

Introduction to security

Dr. Bhawana Rudra

NITK

- Disclaimer: The information provided in this presentation are considered from various sources of the web.

Security

- Dictionary.com says:

1. Freedom from risk or danger; safety.
 2. Freedom from doubt, anxiety, or fear; confidence.
 3. Something that gives or assures safety, as:
 - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
 - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
 - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.
- ...etc.

Some Basic Terminology

- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering plaintext from ciphertext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (codebreaking) - study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - field of both cryptography and cryptanalysis

What is Cryptography

- the art of writing or solving codes.
- Cryptography = the science (art) of encryption
- Cryptanalysis = the science (art) of breaking encryption
- Cryptology = cryptography + cryptanalysis

What is Cryptography

- Cryptography
 - In a narrow sense
 - Mangling information into apparent unintelligibility
 - Allowing a secret method of un-mangling
 - In a broader sense
 - Mathematical techniques related to information security
 - About secure communication in the presence of adversaries
- Cryptanalysis
 - The study of methods for obtaining the meaning of encrypted information without accessing the secret information
- Cryptology
 - Cryptography + cryptanalysis

Need of Security

- Protect vital information while still allowing access to those who need it
 - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
 - Ex: AFS
- Guarantee availability of resources
 - Ex: 5 9's (99.999% reliability)

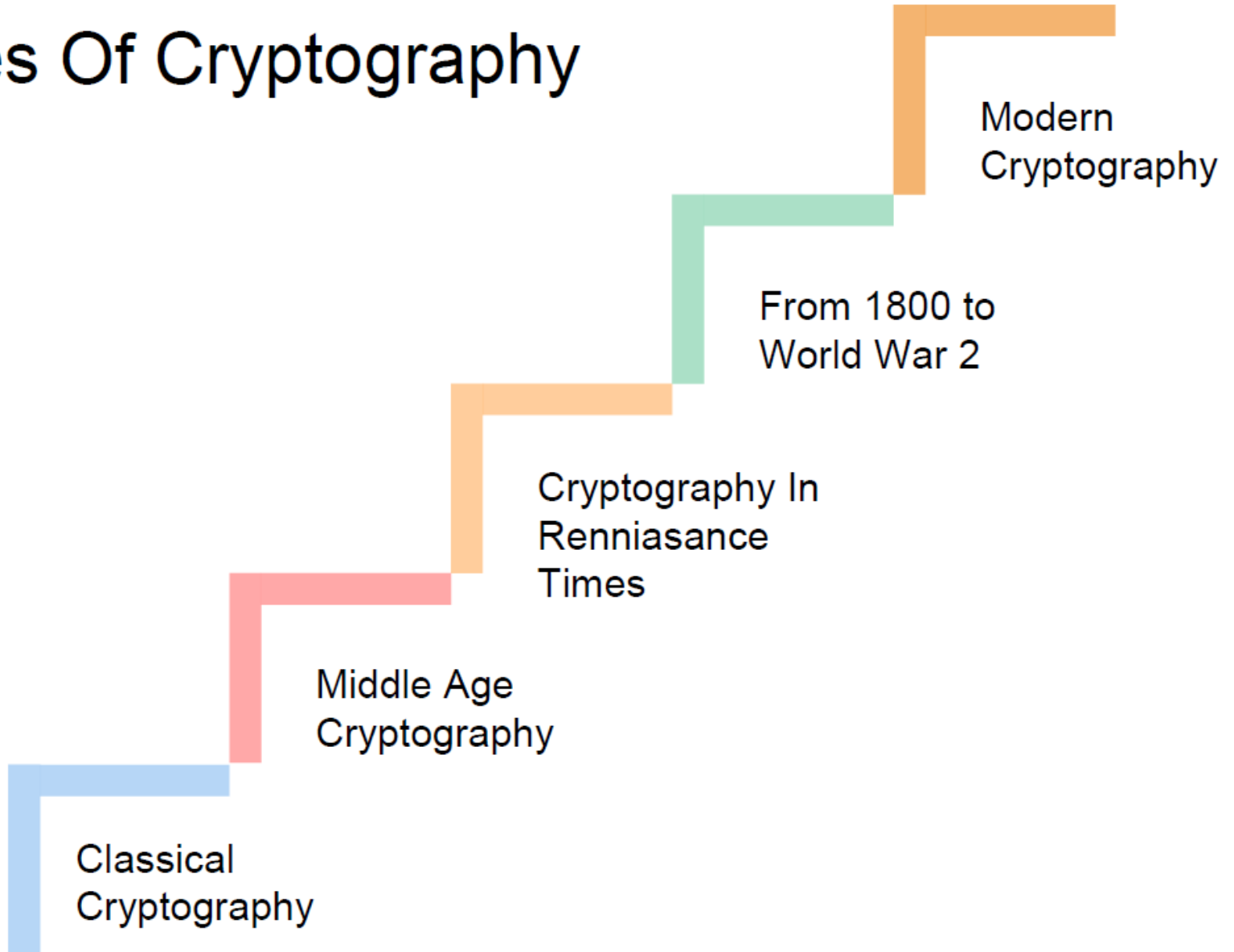
- The network needs security against attackers and hackers.
- Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers.
- Here network security not only means security in a single network rather in any network or network of networks.

Now our need of network security has broken into two needs. One is the need of information security and other is the need of computer security.

- On internet or any network of an organization, thousands of important information is exchanged daily.
- This information can be misused by attackers. The information security is needed for the following given reasons.
- To protect the secret information users on the net only. No other person should see or access it.

- To protect the information from unwanted editing, accidentally or intentionally by unauthorized users.
- To protect the information from loss and make it to be delivered to its destination properly.
- To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broker and denies for the order after two days as the rates go down.
- To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favorable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.
- To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
- To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

Ages Of Cryptography



Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

The **History of Cryptography** begins thousands of years ago. Until recent decades, it has been the story of what might be called classical cryptography.

That is, methods of encryption that use pen and paper, or perhaps simple mechanical aids.

Classical Cryptography
Egypt's Old Kingdom

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

The earliest known use of cryptography is found in non-standard hieroglyphs carved into monuments from Egypt's Old Kingdom (4500+ years ago).



Classical Cryptography

Clay Tablets

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

Some clay tablets from Mesopotamia are clearly meant to protect information—they encrypt recipes, presumably commercially valuable.



- The scytale was first mentioned by the Greek poet Archilochus who lived in the 7th century B.C. (over 2500 years ago).
- The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns

Classical Cryptography Scytale

Medieval Cryptography

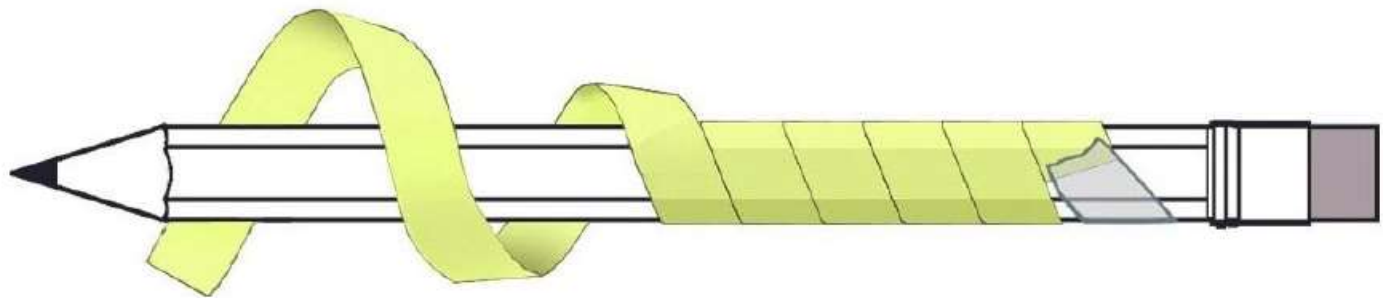
In Renaissance Times

1800 to World War 2

Modern Cryptography

❖ Sender and recipient each had a cylinder (called a scytale) of exactly the same radius. The sender wound a narrow ribbon of parchment around his cylinder, then wrote on it lengthwise.

❖ After the ribbon is unwound, the writing could be read only by a person who had a cylinder of exactly the same radius.



Classical Cryptography

Scytale Example

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

❖ **Original message:**

Kill king tomorrow midnight

❖ **Write Lengthwise:**

k i l l k i n g
t o m o r r o w
m i d n i g h t

❖ **Encoded message:**

ktm ioi lmd lon kri irg
noh gwt

Classical Cryptography
Polybius Square

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

Another Greek method was developed by Polybius (called the "Polybius Square").

Each letter is represented by its coordinates in the grid. Example, "BAT" becomes "12 11 44"

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Classical Cryptography
Caesar Cipher

Medieval Cryptography

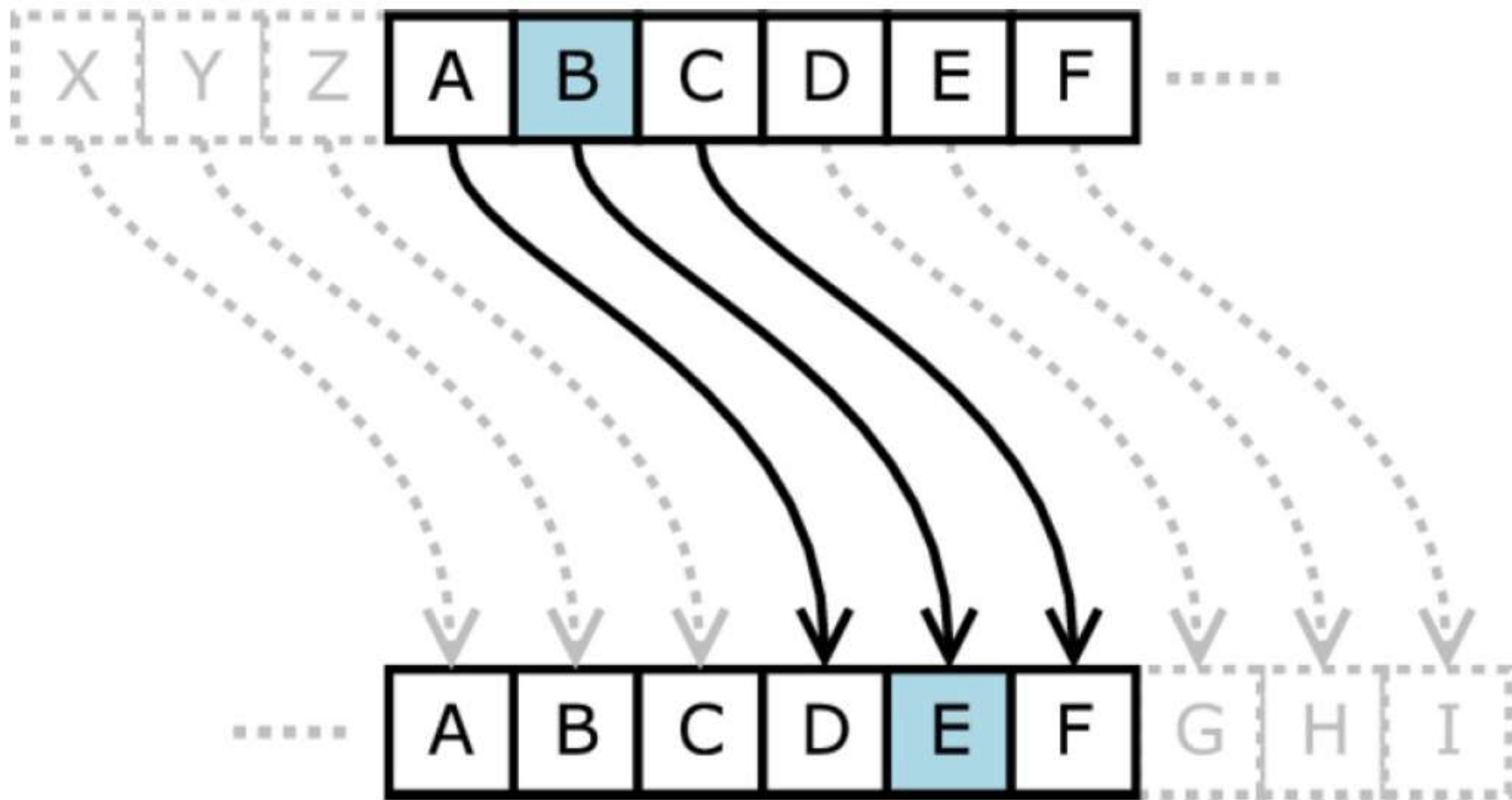
In Renaissance Times

1800 to World War 2


Modern Cryptography

Romans Caesar Cipher:
The method is named after Julius Caesar, who used it to communicate with his generals.

The Caesar Cipher is an example of what is called a shift cipher. To encode a message, letters are replaced with a letter that is a fixed number of letters beyond the current letter.



- **Rail Fence cipher**
- Plain Text: I CAME I SAW I CONQUERED
- write message with letters on alternate rows
- read off cipher row by row
- Plain: I A E S W C N U R D
C M I A I O Q E E
- Cipher: IAESW CNURD CMIAI OQEE



Classical Cryptography
Monoalphabetic Cipher

Medieval Cryptography

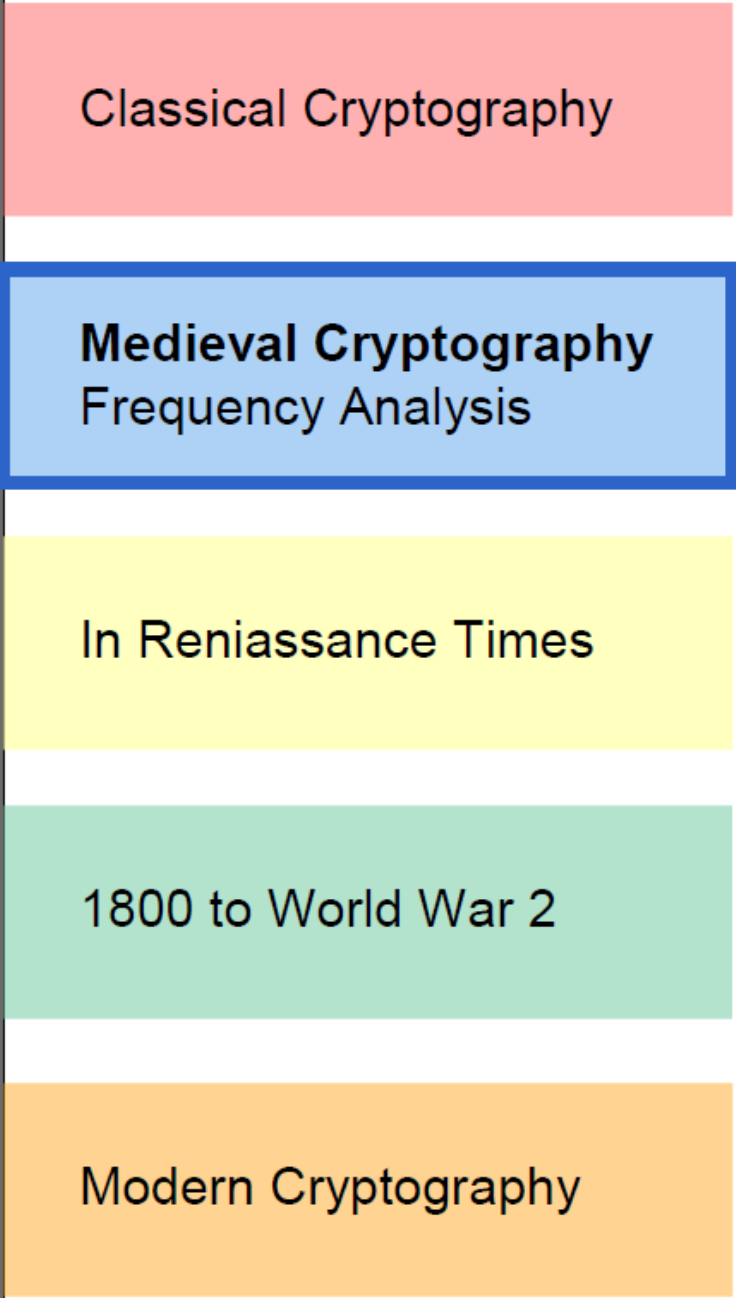
In Renaissance Times

1800 to World War 2

Modern Cryptography

Hebrew scholars made use of simple monoalphabetic substitution ciphers.

The Atbash cipher is a specific case of substitution cipher where the letters of the alphabet are reversed. In other words, all As are replaced with Zs, all Bs are replaced with Ys, and so on.



Classical Cryptography

Medieval Cryptography
Frequency Analysis

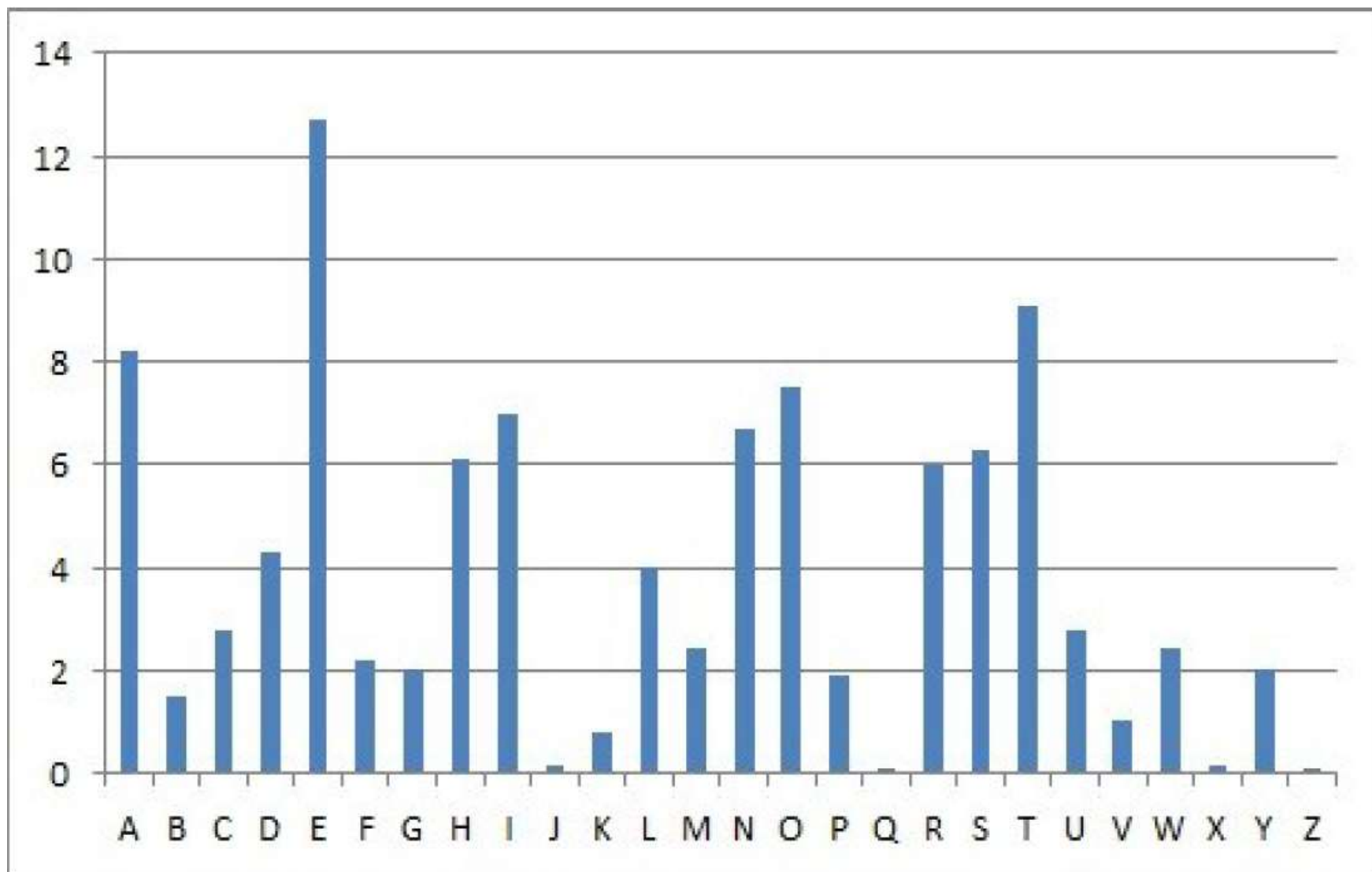
In Renaissance Times

1800 to World War 2

Modern Cryptography

Al - Kindi, wrote a book on cryptology, the "Risalah fi Istikhraj al-Mu'amma" (Manuscript for the Deciphering Cryptographic Messages), circa 850 CE.

He was a pioneer in cryptanalysis and cryptology, and devised new methods of breaking ciphers, including the frequency analysis method.



Classical Cryptography
Caesar Cipher

Medieval Cryptography

In Renaissance Times
Polyalphabetic Cipher

1800 to World War 2

Modern Cryptography

Essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis until the development of the polyalphabetic cipher.

The polyalphabetic cipher was explained by Leon Battista Alberti around the year 1467, for which he was called the "father of Western cryptology".

**CIPHER ALPHABET
for the first letter**

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

**CIPHER ALPHABET
for the second letter**

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

Figure 2

STUDENTS = XHTQKEMG

Polyalphabetic Cipher

Classical Cryptography
Caesar Cipher

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography

In Europe, cryptography became (secretly) more important as a consequence of political competition and religious revolution.

Outside of Europe, after the end of the Muslim Golden Age at the hand of the Mongols, cryptography remained comparatively undeveloped.

Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2
Systematic methods

Modern Cryptography

Edgar Allan Poe used systematic methods to solve ciphers in the 1840s. In particular he placed a notice of his abilities in the Philadelphia paper, inviting submissions of ciphers, of which he proceeded to solve almost all.

Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2
Systematic methods

Modern Cryptography

His success created a public stir for some months. He later wrote an essay on methods of cryptography which proved useful as an introduction for novice British cryptanalysts attempting to break German codes and ciphers during World War I.

Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2
Electro mechanical

Modern Cryptography

In 1917, Gilbert Vernam proposed a teletype cipher in which a previously-prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cyphertext. This led to the development of electromechanical devices as cipher machines.

Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2
Enigma and SIGABA

Modern Cryptography

By World War II, mechanical and electromechanical cipher machines were in wide use, although—where such machines were impractical—manual systems continued in use.

The Enigma machine was widely used by Nazi Germany where as SIGABA was used by British army.



Classical Cryptography

Medieval Cryptography

In Renaissance Times

1800 to World War 2

Modern Cryptography
Claude Shannon

Availability of computers, and the Internet as a communications medium, bring effective cryptography into common use by national governments or large enterprises.

The era of modern cryptography really begins with Claude Shannon, the father of mathematical cryptography.

Classical Cryptography

Medieval Cryptography

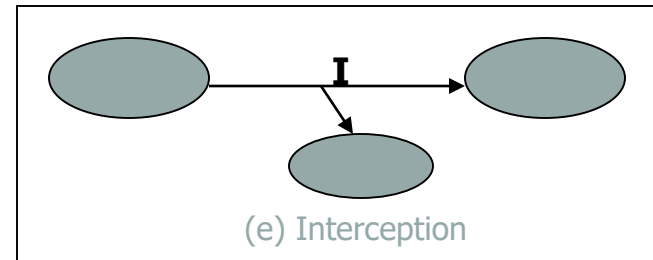
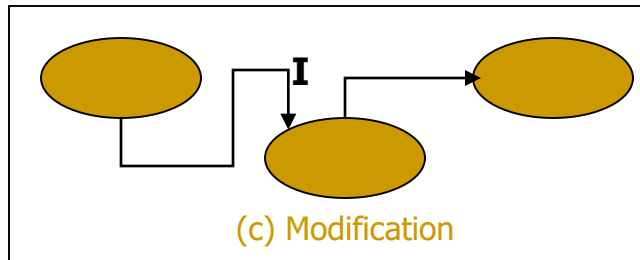
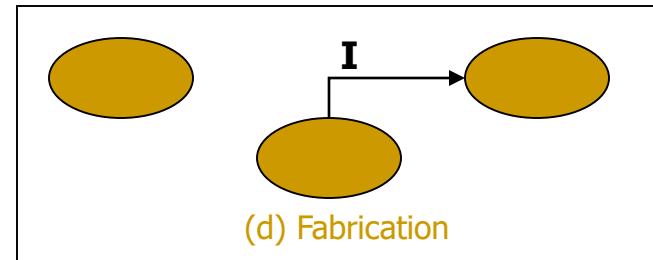
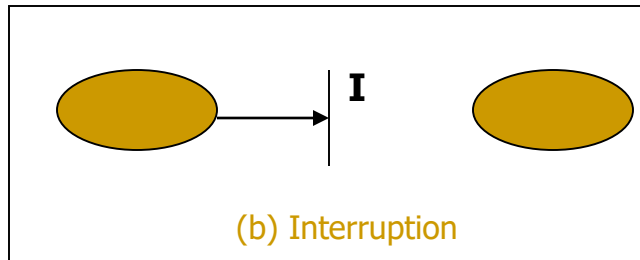
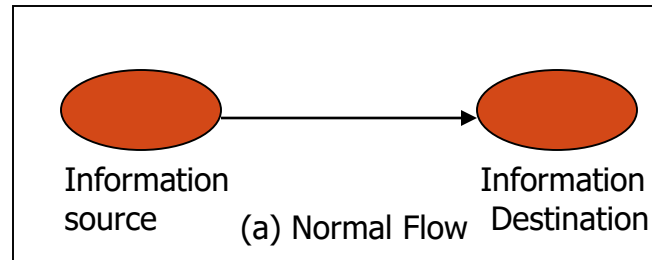
In Renaissance Times

1800 to World War 2

Modern Cryptography
Claude Shannon

He established a solid theoretical basis for cryptography and also for much of cryptanalysis. And with that, cryptography more or less disappeared into secret government communications organizations such as NSA, GCHQ, and their equivalents elsewhere.

- These are actions that compromise the security of information owned or transferred by an entity. Attacks can be one of 4 forms:
- **Interruption**
- **Interception**
- **Modification**
- **Fabrication**



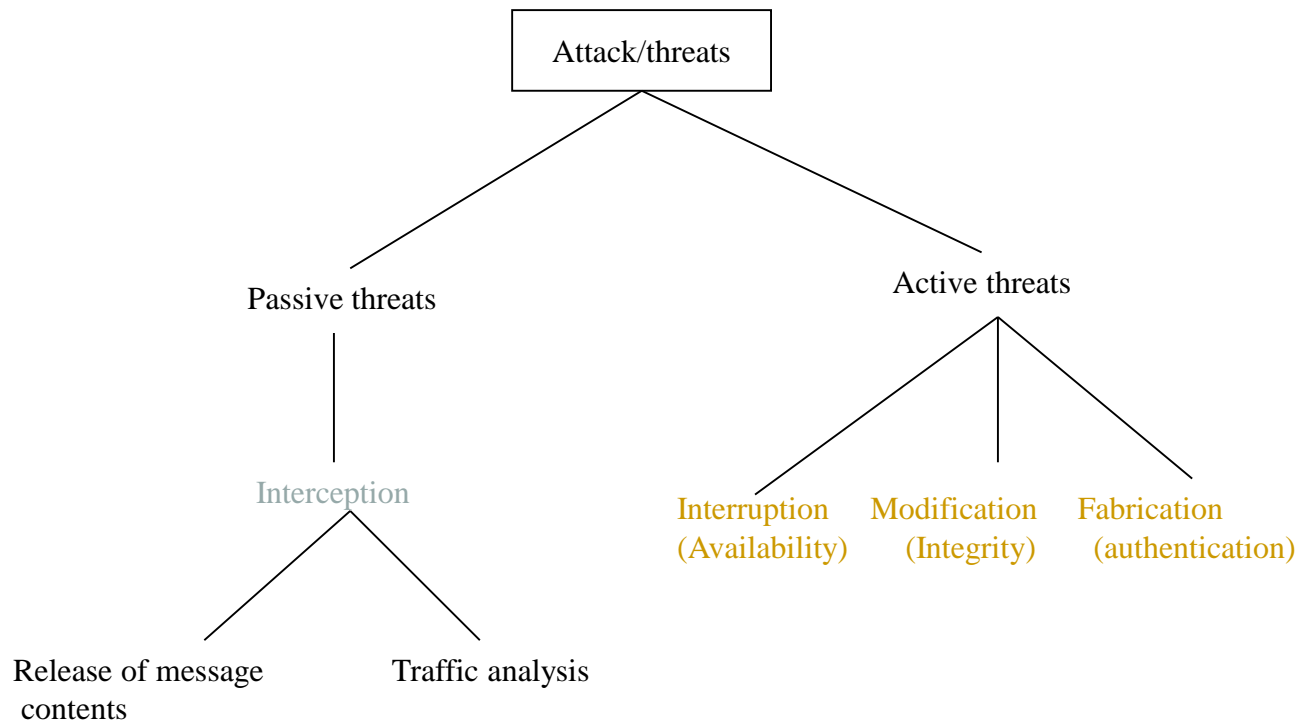
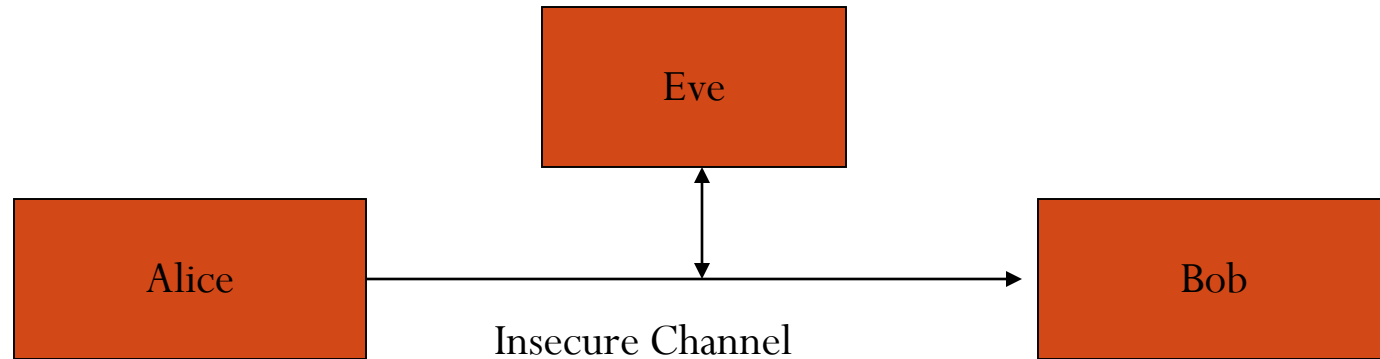


Figure 2: Threats/Attacks

Security Attacks

- Passive attacks
 - Obtain message contents
 - Monitoring traffic flows
- Active attacks
 - Masquerade of one entity as some other
 - Replay previous messages
 - Modify messages in transmit
 - Add, delete messages
 - Denial of service

Cryptography Goals



- Encryption – Prevent Eve from intercepting message
- Authentication – Prevent Eve from impersonating Alice

Who are Vulnerable

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Objectives of Information Security

- Confidentiality (secrecy)
 - Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication
 - Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity
 - The content of their communication is not altered, either maliciously or by accident, in transmission.
- Availability
 - Timely accessibility of data to authorized entities.

Objectives of Information Security

- Non-repudiation
 - An entity is prevented from denying its previous commitments or actions
- Access control
 - An entity cannot access any entity that it is not authorized to.
- Anonymity
 - The identity of an entity is protected from others.

Types of Cryptographic Functions

- Secret key functions
- Public key functions
- Hash functions

Common security attacks and their countermeasures

- Finding a way into the network
 - Firewalls
- Exploiting software bugs, buffer overflows
 - Intrusion Detection Systems
- Denial of Service
 - Ingress filtering, IDS
- TCP hijacking
 - IPSec
- Packet sniffing
 - Encryption (SSH, SSL, HTTPS)
- Social problems
 - Education

- Applications of cryptography:
 - computer and information security: cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet;
 - e-commerce, e-payment, e-voting, e-auction, e-lottery, and e-gambling schemes, are all based on cryptographic (security) protocols.