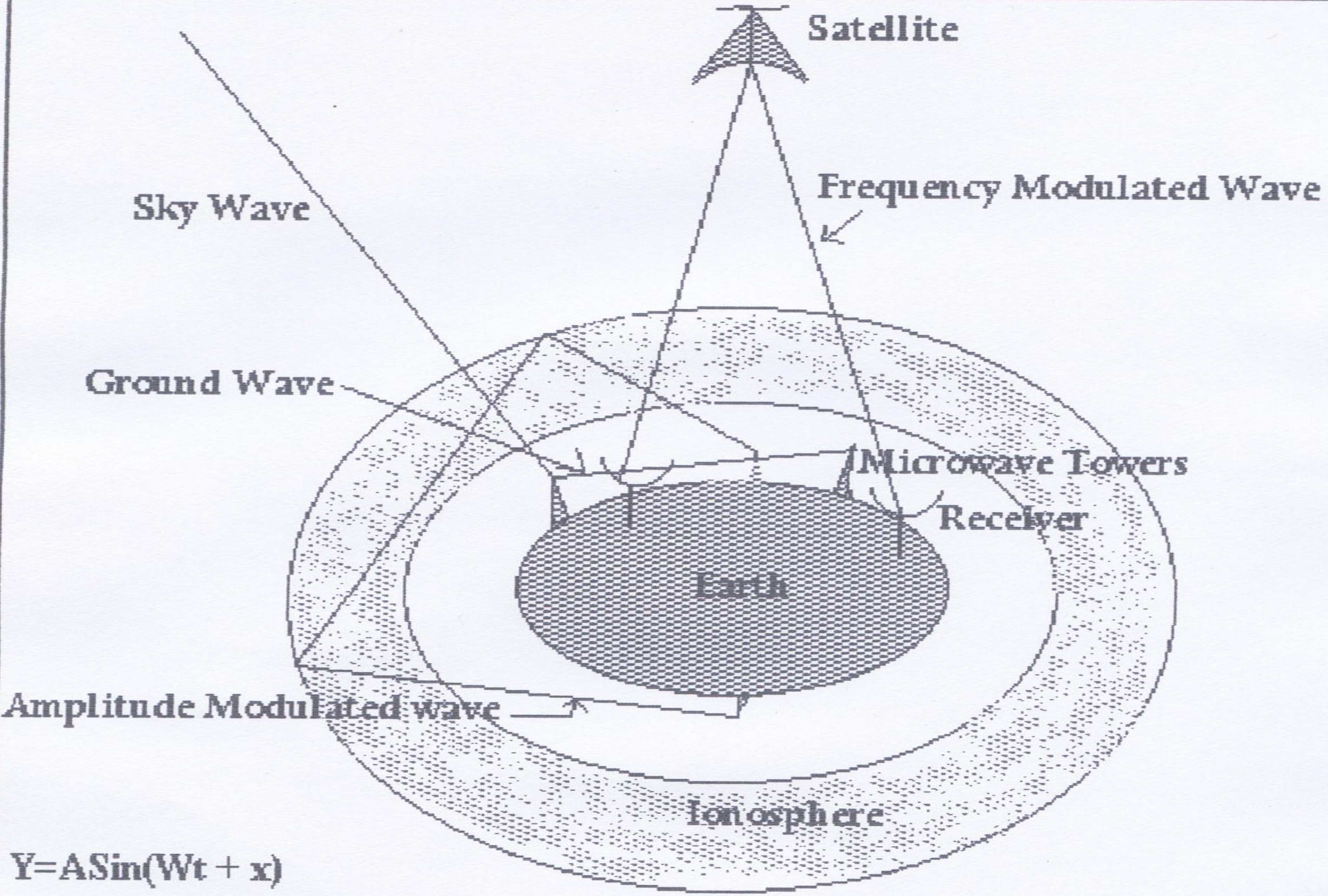
Information Security

Prof.(Dr.) J. K. Mandal

Ex-Dean, Faculty of Engineering, Technology & Management
Professor & Head, Department of Computer Science & Engineering
University of Kalyani
Kalyani, Nadia, West Bengal
E-mail: jkmandal@klyuniv.ac.in, jkm.cse@gmail.com
Mobile:91 9434352214



Y=ASin(Wt + x)

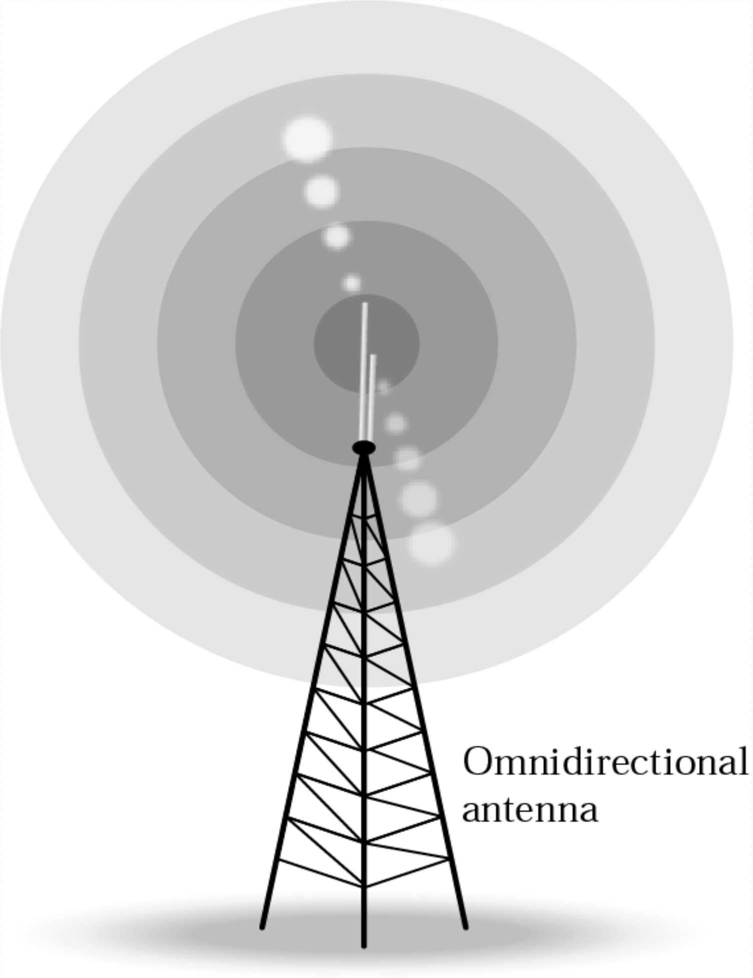
A=Amplitude

W=Frequency

x= Phase

Communication

Figure 7.20 *Omnidirectional antennas*



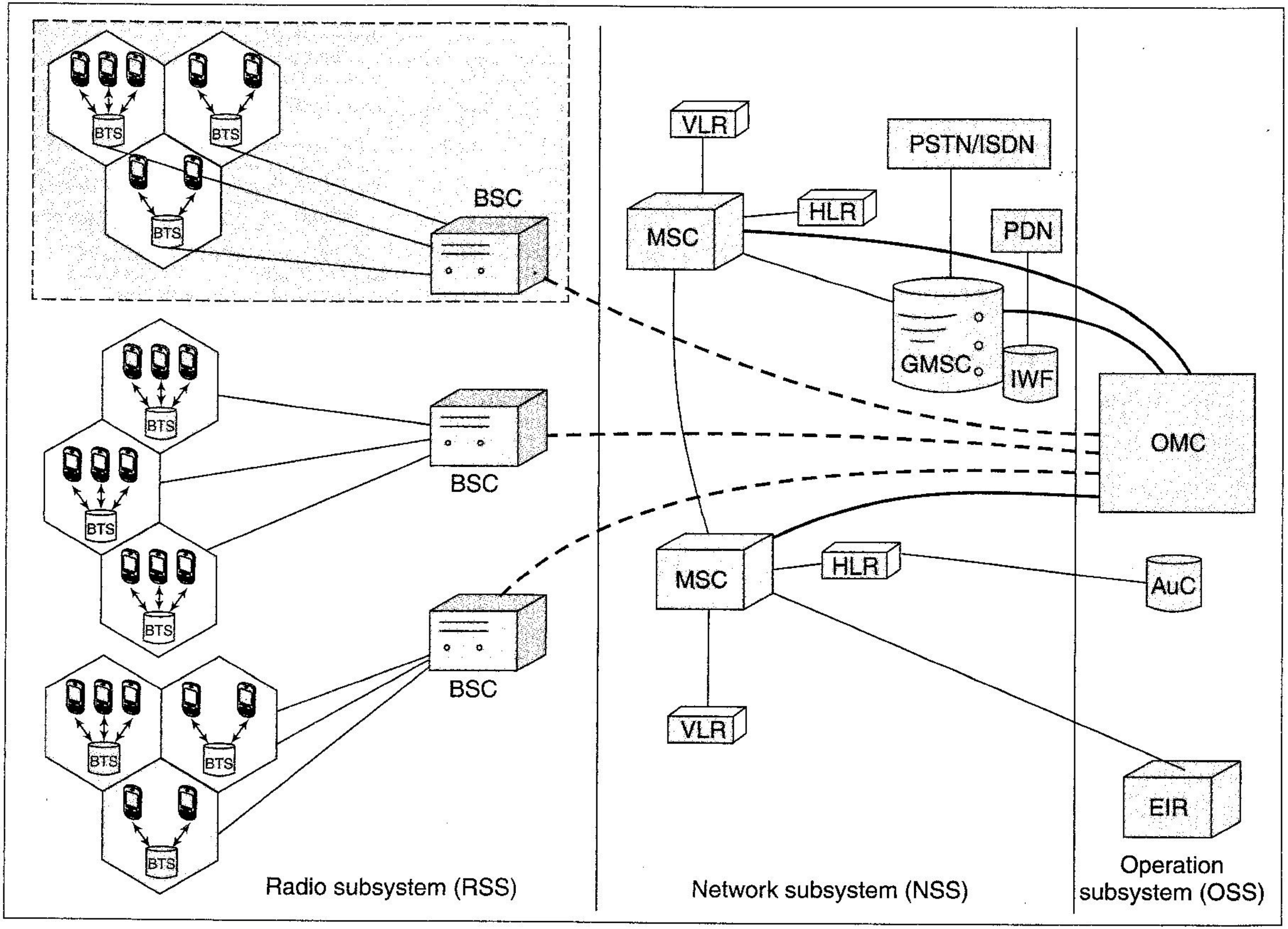
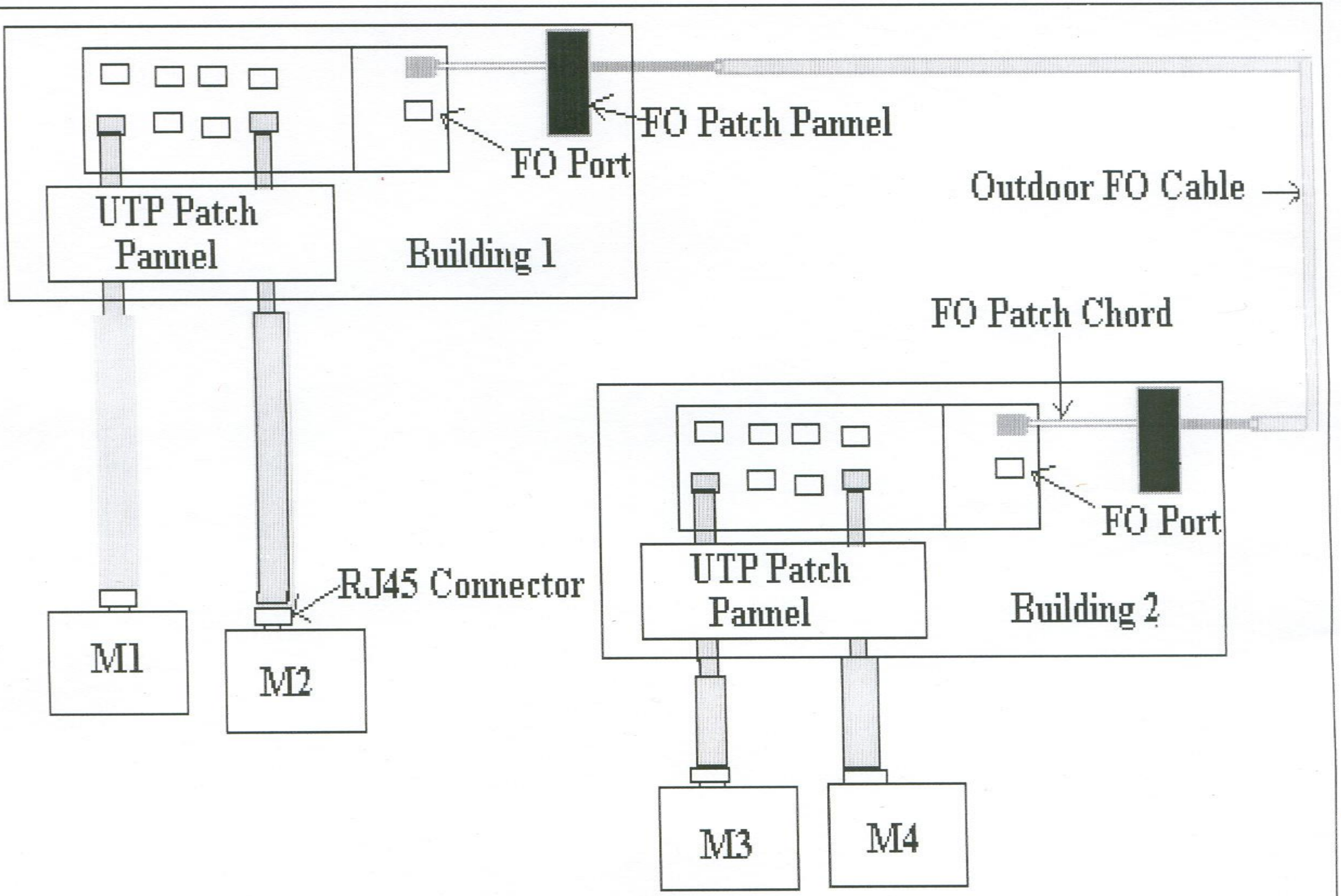
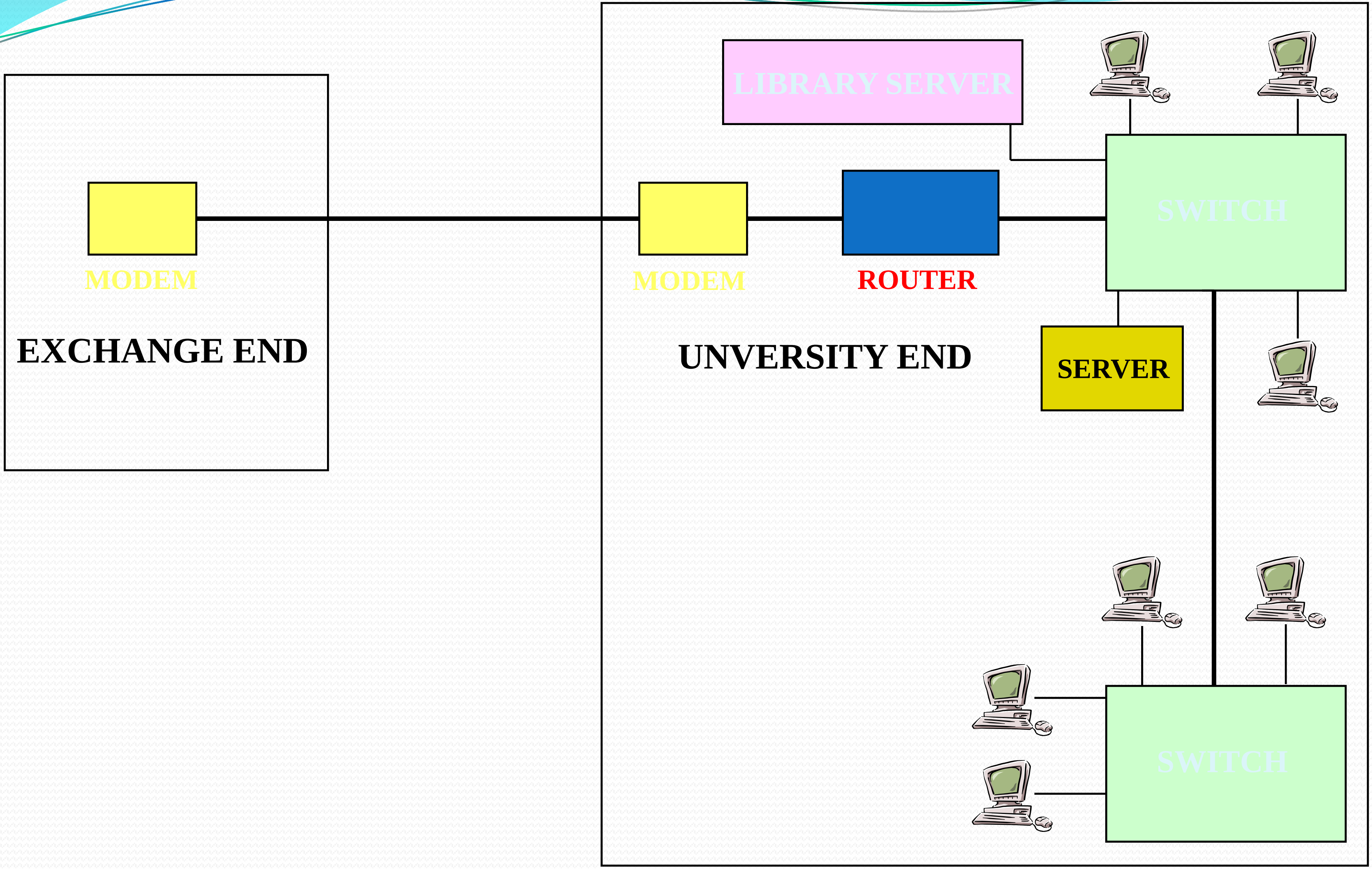


Fig. 3.2 GSM network architecture



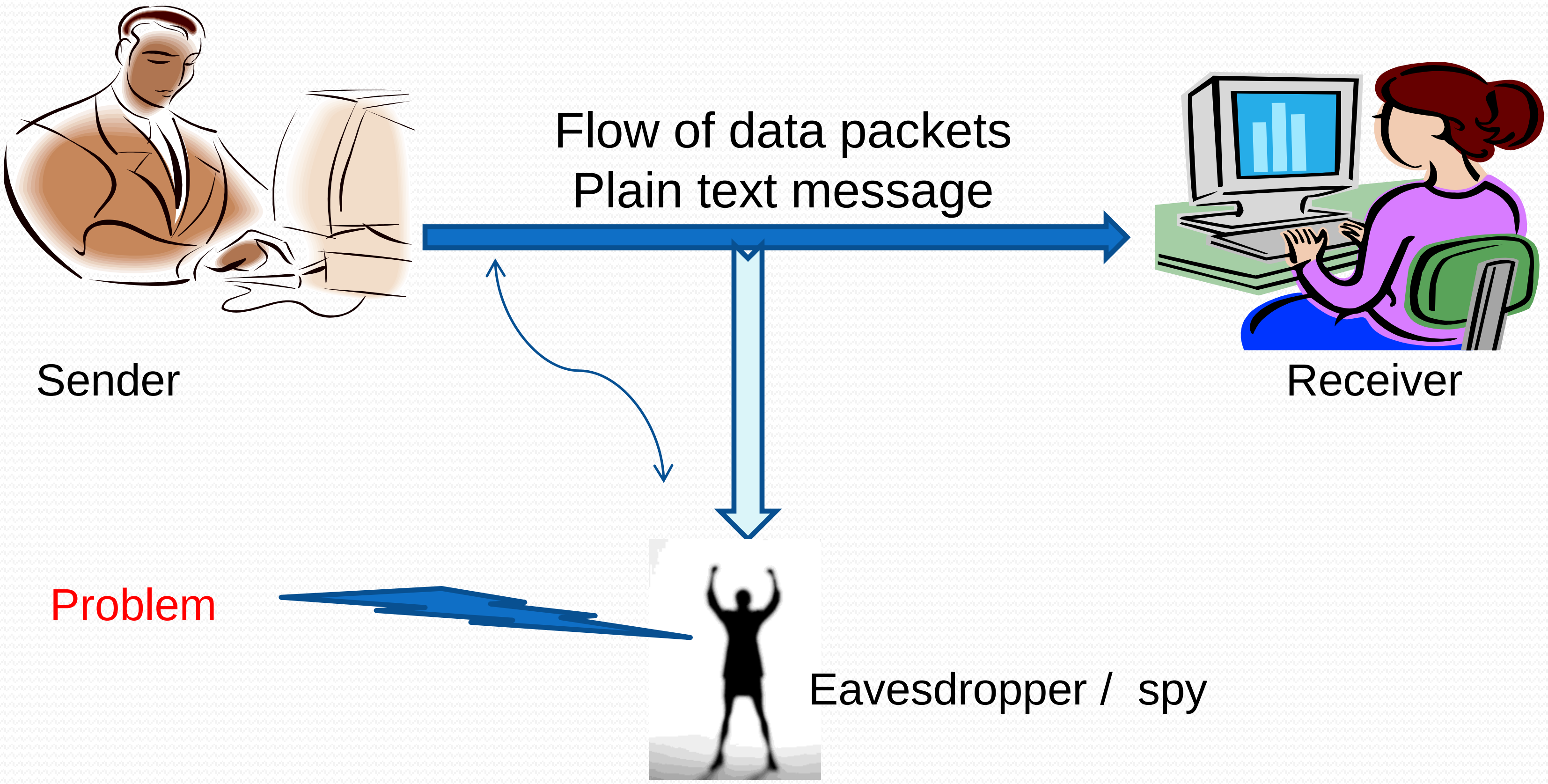
Composite FO/UTP Network for different Buildings

OVERALL REPRESENTATION OF THE LAN & INTERNET SYSTEM



COMMUNICATION

Communication Through Network



Flow of data packets
Plain text message

Sender

Receiver

Problem

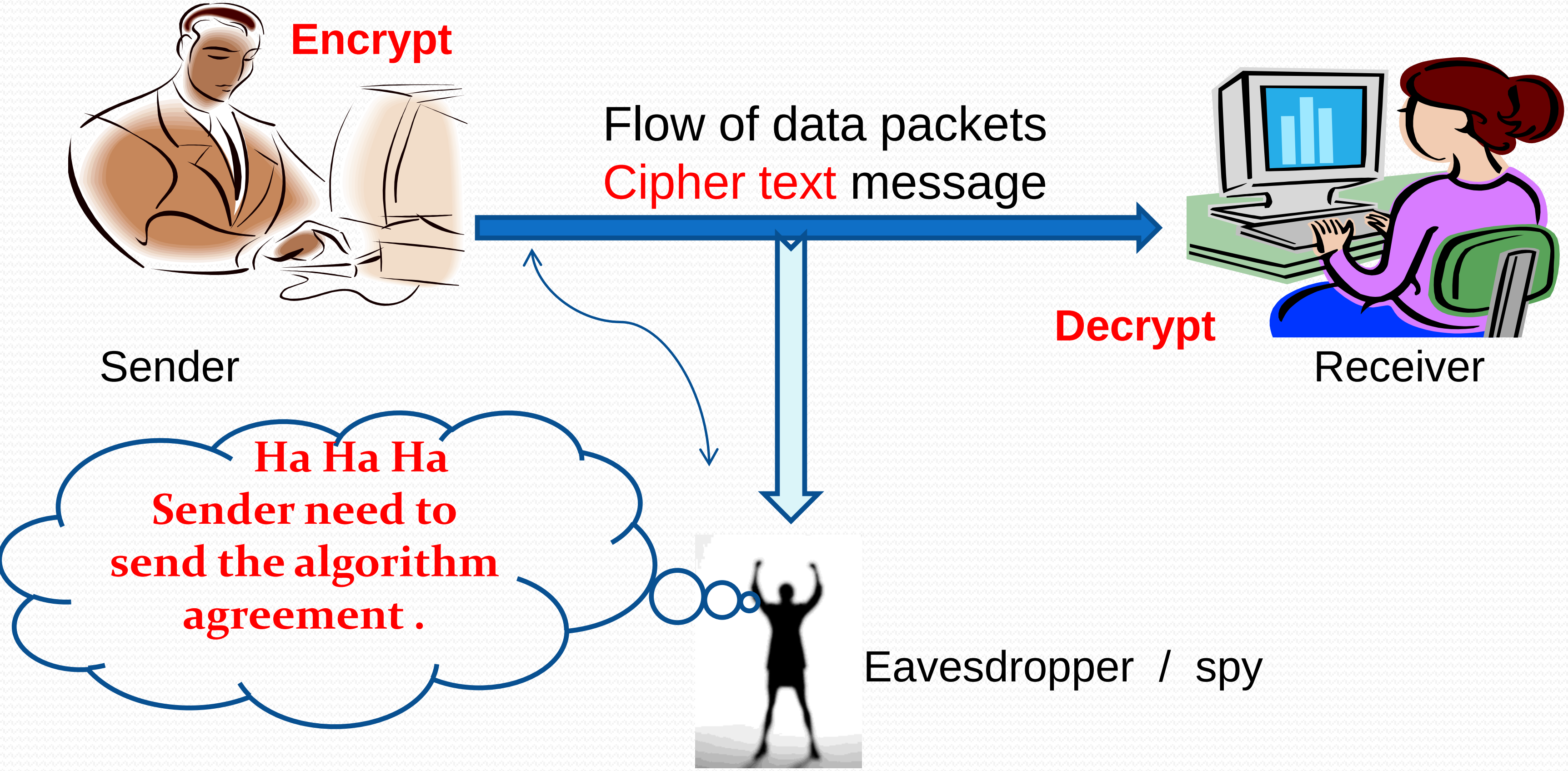
Eavesdropper / spy

Plain text to Cipher text

- Substitution Techniques
  - Caesar Cipher
  - Mono-alphabetic Cipher
  - Homophonic Substitution Cipher
  - Playfair Cipher……………
- Transposition Techniques
  - Rail Fence Technique
  - Vernam Cipher(One Time Pad)
  - Book Cipher/ Running key cipher…………..

Encryption
Decryption
Technique…

Communication…….



Encrypt

Flow of data packets
Cipher text message

Decrypt

Sender

Receiver

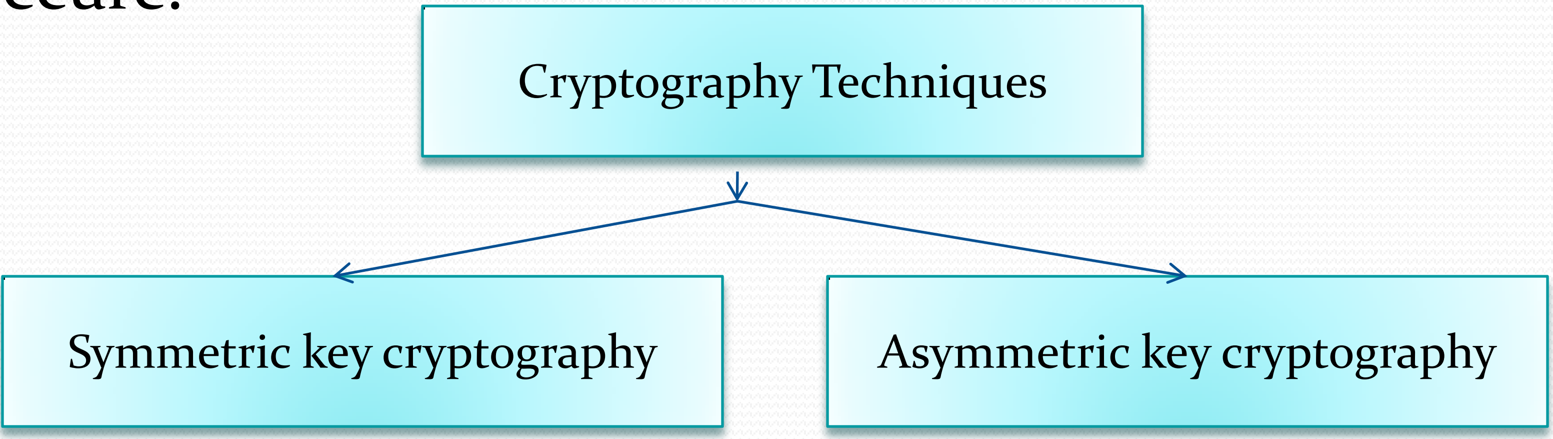
Ha Ha Ha
Sender need to
send the algorithm
agreement .

Eavesdropper / spy

Note:- The decryption algorithm must be the same as the encryption algorithm. Otherwise decryption would not be able to retrieve the original message.

Cryptography

In general , the algorithm used for encryption and decryption process is usually known to everybody. However, it is the key used for encryption and decryption that makes the process of cryptography secure.

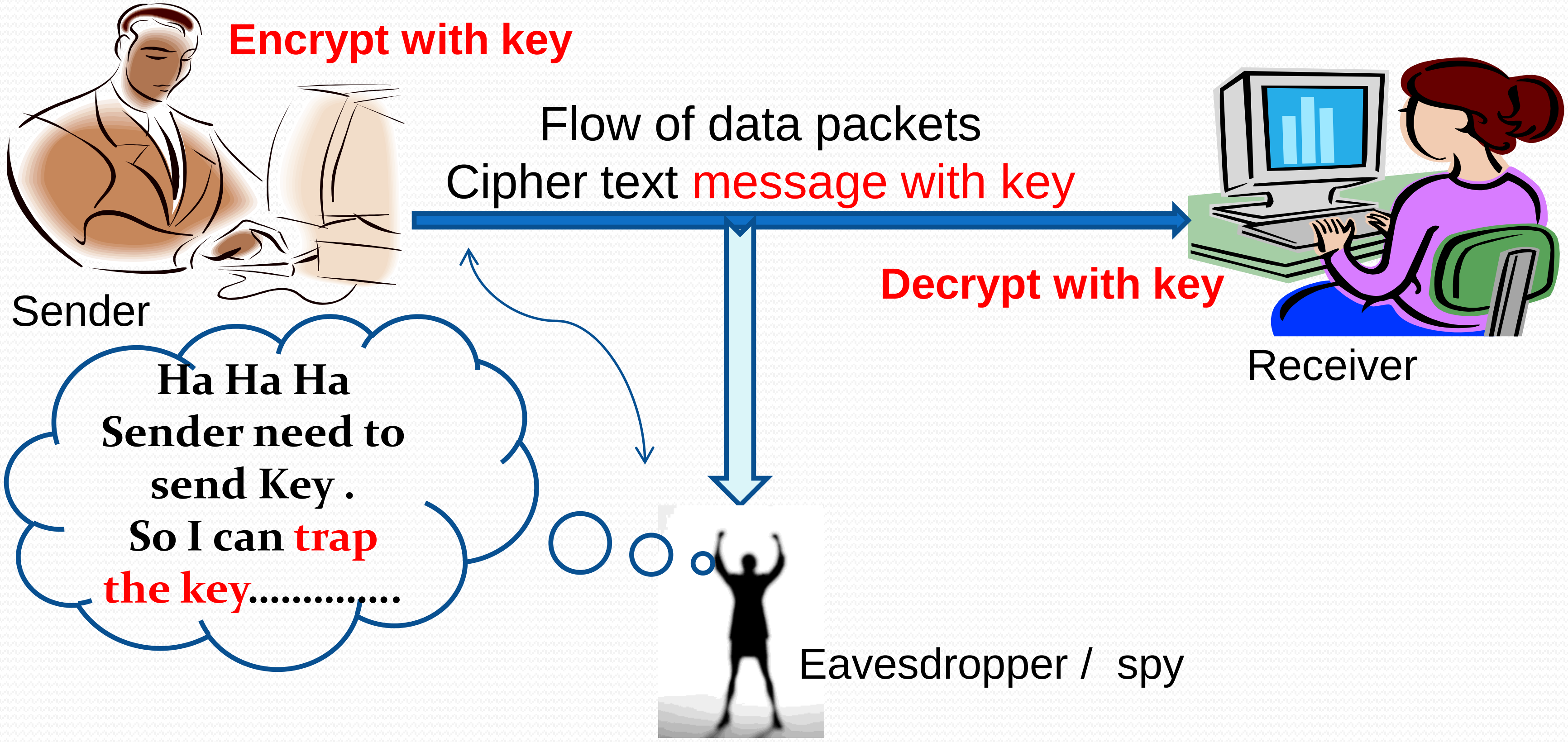


Cryptography Techniques

Symmetric key cryptography

Asymmetric key cryptography

Communication…….
With the concept of key



Encrypt with key

Flow of data packets

Cipher text message with key

Decrypt with key

Sender

Receiver

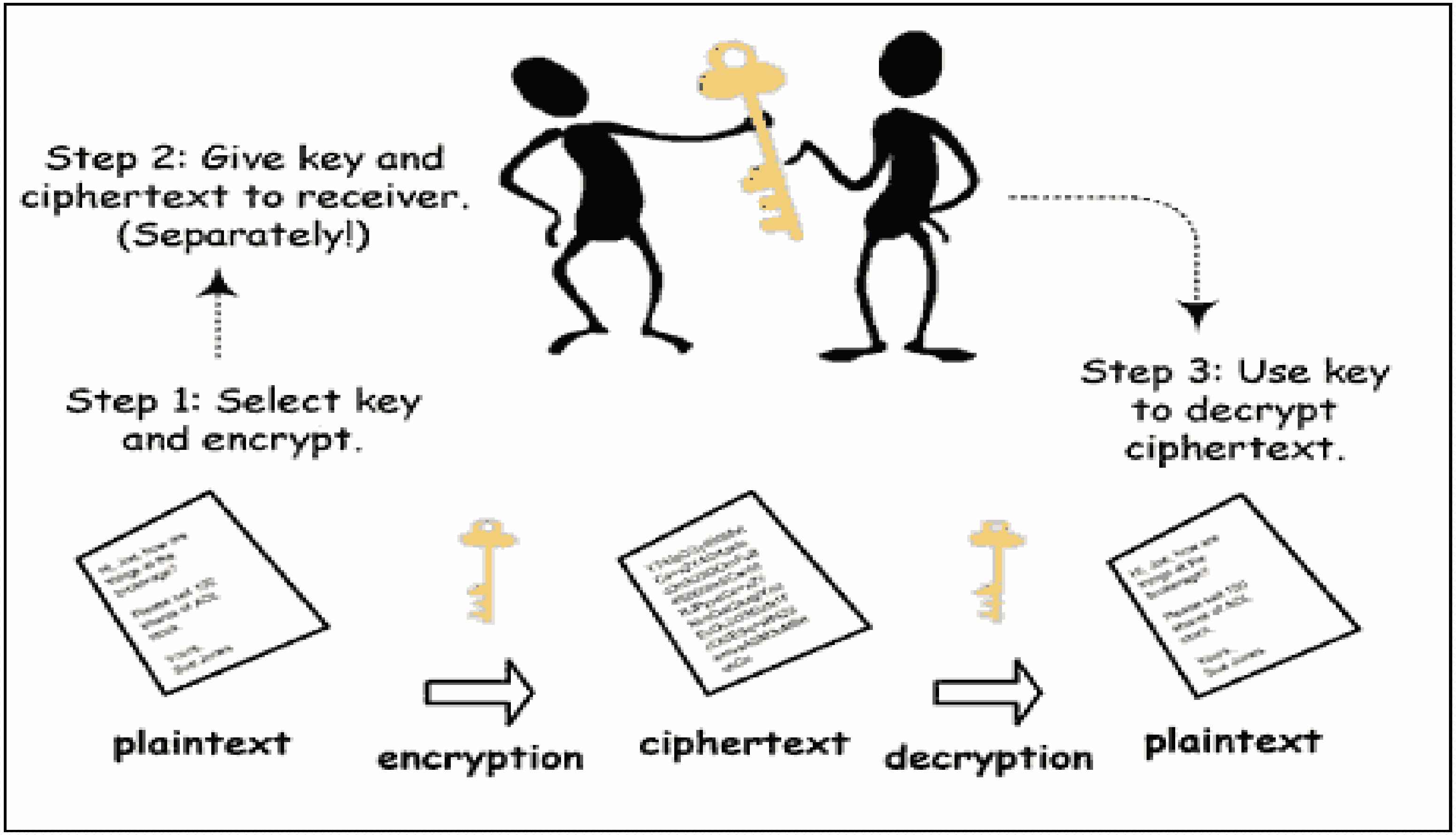
Ha Ha Ha
Sender need to
send Key .
So I can trap
the key…………..

Eavesdropper / spy

Note:- The sender and the receiver using same key ----------

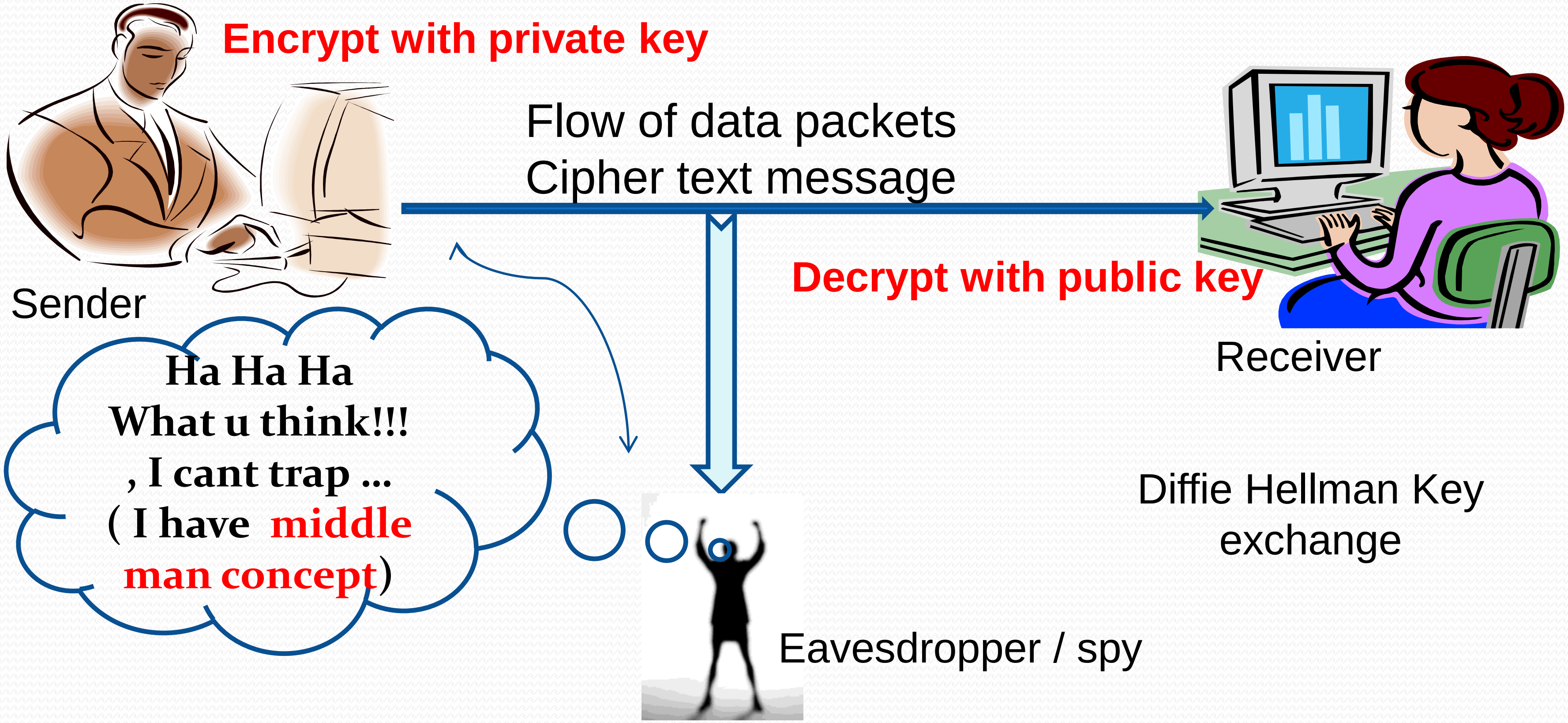
Symmetric key cryptography

Applications of Symmetric Algorithms


Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Communication……

With the concept of key



Encrypt with private key

Flow of data packets
Cipher text message

Decrypt with public key

Sender

Receiver

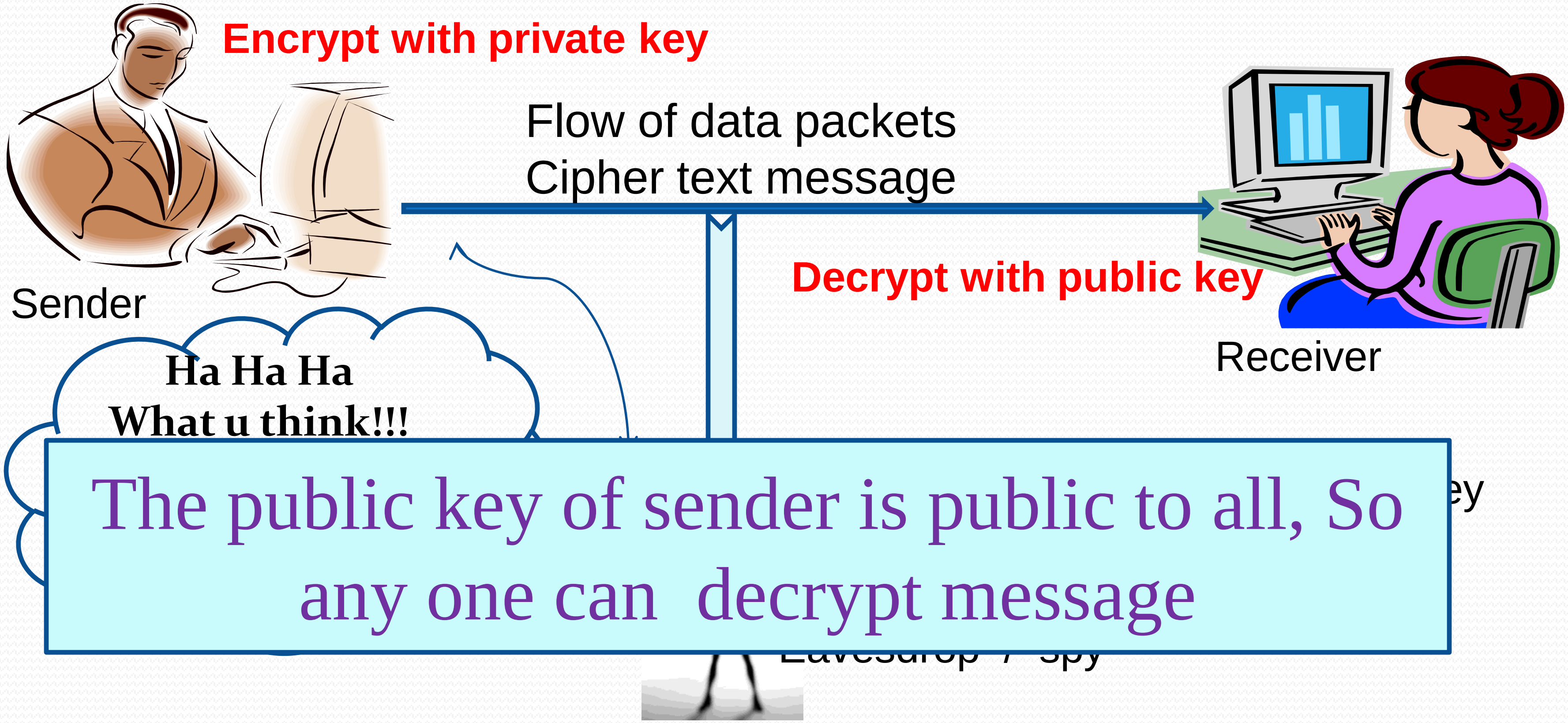
Ha Ha Ha
What u think!!!
, I cant trap …
(I have middle man concept)

Diffie Hellman Key exchange

Eavesdropper / spy

Note:- The sender and the receiver using different key ----------
Asymmetric key cryptography

Communication……. With the concept of key



Encrypt with private key

Flow of data packets
Cipher text message

Decrypt with public key

The public key of sender is public to all, So any one can decrypt message

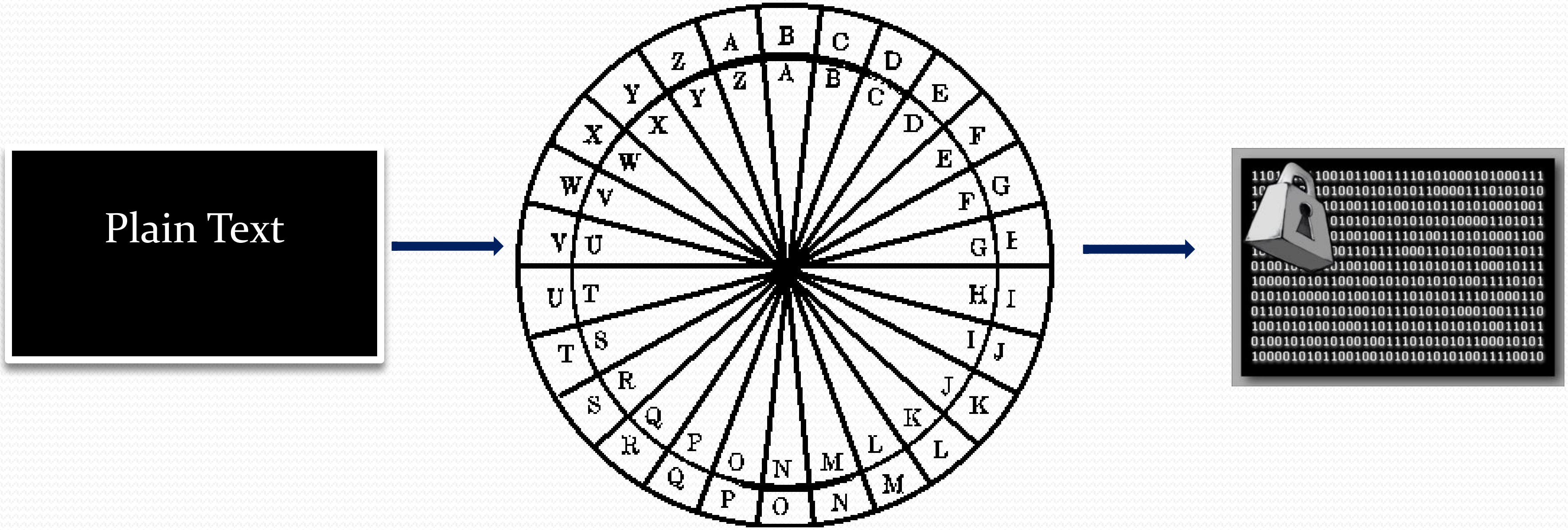
Note:- The sender and the receiver using different key ---------- Asymmetric key cryptography

Security aspects

CRYPTOGRAPHY

STEGANOGRAPHY

CRYPTOGRAPHY



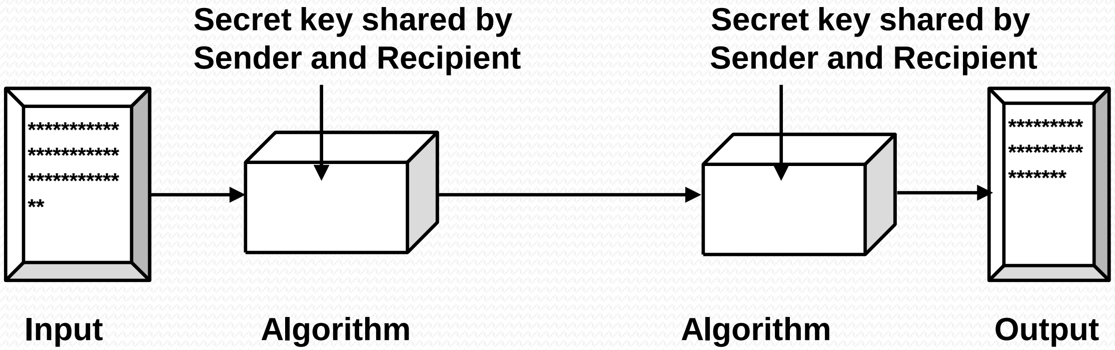
Plain Text

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
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

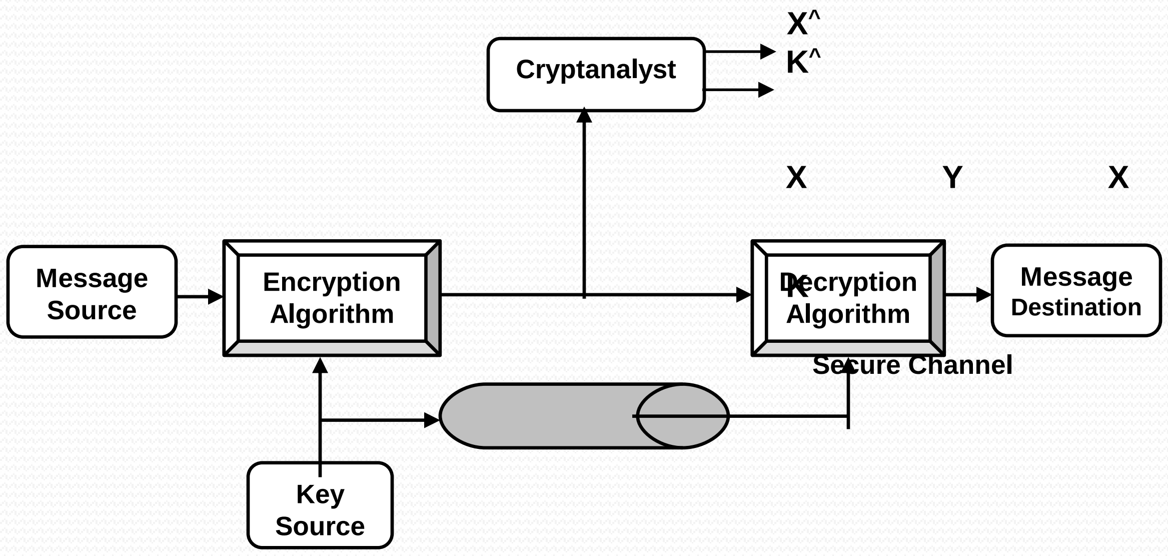
In general, there exist following types of problems associated with such data transmission

- **A huge amount of data is to be handled**
- **Much of the data is very sensitive to errors**
- **The security of data transmitted from source to destination over communication links via different nodes is the most important matter to be worried.**

- **Data Encryption.**
- **Data Decryption**



Simplified Model of Secret Key Cryptosystem



Model of Secret Key Cryptosystem

There are two general approaches to attack a conventional encryption scheme.

1. Cryptanalysis
2. Brute-force Attack:

Average Time Required for Exhaustive Key Search

Key Size (Bits)	Number of Alternative Keys	Time Required at 1 Encryption / µs	Time Required At 10^6 Encryptions / µs
56	$2^{56} = 7.2 \text{ X } 10^{16}$	2^{55} µs =1142 years	10.01 hours
128	$2^{128} = 3.4 \text{ X } 10^{38}$	2^{127} µs = $5.4 \text{ X } 10^{24}$ years	$5.4 \text{ X } 10^{18}$ years
168	$2^{168} = 3.7 \text{ X } 10^{50}$	2^{167} µs = $5.9 \text{ X } 10^{36}$ years	$5.9 \text{ X } 10^{30}$ years
26 characters (Permutation)	$26! = 4 \text{ X } 10^{26}$	$2 \text{ X } 10^{26}$ µs = $6.4 \text{ X } 10^{12}$ years	$6.4 \text{ X } 10^{6}$ years

The 56-bit key size is used with the DES (Data Encryption Standard) algorithm.

- The 128-bit key size is used with the AES (Advanced Encryption Standard) algorithm.

- The 168-bit key size is used with triple DES.

The two basic building blocks of all encryption techniques are:

1. **Substitution Techniques**
2. **Transposition Techniques**

S-Boxes

provide **confusion** of input bits

P-Boxes

provide **diffusion** across S-box inputs

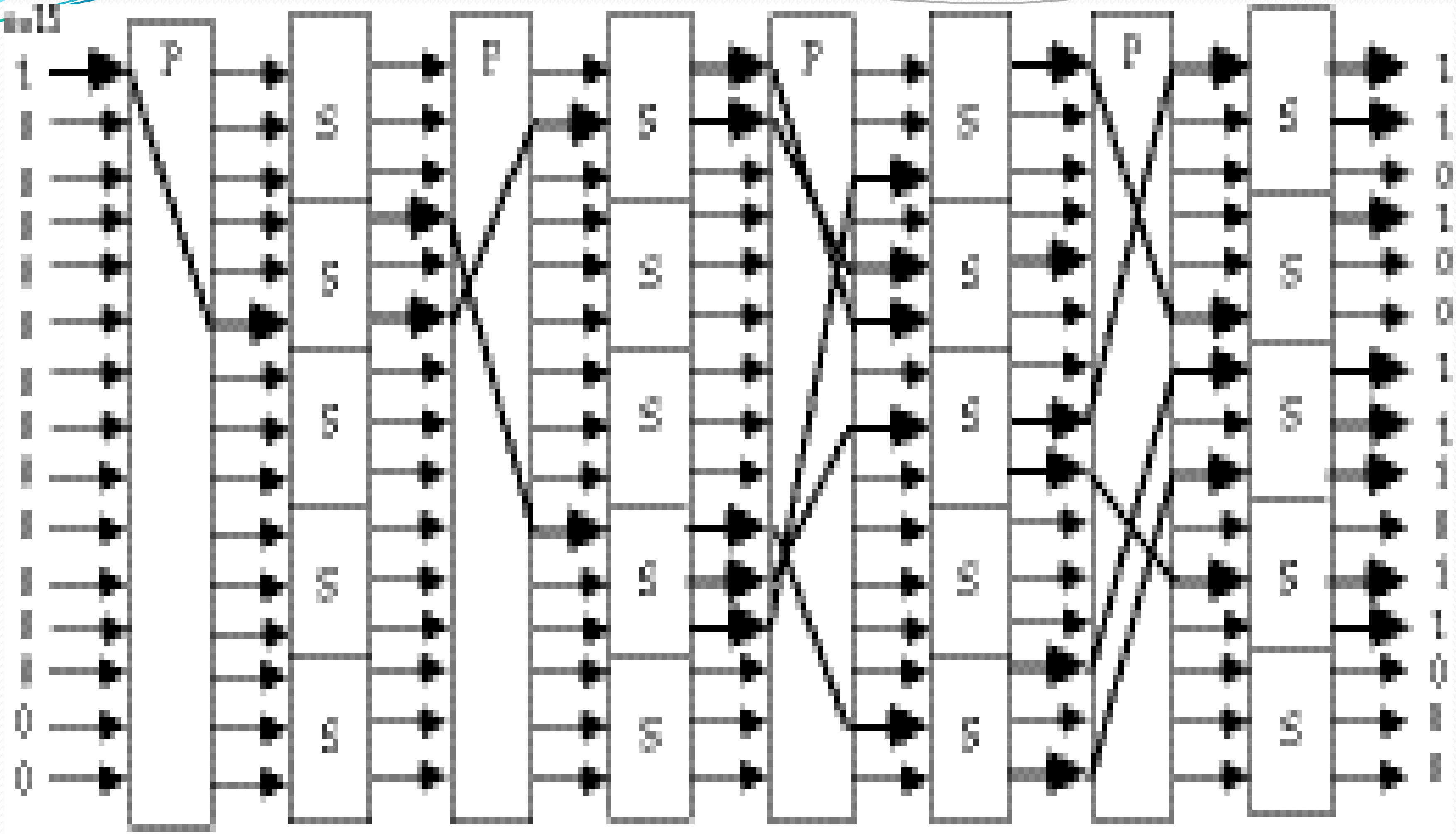
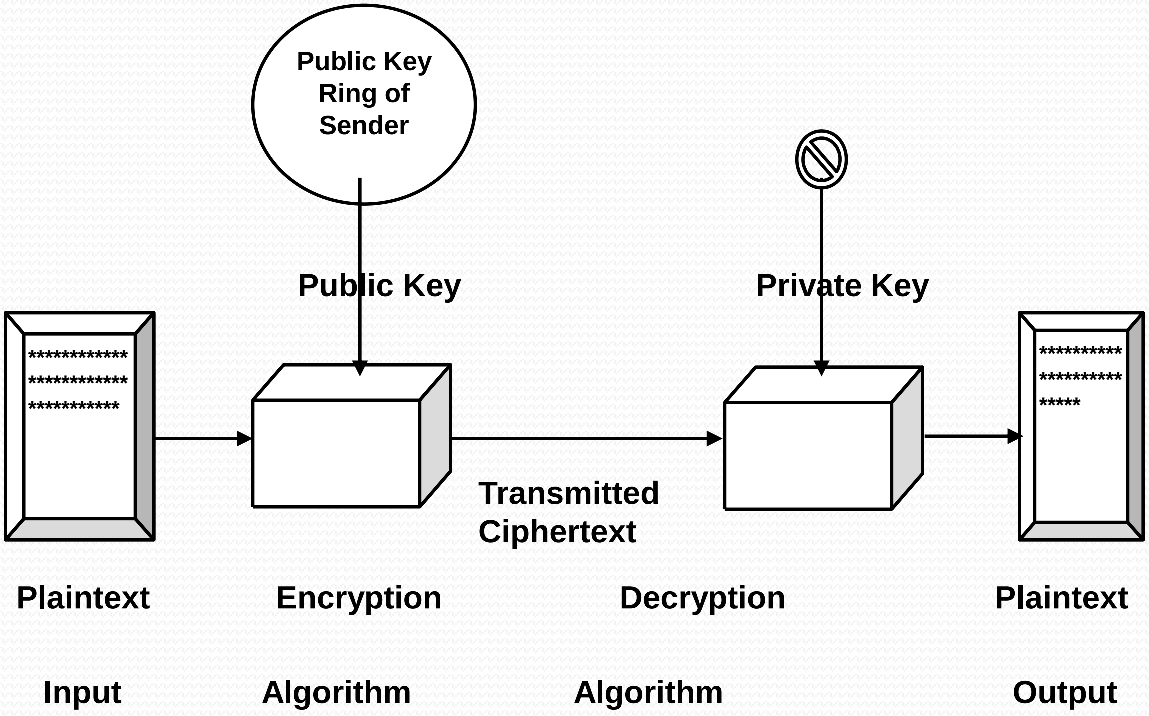


Fig 2.3 - Substitution-Permutation Network with the Avalanche Characteristic

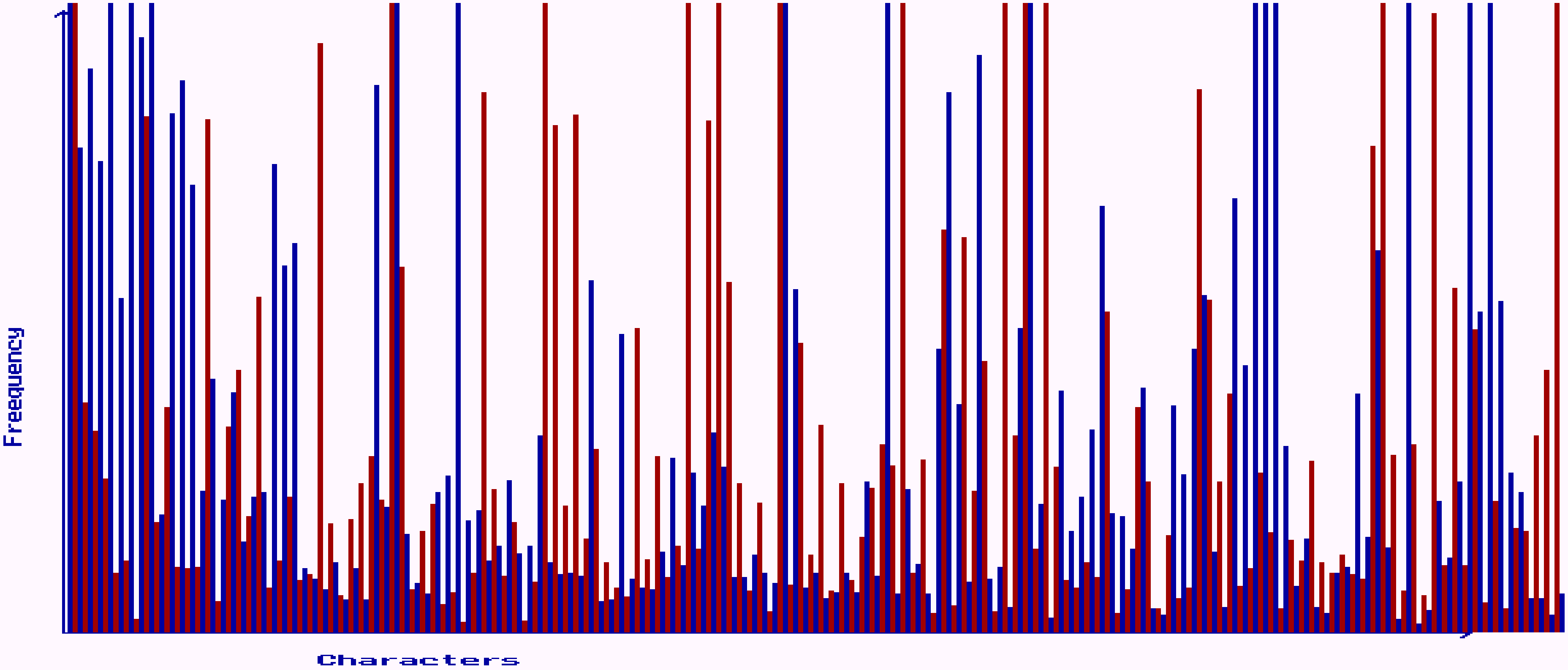


Simplified Model of Public Key Cryptosystem

Factors considered for Evaluating Proposed Techniques

- Frequency Distribution Test
- Chi Square Test
- Analysis of the Key Space
- Computation of the Encryption/Decryption Time
- Comparison of Performance with the RSA System

A segment of frequency distribution for characters in tlib.exe and its encrypted file

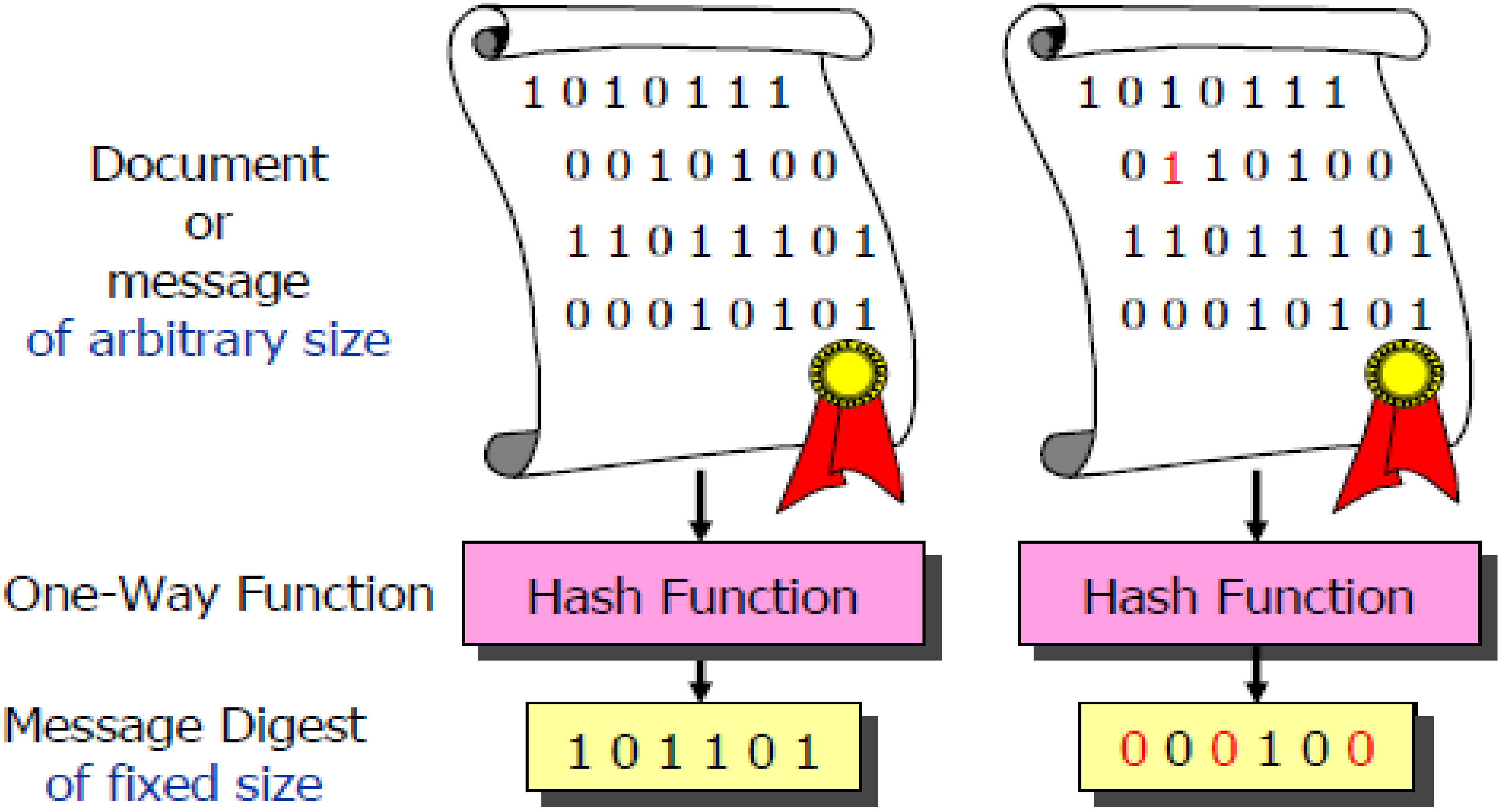


Blue lines indicate the occurrences of characters in the source file and red lines indicate the same in the corresponding encrypted file

DIGITAL SIGNATURE

MESSAGE DIGEST

Message Digests based on One–Way Hash Functions



Document
or
message
of arbitrary size

1 0 1 0 1 1 1
0 0 1 0 1 0 0
1 1 0 1 1 1 0 1
0 0 0 1 0 1 0 1

1 0 1 0 1 1 1
0 1 1 0 1 0 0
1 1 0 1 1 1 0 1
0 0 0 1 0 1 0 1

One-Way Function

Hash Function

Hash Function

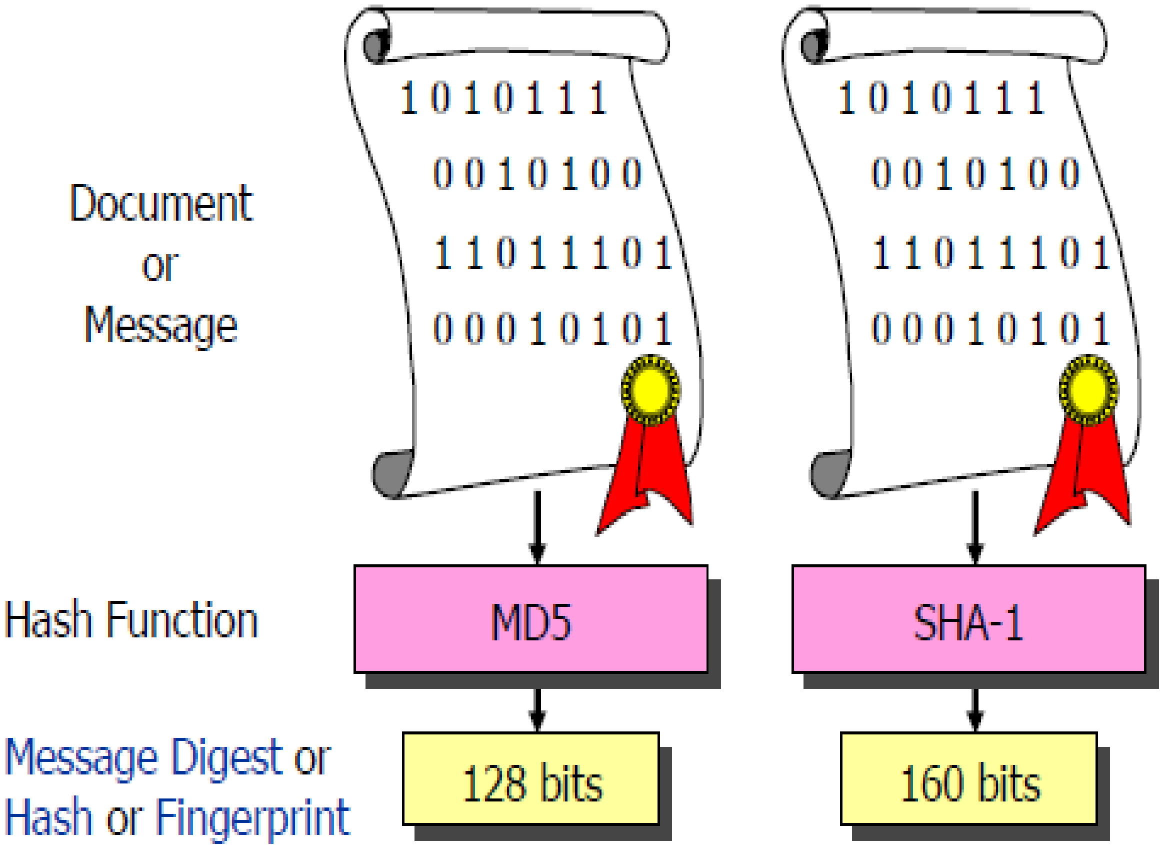
Message Digest
of fixed size

1 0 1 1 0 1

0 0 0 1 0 0

- A single bit change in a document should cause about 50% of the bits in the digest to change their values !

