-key encryption scheme are given below:

- 1.) Each user generates a pair of keys to be used for encryption and decryption.
- 2.) Each user places one of the two keys in a public register and the other key is kept private.
- 3.) If B wants to send a confidential message to A, B encrypts the message using A's public key.
- 4.) When A receives the message, she decrypts it using her private key. Nobody else can decrypt the message because that can only be done using A's private key (Deducing a private key should be infeasible).

Applications For Public-Key Cryptosystems:

- 1.) **Encryption/decryption:** sender encrypts the message with the receiver's public key.
- 2.) **Digital signature:** sender "signs" the message (or a representative part of the message) using his private key
- 3.) **Key exchange:** two sides cooperate to exchange a secret key for later use in a secret-key cryptosystem.

TLS :- Transport layer security } Security
SSL :- Secure Sockets layer } protocols.
NAME: _____
DATE: ____/____/____

Use of Public Key Cryptography:-

TLS/SSL uses public key cryptography to keep our internet connections secure.

① Encryption :- When you visit a secure website (HTTPS), TLS/SSL helps encrypt data exchanged between your browser & the website's server.

Your browser & server agree on a secret key for this session, which keeps your data safe from eavesdroppers.

② Authentication :- TLS/SSL verifies the identity of websites. When you connect to a site, it presents a digital ~~signature~~ certificate signed by a trusted authority.

Your browser checks this certificate to ensure you are really connecting to the right site & not a fake one trying to steal your information.

Components of Public Key Encryption:-

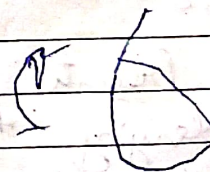
- ① Plaintext:- This is the message which is readable / understandable. This message is given to the encryption algorithm as an input.
- ② Ciphertext:- is produced as an o/p of encryption algorithm. It is unreadable.
- ③ Encryption Algorithm:- used to convert plaintext to ciphertext.
- ④ Decryption Algorithm:- It takes the ciphertext as i/p & the matching key (Private key or Public key) & produces the original plaintext.
- ⑤ Public key & Private key:- One key is Public Key - known to everyone & is used for encryption. One key is Private key (Secret key) & is used for decryption.

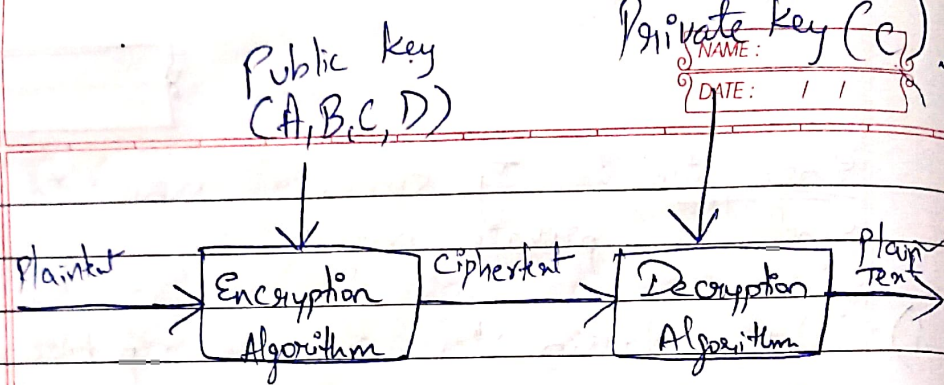
Encryption:- If someone wants to send a private msg:

- i) They obtain the recipient's public key.
- ii) They encrypt the msg using that public key.
- iii) The encrypted msg is sent over a net.

Decryption:- Upon receiving the msg:

- The receiver uses their private key to decrypt the message & recover the original plaintext.





* Applications of Public Key Cryptosystems:-

- ① Digital Signatures:- Proves who sent a file or document & guarantees the data was not changed in transit.
- ② Code signing:- Validates software updates & application publishers like Microsoft or Apple to ensure programs have not been modified by hackers.
- ③ Non-Repudiation:- Prevents a sender from falsely denying they approved or sent a digitally signed document.

- NAME: _____
DATE: / /
- ④ Blockchain Wallets:- Public keys act as visible account numbers or addresses, while matching private keys authorize fund transfers & verify ownership.

* RSA (Rivest ; Shamir & Adleman) Algorithm:-

- RSA algorithm is an asymmetric or public-key cryptography algorithm, which means it works on two different keys.
- Public key (K_P) is used for encryption & is known to everyone.
- Private key (K_R) is used for decryption & must be kept secret by the receiver.
Ex:- If person A wants to send a message securely to person B:
- Person A encrypts the message using Person B's Public key.
- Person B decrypts the message using their Private key.

* RSA Algorithm:-

- It is based on factorization of large number & modular arithmetic for encryption & decryption of data.
- It consists of three main stages:-
 - i) Key Generation : Creating Public & Private Keys.
 - ii) Encryption : Sender encrypts the data using public key to get ciphertext.
 - iii) Decryption : Decrypting the ciphertext using Private Key to get the original data.