Popular Hash Functions



Document or Message

Hash Function

MD5

SHA-1

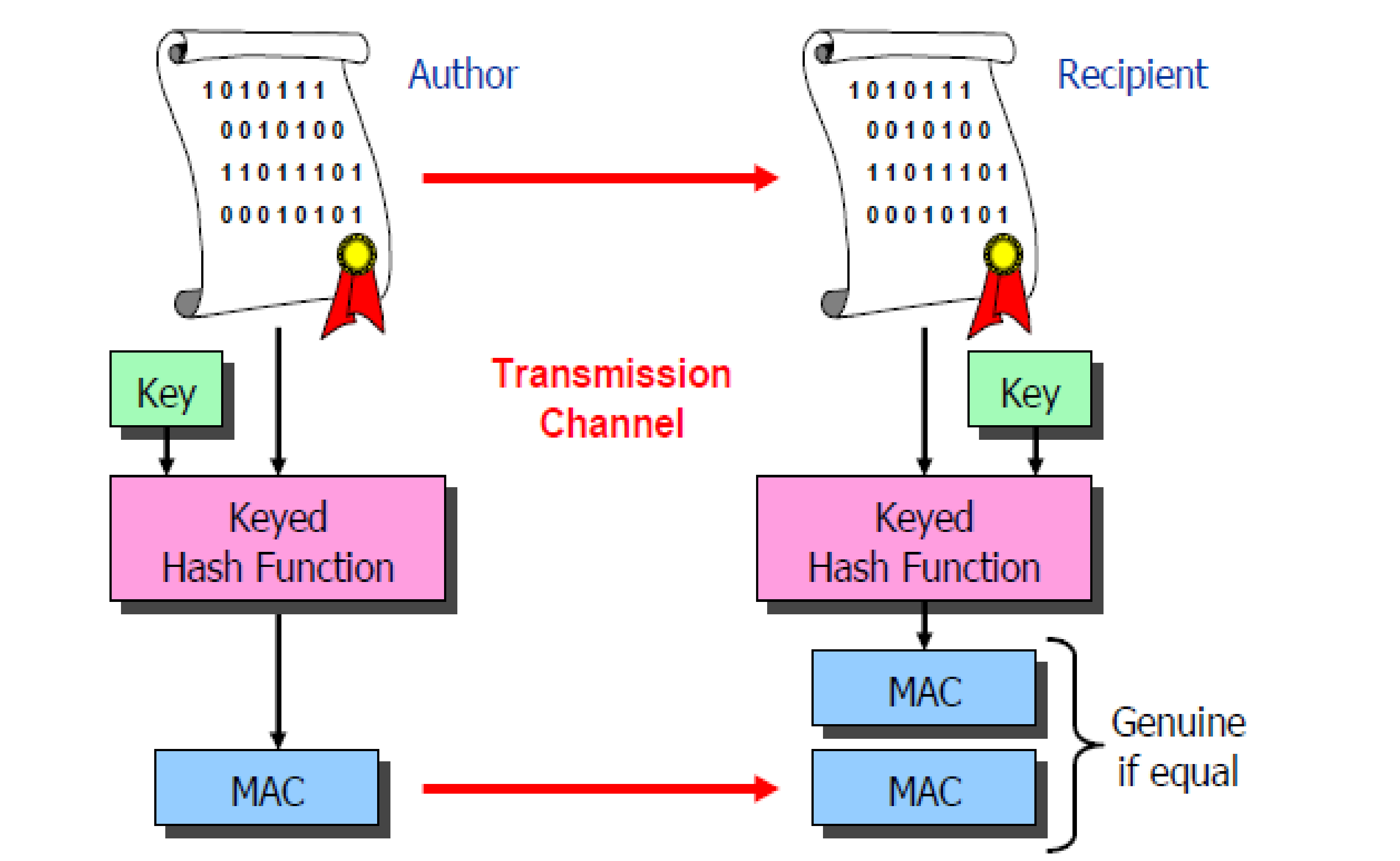
Message Digest or Hash or Fingerprint

128 bits

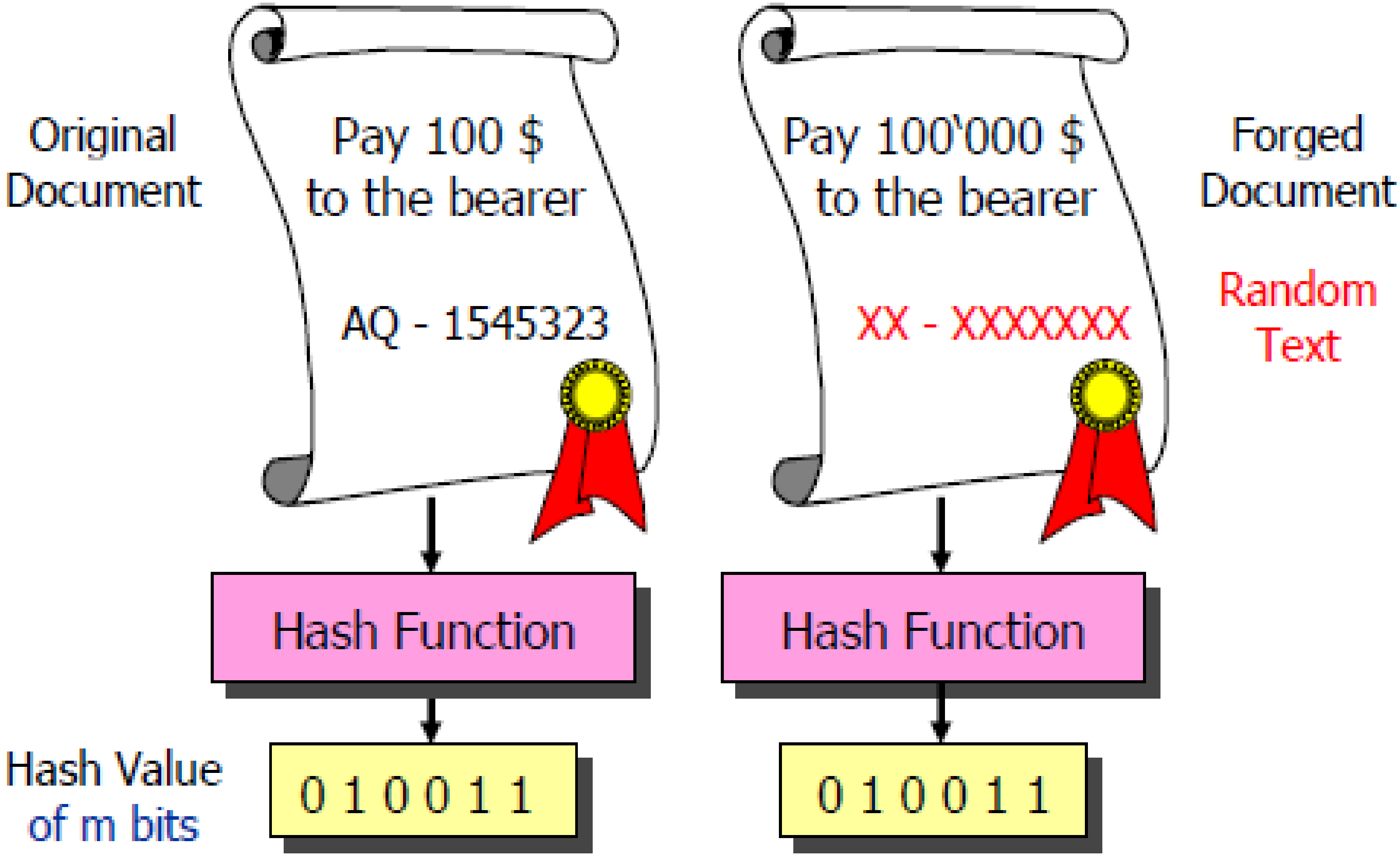
160 bits

- MD5 – Message Digest # 5, Ron Rivest, RSA
- SHA-1 – Secure Hash Algorithm, NIST / NSA

Message Authentication Codes based on Keyed One–Way Hash Function



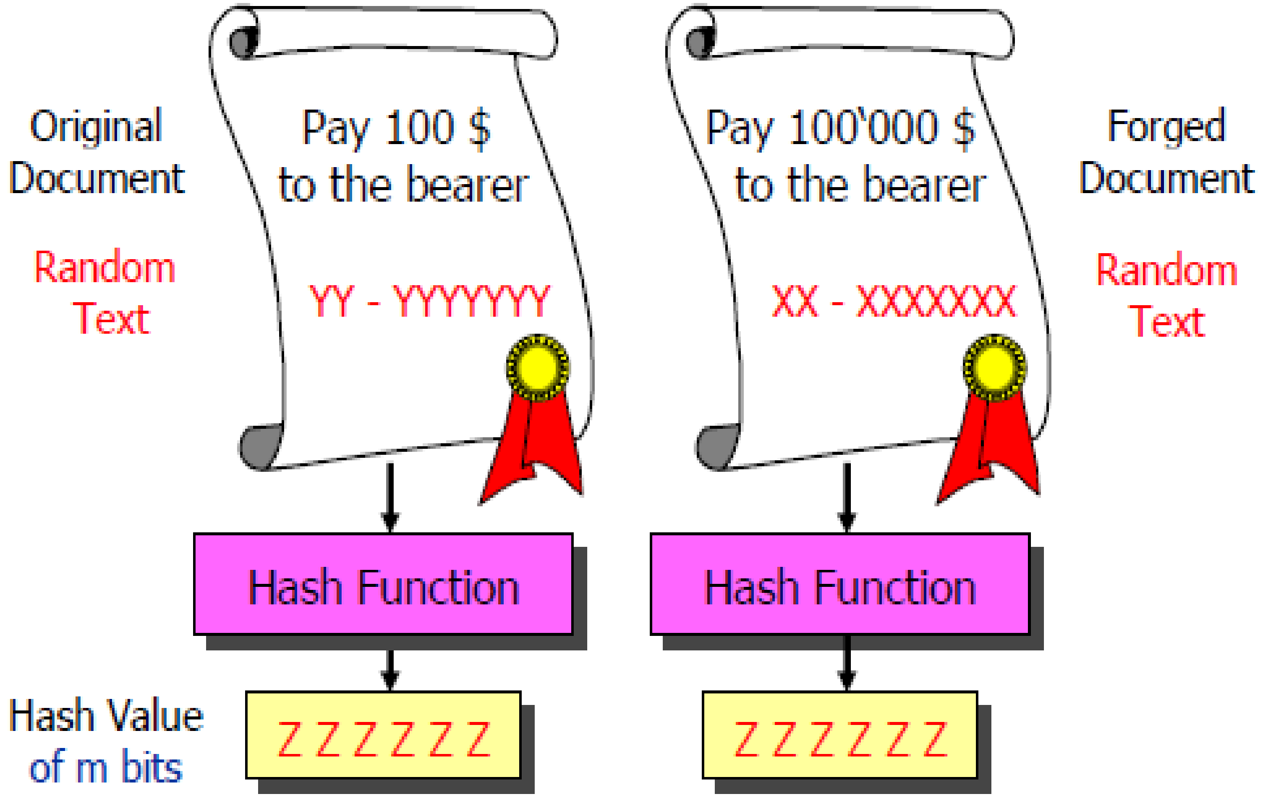
Forging Documents



- On average 2^m trials are required to find a document having the same hash value as a given one !

Birthday Attacks against Hash Functions

Looking for Collisions !



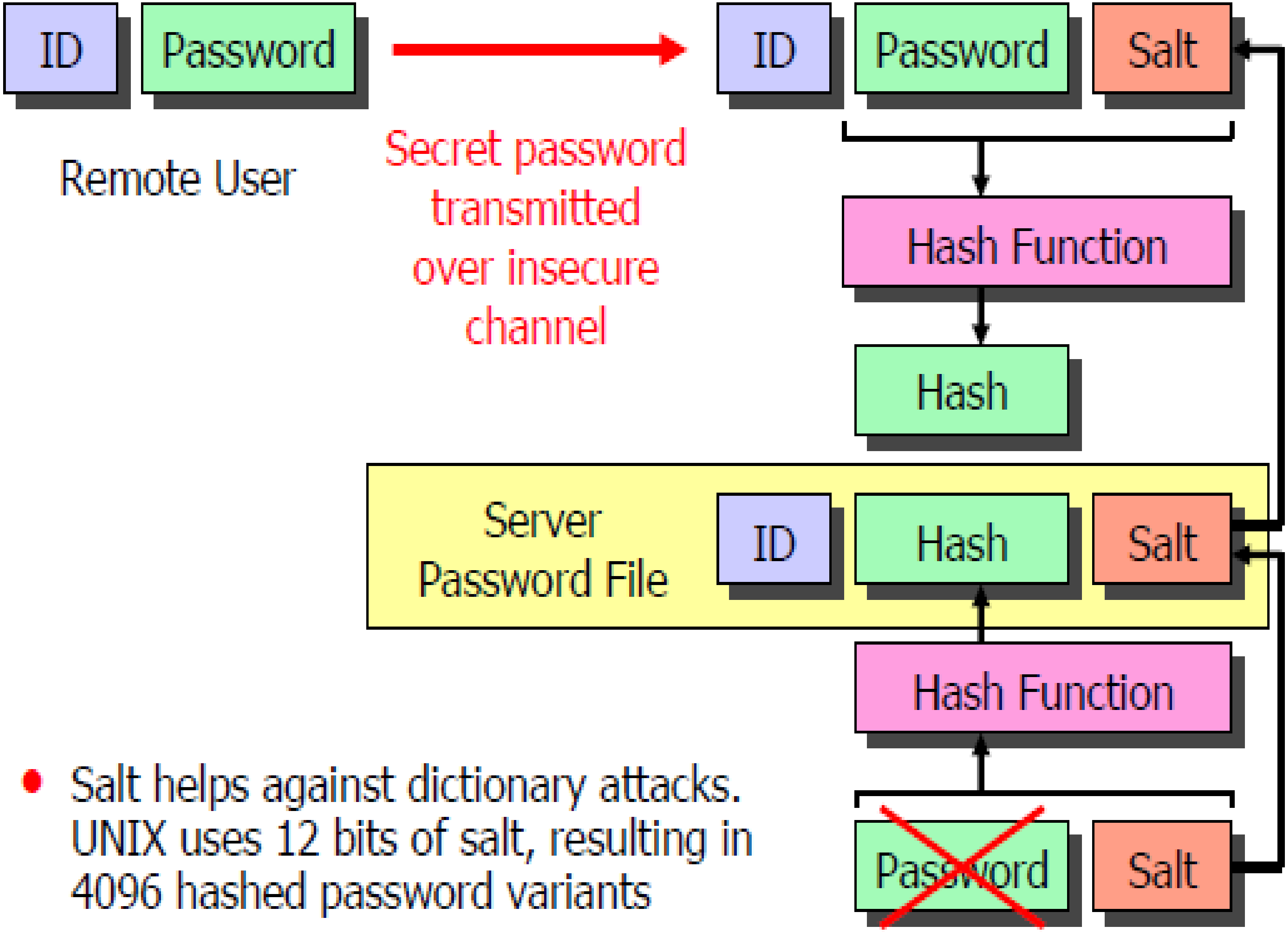
- Less than $2^{m/2}$ trials are required to find two documents having the same hash value ⇒ MD5 with 2^{39} and SHA-1 with 2^{63} trials are both insecure !

User Authentication

"On the Internet, nobody knows you're a dog."

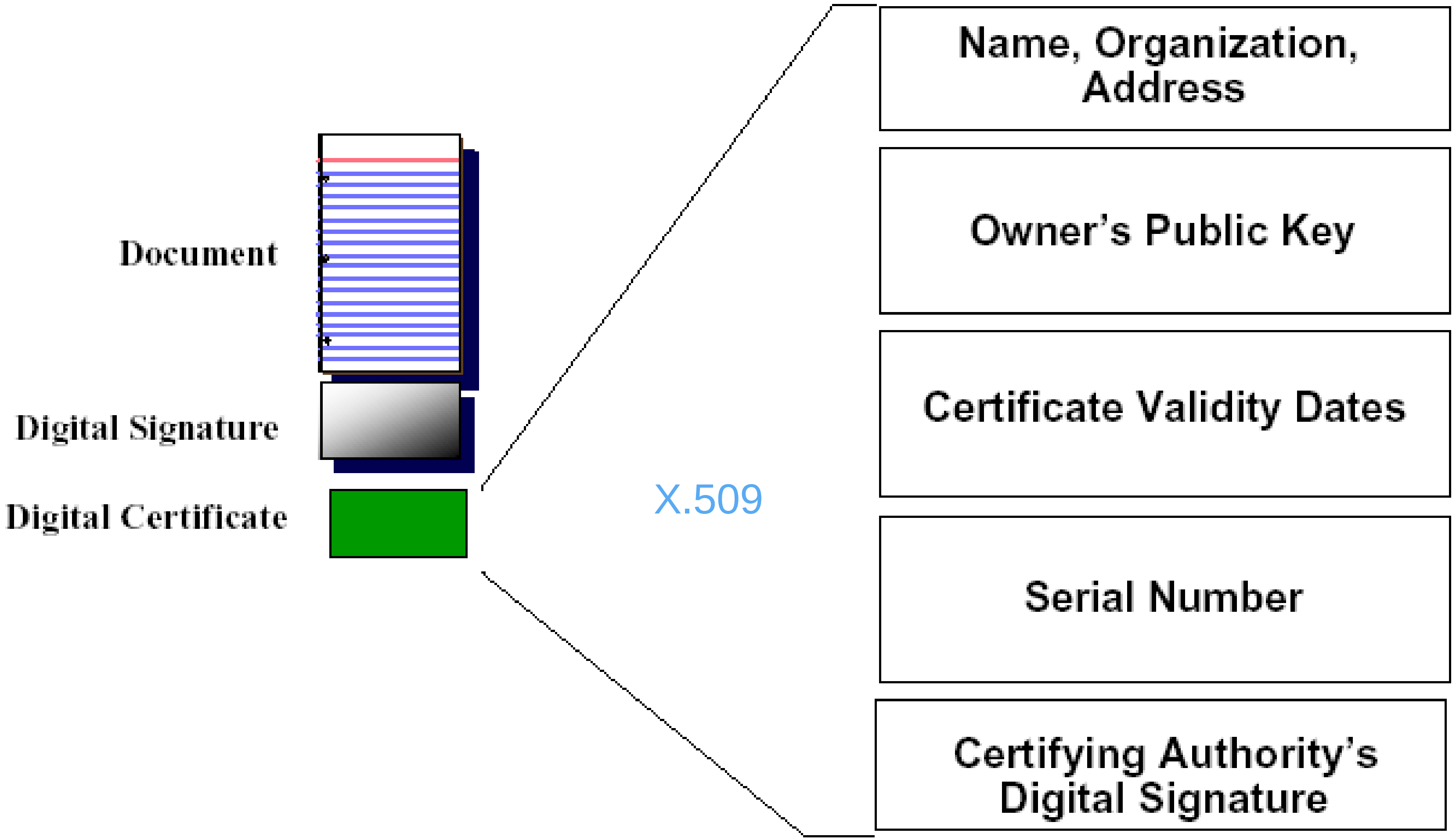
- Username / Password
  - Dictionary Attacks
- One-Time Passwords
  - Token: SecureID, etc.
- Public Key Algorithms
  - Smartcards, Certificates, Public Key Infrastructure
- Biometrical Methods
  - Fingerprint, Iris-Scan, Voice, Face, Hand, etc.

Insecure Authentication based on Passwords



- Salt helps against dictionary attacks. UNIX uses 12 bits of salt, resulting in 4096 hashed password variants

Digital Certificates



Document

Digital Signature

Digital Certificate

X.509

Name, Organization, Address

Owner's Public Key

Certificate Validity Dates

Serial Number

Certifying Authority's Digital Signature

Public Key Infrastructure

The **Public Key Infrastructure (PKI)** is the road ahead for almost all cryptography system.

The **PKI** is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates .

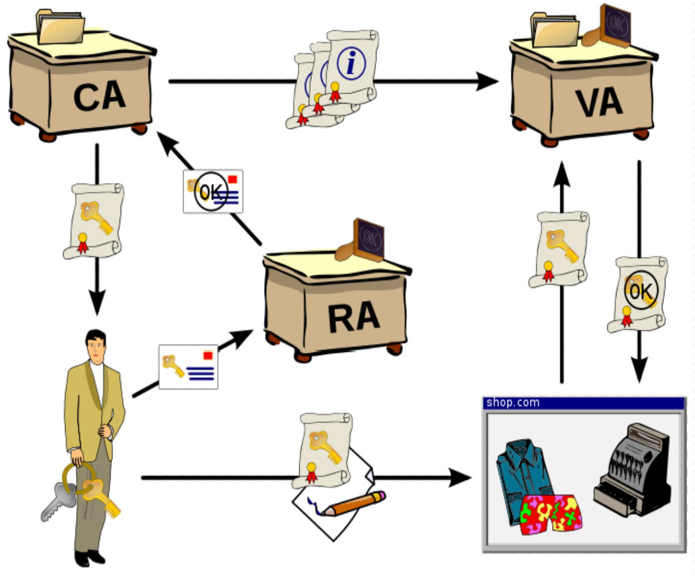
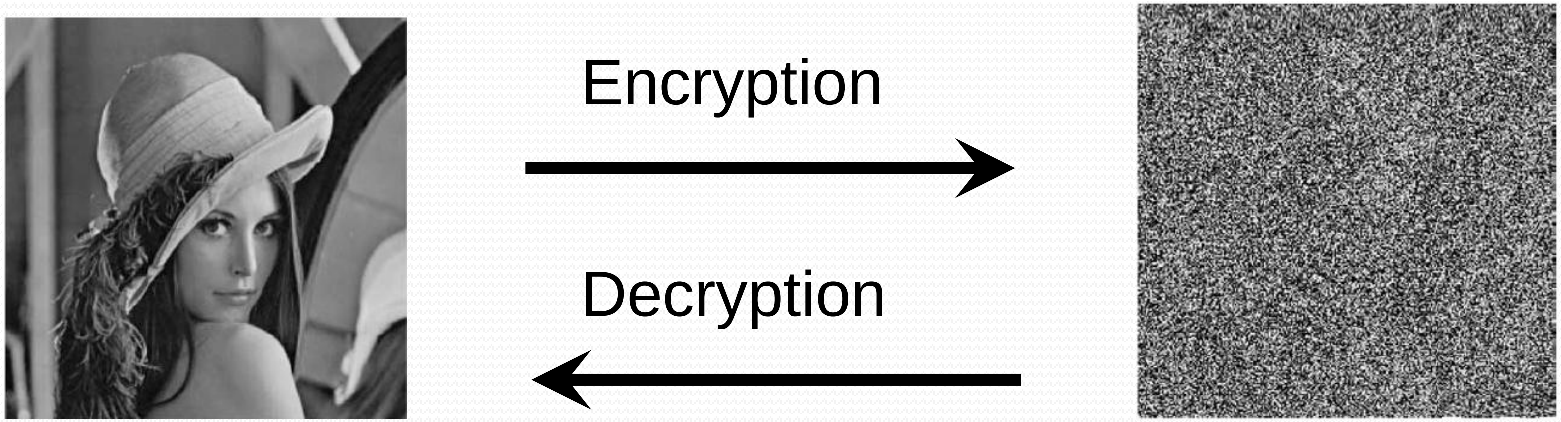


IMAGE ENCRYPTION



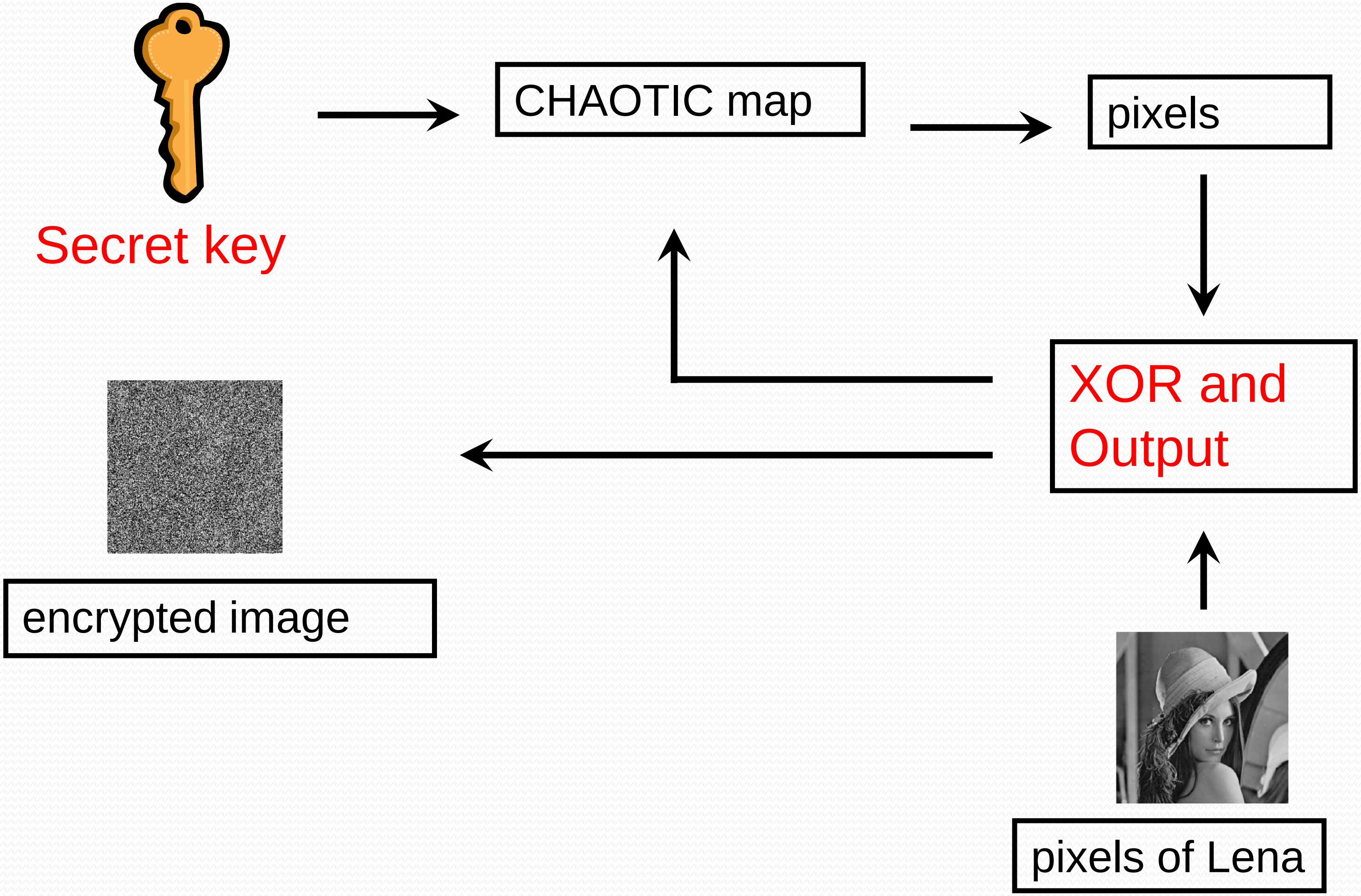
Encryption

Decryption

Lena

encrypted image

ENCRYPTION



Secret key

CHAOTIC map

pixels

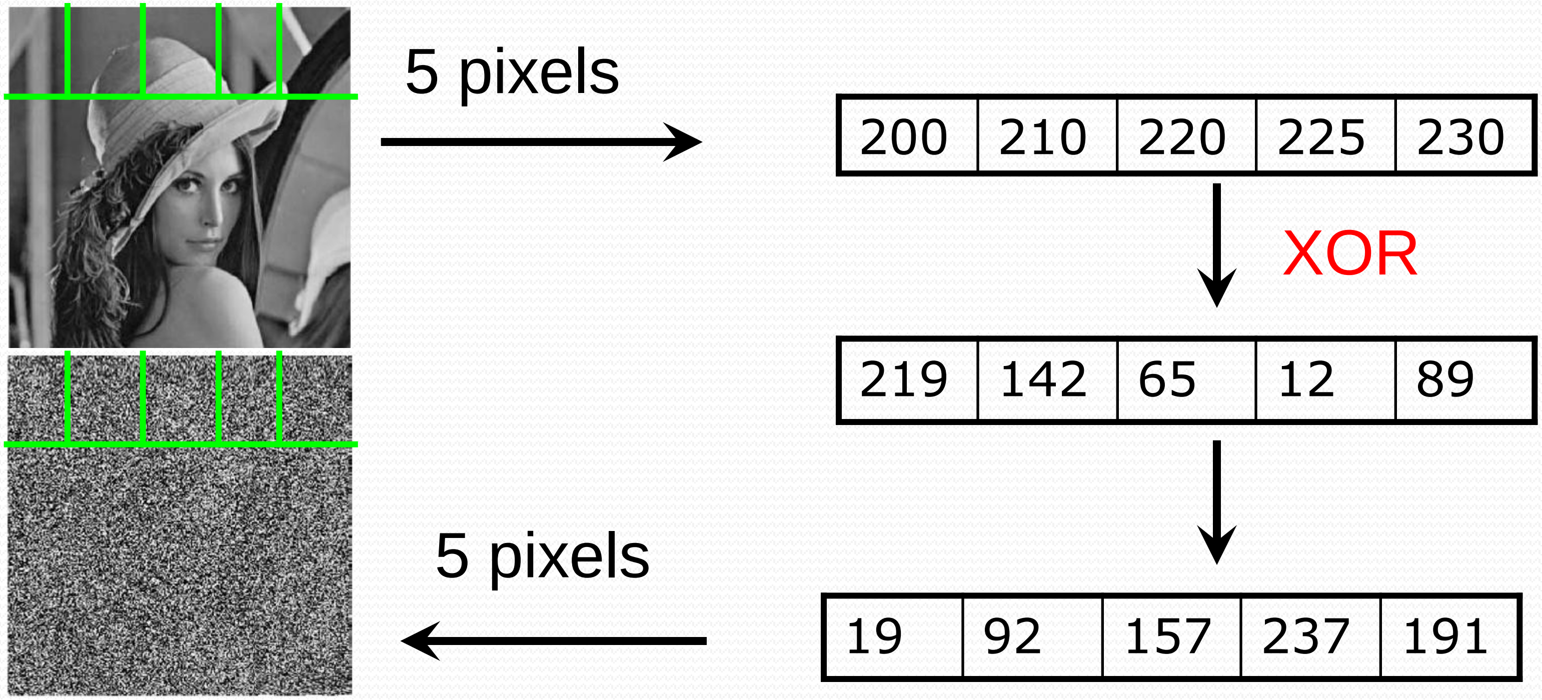
XOR and Output

encrypted image

pixels of Lena

Encryption algorithm

- Secret key
- (x_0, α, β)=(0.98765432101234 5, 1.1, 5)
- 987 mod 256=219, 654 mod 256=142, 321 mod 256=65, 012 mod 256=12, 345 mod 256=89



5 pixels

200	210	220	225	230

XOR

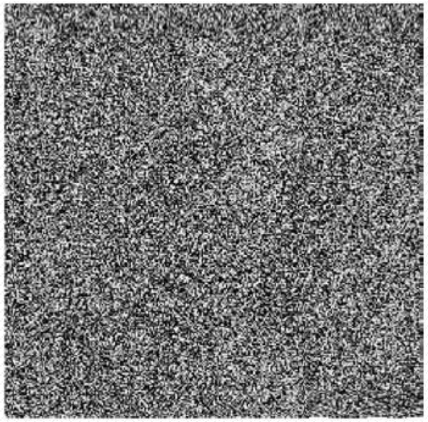
219	142	65	12	89

19	92	157	237	191

5 pixels

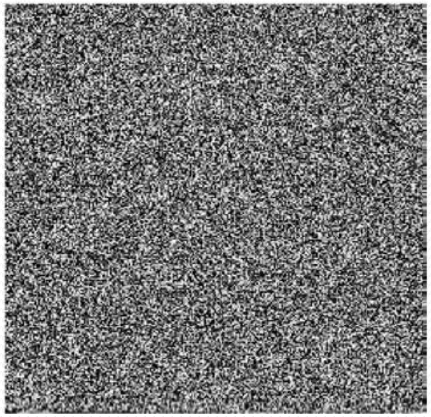
Experimental results

Encryption



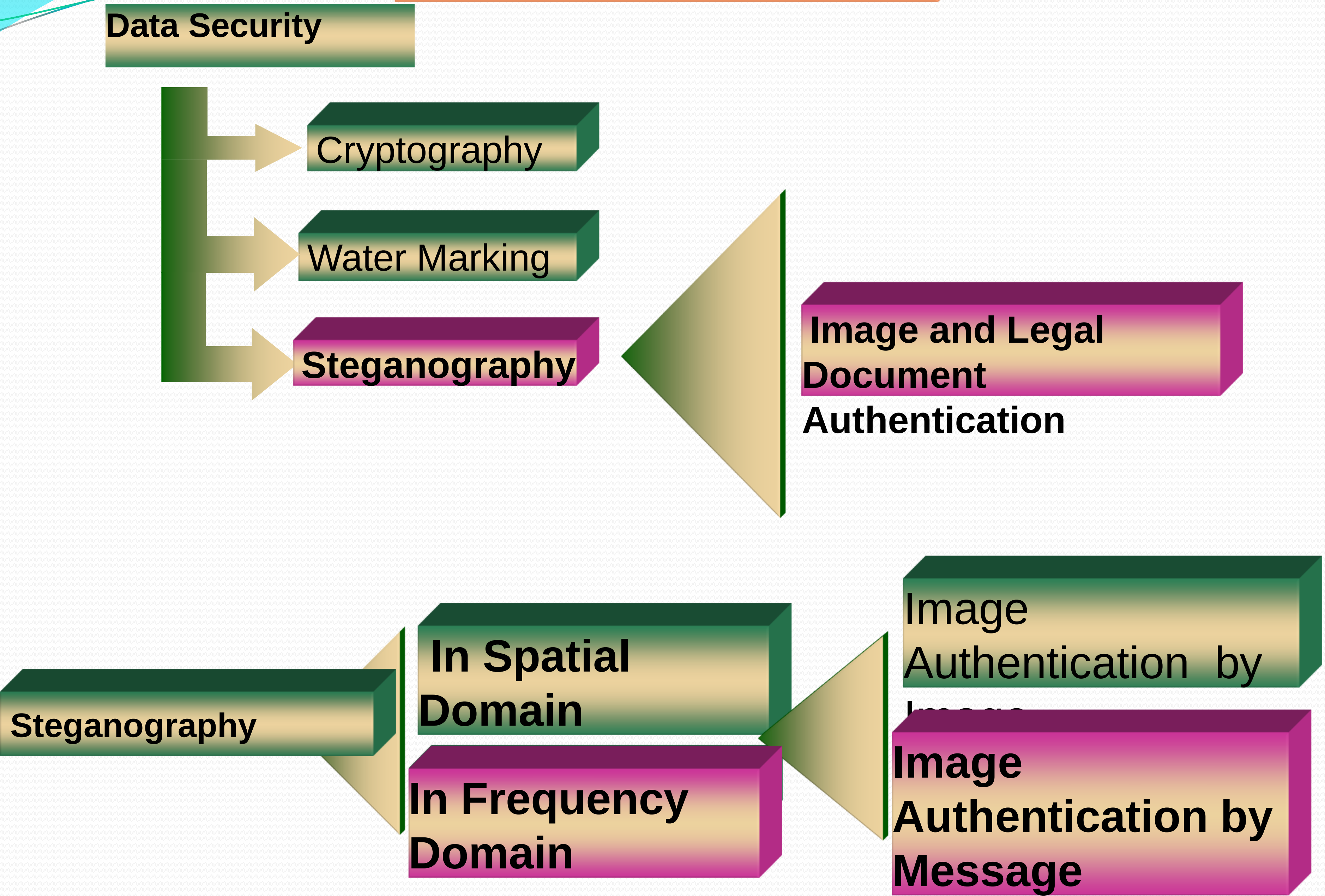
encryption key $K = (x_0, \alpha, \beta) = (0.987654321012345, 1.1, 5)$

Decryption with wrong key



wrong key $K_1 = (x_0, \alpha, \beta) = (0.987654321012346, 1.1, 5)$

PROBLEM DOMAIN



Data Security

Cryptography

Water Marking

Steganography

Image and Legal Document Authentication

Steganography

In Spatial Domain

In Frequency Domain

Image Authentication by Image

Image Authentication by Message

STEGANOGRAPHY

Steganography

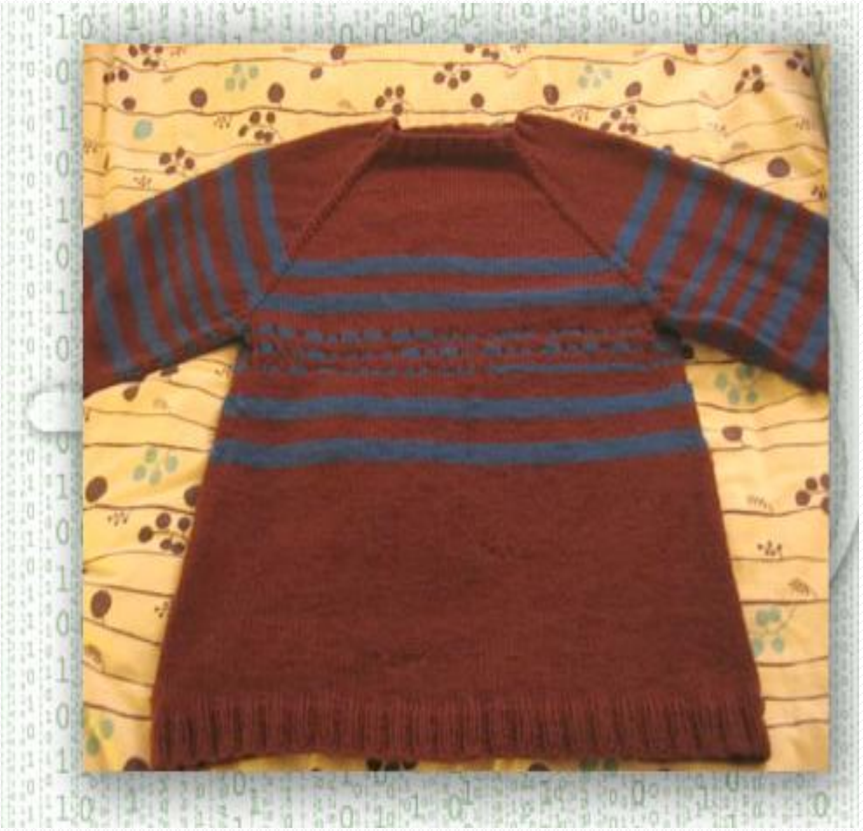
Second Example

An ancient Greek named Histaiaeus was fomenting revolt against the king of Persia and needed to pass along a message secretly. He shaved the head of a slave, tattooed the message on his scalp, then sent him on his way when his hair grew back in. Recipients of the message shaved his head again to read the alert. The Greeks used the same trick shaving and writing on the belly of a rabbit.

Third Example

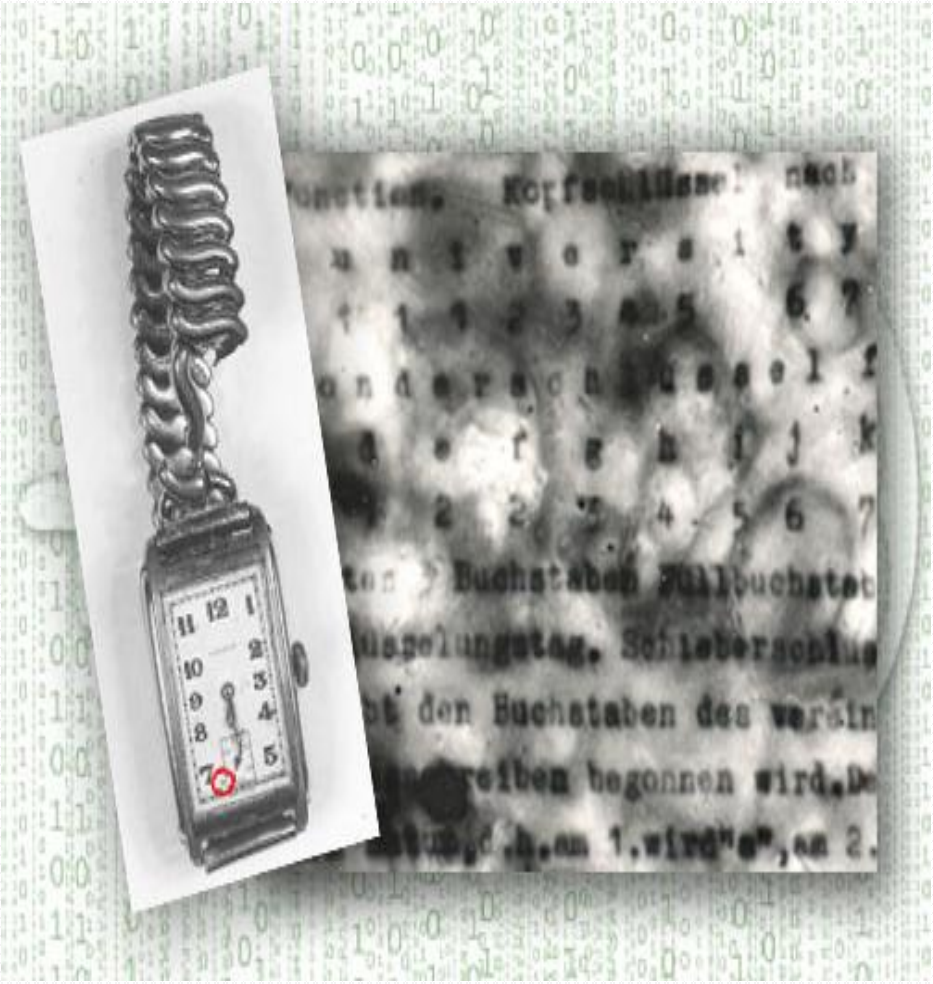
Sometime in the 5th century B.C., an exiled Greek named Demaratus wrote a warning that the Persians planned to attack Sparta. He wrote the message on the wooden backing for a wax tablet, then hid it by filling in the wood frame with wax so it looked like a tablet containing no writing at all. The wife of the Spartan king divined that there was a message behind the wax, so they scraped it off and got the warning in time to set up a desperate defence at Thermopylae, incidentally giving modern screenwriters the plot for the movie The 300.

FOURTH EXAMPLE



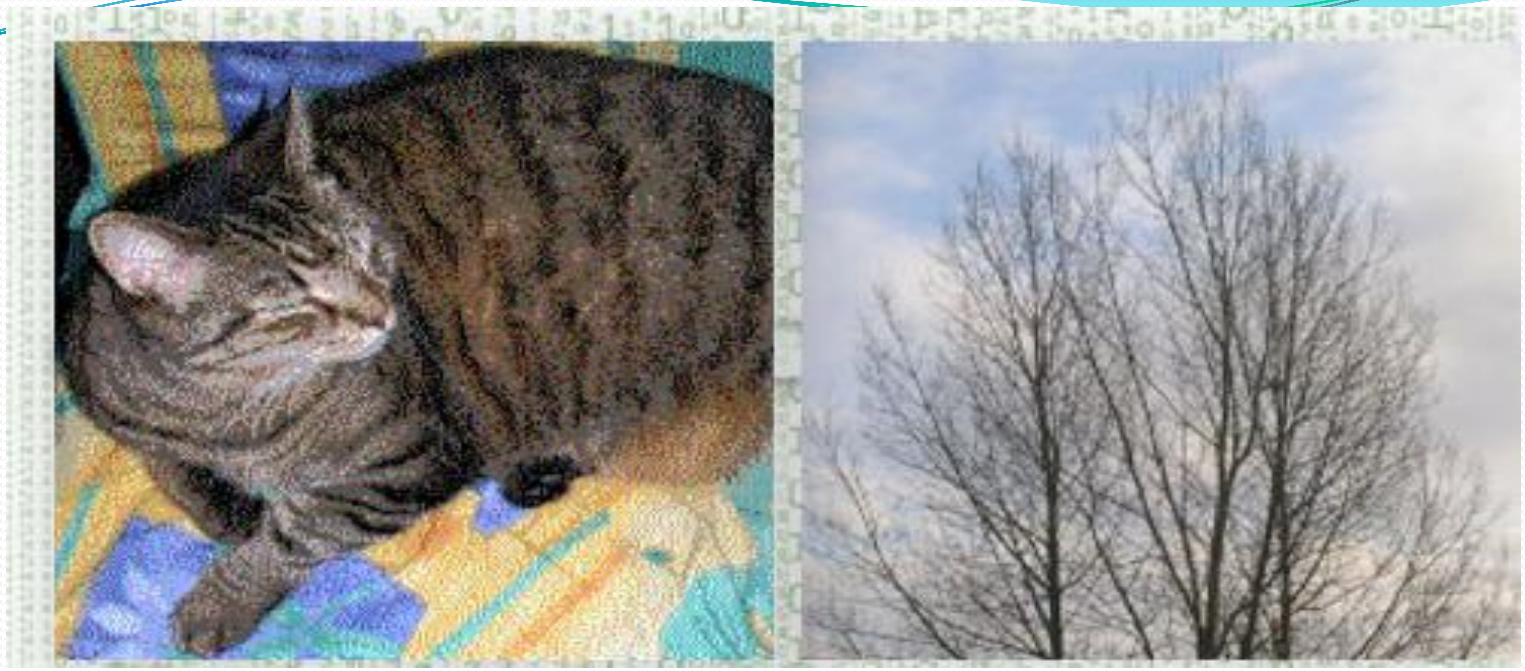
Encoded messages have been knitted into sweaters and other garments. In this example, the blue dotted lines are Morse Code for, "My girlfriennd knit this." Yes, the sweater has a typo – an extra n in girlfriend - according to the woman who knitted it.

FIFTH EXAMPLE


Kopfschlüsse nach
Buchstaben Füllbuchstaben
den Buchstaben des verein
geschrieben begonnen wird.
d.h.am 1.wird"e",am 2.

During World War II, microdots - miniaturized photos that can be hidden in plain sight, then read using magnifiers – were used by spies to carry data out of enemy countries. Here the microdot circled in red piggybacks on a watch face. Blown up, it reveals a message written in German.

Seventh Example



Digital photo steganography uses code fields for unimportant bits as places to hide encoded messages or images. While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. In these pictures, the image of the cat has been embedded in the image of the branches against the sky.

Applications Steganography

1. Usage in modern printers

   Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2. Usage in Legal document

   Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified, copyright protection, Bank draft, cheque and many other.

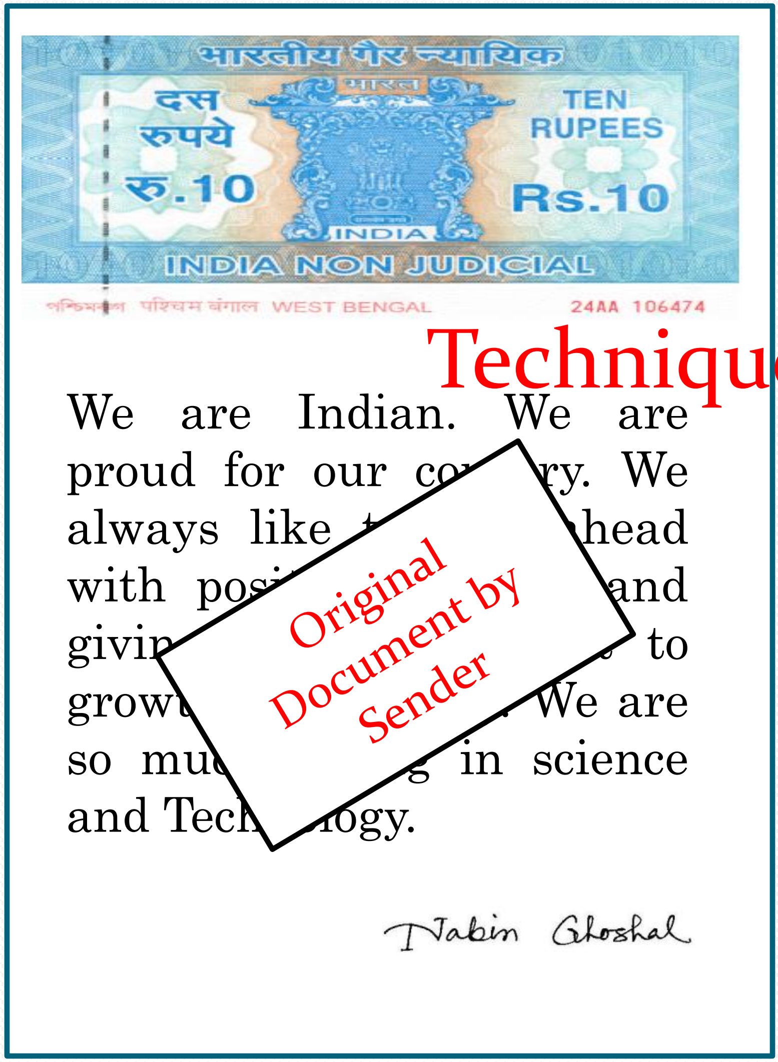
3. Steganography in audio can be used with mobile phone.

Rumored Usage in Terrorism

Rumors about terrorists using steganography started first in the daily newspaper USA Today on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July of the same year, the information looked even more precise: "Militants wire Web with links to jihad".

DOCUMENT AUTHENTICATION

Technique to Authenticate



भारतीय गैर न्यायिक

दस रुपये

रु.10

भारत

TEN RUPEES

Rs.10

INDIA

INDIA NON JUDICIAL

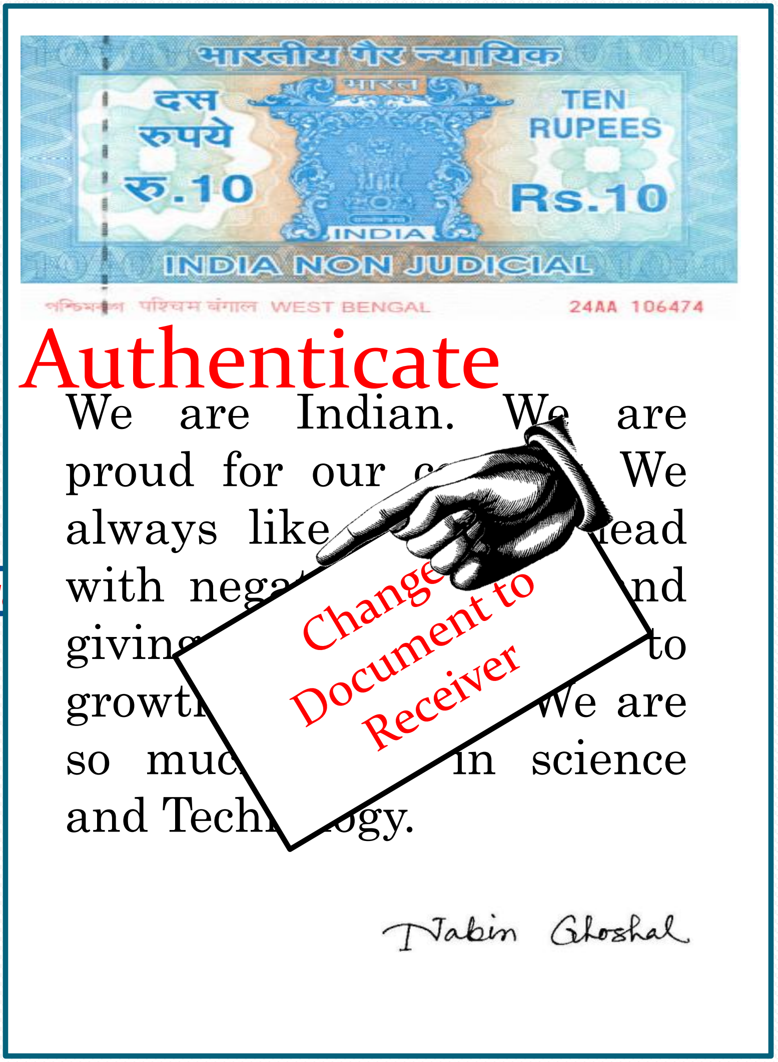
পশ্চিমবঙ্গ पश्चिम बंगाल WEST BENGAL 24AA 106474

We are Indian. We are proud for our co ry. We always like t head with posi and givi e to grow . We are so mu g in science and Tech ogy.

Original Document by Sender

Nabin Ghoshal

Tr



भारतीय गैर न्यायिक

दस रुपये

रु.10

भारत

TEN RUPEES

Rs.10

INDIA

INDIA NON JUDICIAL

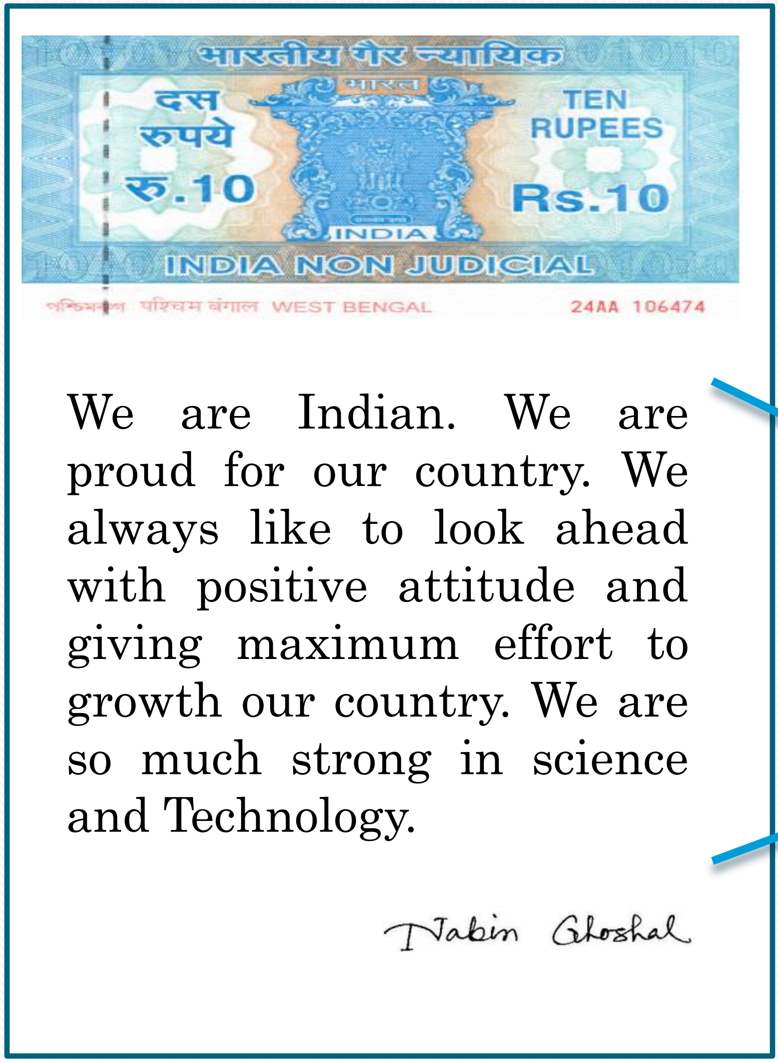
পশ্চিমবঙ্গ पश्चिम बंगाल WEST BENGAL 24AA 106474

We are Indian. We are proud for our c We always like ead with nega nd givin to growt We are so muc in science and Techn ogy.

Change Document to Receiver

Nabin Ghoshal

Document Authentication

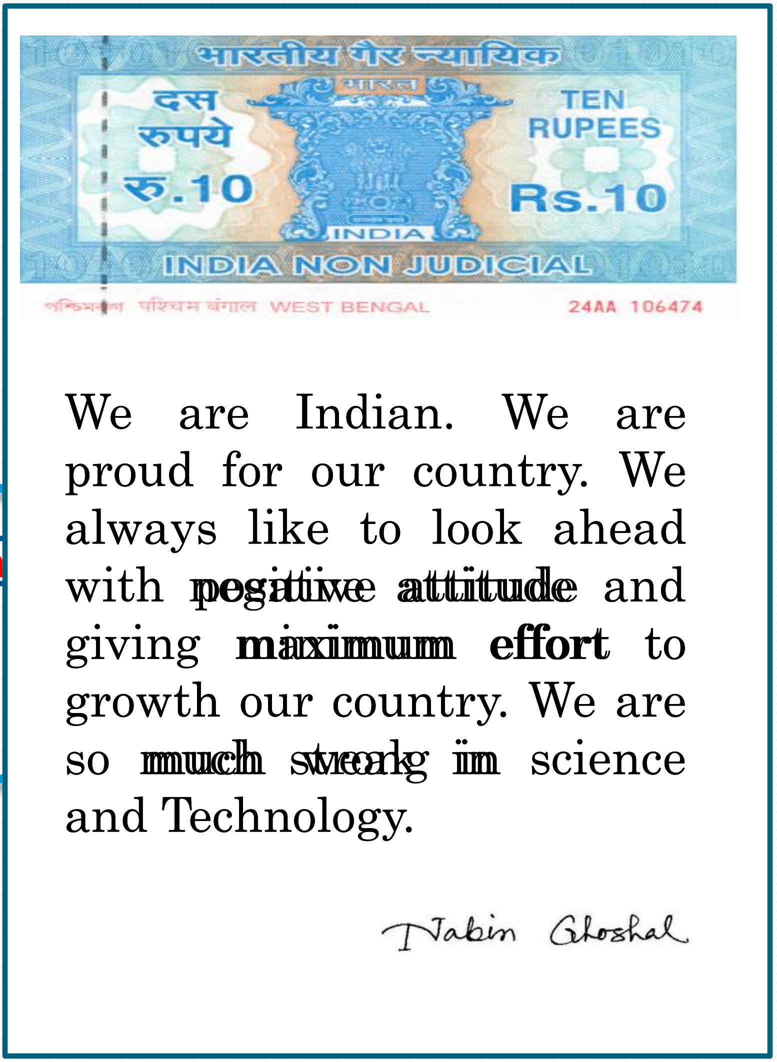


भारतीय गैर न्यायिक
दस रुपये
रु.10
भारत
TEN RUPEES
Rs.10
INDIA
INDIA NON JUDICIAL
পশ্চিমবঙ্গ पश्चिम बंगाल WEST BENGAL
24AA 106474

We are Indian. We are proud for our country. We always like to look ahead with positive attitude and giving maximum effort to growth our country. We are so much strong in science and Technology.

Nabin Ghoshal

Tran

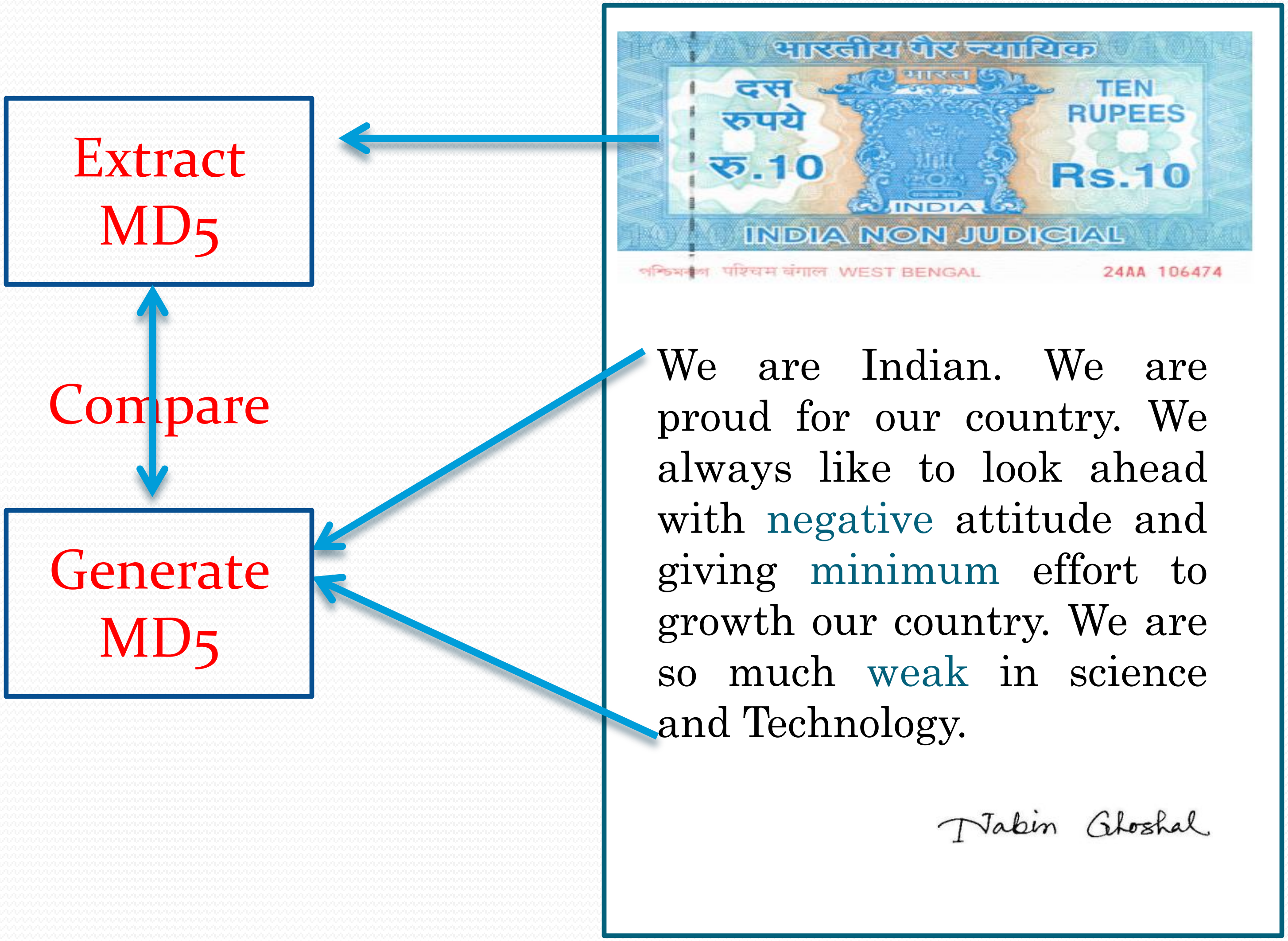


भारतीय गैर न्यायिक
दस रुपये
रु.10
भारत
TEN RUPEES
Rs.10
INDIA
INDIA NON JUDICIAL
পশ্চিমবঙ্গ पश्चिम बंगाल WEST BENGAL
24AA 106474

We are Indian. We are proud for our country. We always like to look ahead with negative attitude and giving minimum effort to growth our country. We are so much weak in science and Technology.

Nabin Ghoshal

Document Authentication

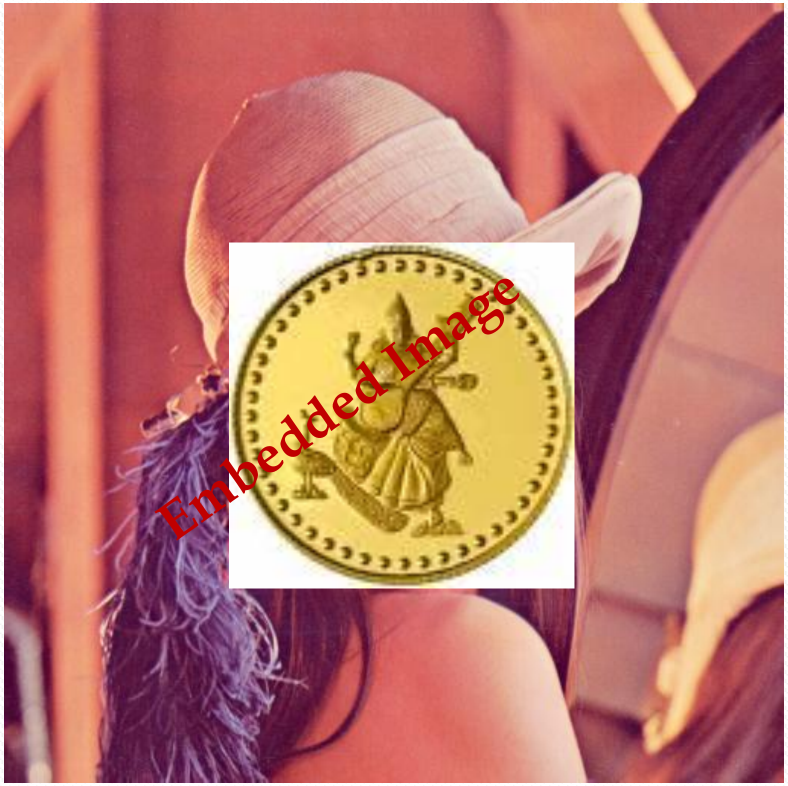


We are Indian. We are proud for our country. We always like to look ahead with negative attitude and giving minimum effort to growth our country. We are so much weak in science and Technology.

Nabin Ghoshal

IMAGE AUTHENTICATION

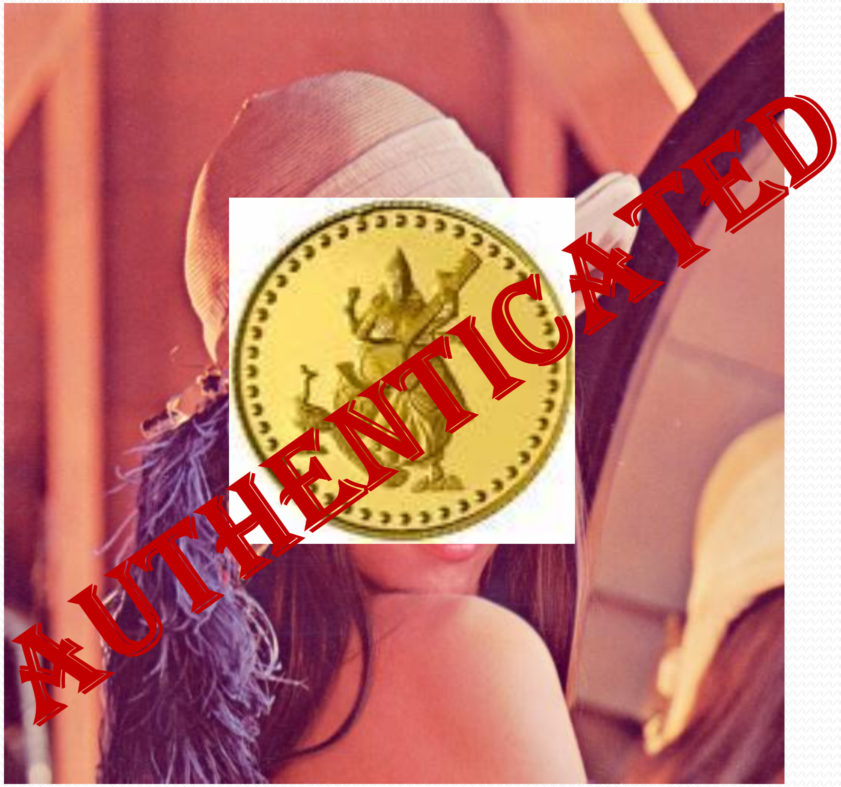
Lena Image



Lena Image

SENDER SIDE OPERATION

IMAGE AUTHENTICATION



Embedded Lena Image

Original Secret Image

COMPARE

Extracted Image

RECEIVER SIDE OPERATION

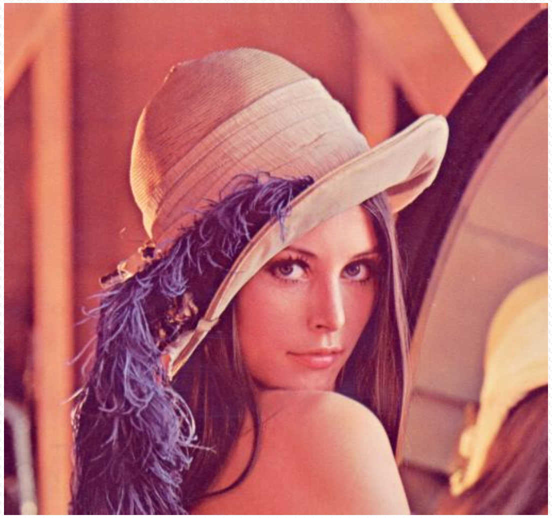
Objectives of Image Steganography

- Data Hiding
- Secured message Transmission
- Invisible data transmission
- Ownership verification

IMAGE STEGANOGRAPHY

Source Image Lenna

Authenticating Image Earth

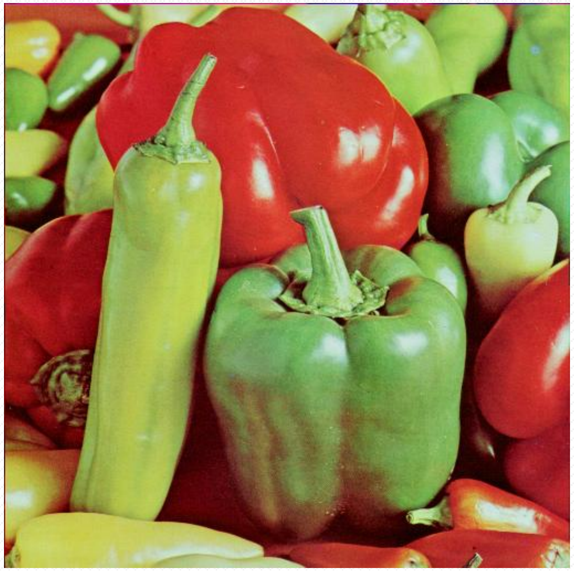


Authenticated Image Lenna

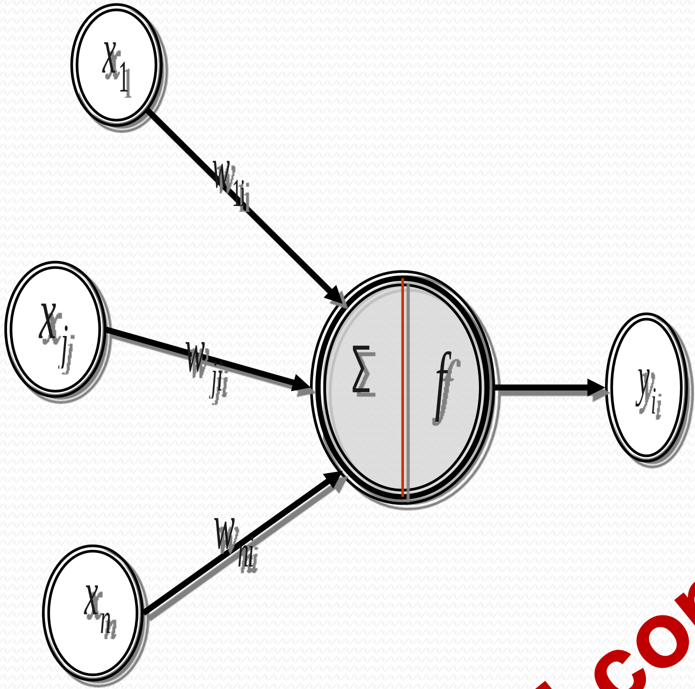
IMAGE STEGANOGRAPHY

Source Image Peppers

Authenticating Image

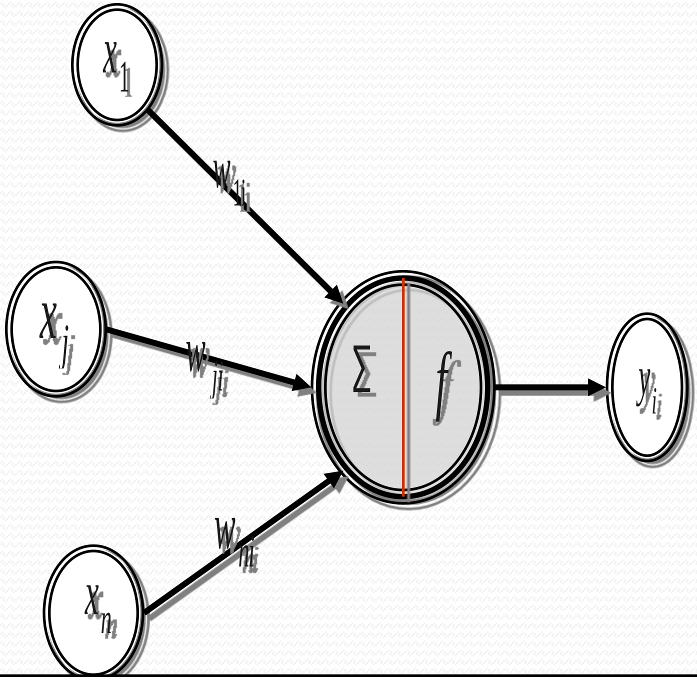


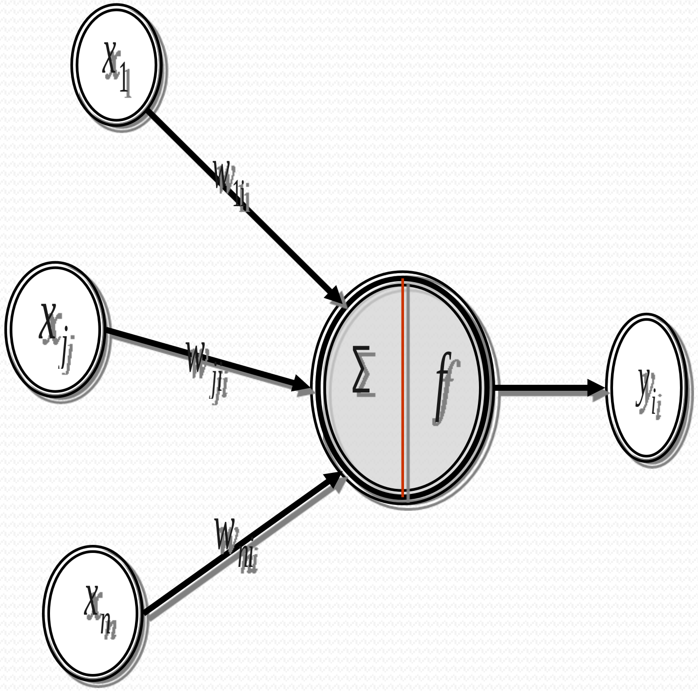
Embedded Image Peppers



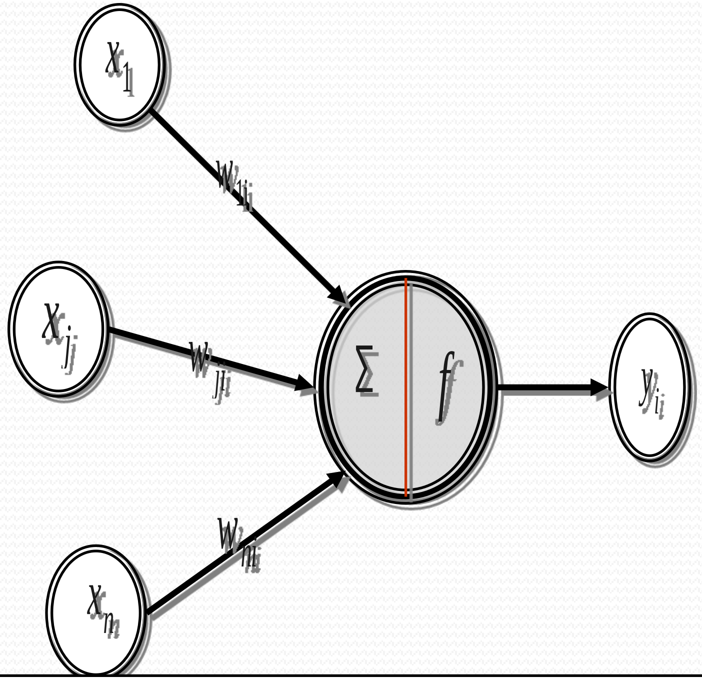
Questions?

jkm.cse@gmail.com





Thanks



THANK YOU