1. Key Generation:-

- Each user selects two large primes at random - p, q .
- Calculate the product of primes, $n = p * q$. This product is part of the public as well as the private key.
- Calculate Euler Totient Function $\phi(n)$, where $\phi(n) = (p-1)(q-1)$.
- Selecting at random the encryption key e , where $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
i.e. e should be co-prime with $\phi(n)$.
- Calculate decryption exponent d , such that

$$(d * e) \equiv 1 \pmod{\phi(n)},$$
 i.e. d is modular multiplicative inverse of $e \pmod{\phi(n)}$.

Finally, Public Key $KU = (n, e)$.

Private Key $KR = (n, d)$.

2. Encryption:-

- To encrypt a message 'M', it is first converted to numerical representation using ASCII and other encoding schemes.
- Now, use the following formula to generate ciphertext using public key (n, e) :-

$$C = M^e \bmod n$$

$$C = M^e \bmod n = (\dots)$$

3. Decryption:-

To decrypt the cipher text C , use the private key (n, d) & get the original data using the formula:

$$M = C^d \bmod n$$

Example:-

Step 1:-

- Select two prime numbers: Let $p = 3$ and $q = 11$.

- Calculate n :

$$\begin{aligned} n &= p \times q \\ &= 3 \times 11 \\ &= 33. \end{aligned}$$

- Calculate the Totient $\phi(n)$: Find the count of numbers coprime to 'n'.

$$\begin{aligned} \phi(n) &= (p-1)(q-1) = (3-1) \times (11-1) \\ \phi(n) &= 2 \times 10 \\ \phi(n) &= 20. \end{aligned}$$

- Select e :- $\gcd(e, 20) = 1$.
 e should be coprime to n i.e. they share no common factors besides 1.
Let $e = 3$ (since 3 & 20 have no common factors).

- Calculate d :- Find a number where $(d \times e) \pmod{\phi(n)} = 1$.

We need $(d \times 3) \pmod{20} = 1$.

If we test values, $d=7$ works because

$$7 \times 3 = 21$$

$$\& \quad 21 \pmod{20} = 1.$$

- Therefore we get :-

Public Key $(n, e) = (33, 3)$

$\&$ Private Key $(n, d) = (33, 7)$

$\Rightarrow$ Step 2:- Encryption
Consider message to be sent $M=5$.

Using Public Key $(33, 3)$ we generate the ciphertext as:

$$C = m^e \pmod{n}$$

$$C = 5^3 \pmod{33}$$

$$= 125 \pmod{33}$$

$$= 26$$

$\therefore$ Ciphertext 26 is sent over the net.

$\Rightarrow$ Step 3 :- Decryption
Use private key $(7, 33)$ & the decryption formula:

$$d \cdot m \equiv c^d \pmod{n}$$

$$m = 26^7 \pmod{33}$$

$$= 896 \pmod{33}$$

$$= 5.$$

Solve for $p=5$ & $q=11$.

* RSA Security:-

1. Use strong key sizes (2048-bit or higher):-

RSA security depends on the key size. Larger keys are much harder to break.

- Minimum recommended size: 2048 bits
- For highly sensitive data: 3072 or even 4096 bits is better.

2. Rotate & Regenerate keys regularly:-
Even strong keys can become a risk over time.

Key rotation means generating new keys after a period of use.

3. Use Secure Random Number Generators (RNG)

- RSA keys are generated using random numbers, especially the prime numbers p & q .

- Weak or predictable RNGs can lead to repeated or weak keys, making them easier to break.

- Always use a cryptographically secure pseudo-random number generator (CSPRNG).

4. Asymmetric Encryption:- Public keys encrypt information or verify signatures, while private keys decrypt information or sign data.

5. Prime Factorization:- The mathematical backbone of RSA encryption relies on the extreme difficulty of factoring the product of two massive prime numbers.

Steganography

Steganography (is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the Greek words *steganos* (στεγανός), meaning "covered, concealed, or protected," and *graphein* (γράφειν) meaning "writing".

Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.^[1]

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.^[2]

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Digital text

1. Making text the same color as the background in word processor documents, e-mails, and forum posts.
2. Using Unicode characters that look like the standard ASCII character set. On most systems, there is no visual difference from ordinary text. Some systems may display the fonts differently, and the extra information would then be easily spotted, of course.
3. Using hidden (control) characters, and redundant use of markup (e.g., empty bold, underline or italics) to embed information within HTML, which is visible by examining the document source. HTML pages can contain code for extra blank spaces and tabs at the end of lines, and colours, fonts and sizes, which are not visible when displayed.
4. Using non-printing Unicode characters Zero-Width Joiner (ZWJ) and Zero-Width Non-Joiner (ZWNJ).^[3] These characters are used for joining and disjoining letters in Arabic and Persian, but can be used in Roman alphabets for hiding information because they have no meaning in Roman alphabets: because they are "zero-width" they are not displayed. ZWJ and ZWNJ can represent "1" and "0".
4. Embedding a secret message in the pattern of deliberate errors and marked corrections in a word processing document, using the word processor's change tracking feature.^[10]

Social steganography

In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers.^[11] Examples include: