Introduction to Cryptography

Lectrue 1

Assistant Lecturer

Rasha Hussein

Dr. Eng. Sattar B. Sadkhan

Network Securty Theory & Algorithms

3rd Class-First Course

Outline

- **What is information security?**
- **Key Security Objectives or CIA Triad**
- **The Basic Problem**
- **Why study cryptology?**
- **What is Cryptography?**
- **Basic terms**
- **What is the Encryption / Decryption Process ?**
- **Structure of Cryptography , Notions , Examples of “Messages”**
- **Types of Ciphers**
- **Classical Cryptographic Techniques**
- **Substitution Ciphers System(Caesar Cipher)**
- **Modern Cryptography Applications**
- **4 types of cryptanalysis**

What is information security?

- **Information security (also known as InfoSec)** ensures that both physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. Information security differs from cybersecurity in that InfoSec aims to keep data in any form secure, whereas cybersecurity protects only digital data.

Key Security Objectives or CIA Triad

- **Confidentiality**

  - Data confidentiality: assure confidential information not made available to unauthorized individuals(for Data).

  - Privacy: assure individuals can control what information related to them is collected, stored, distributed (for people)

- **Integrity**

  - Data integrity: assure information and programs are changed only in a authorized manner

  - System integrity: assure system performs intended function

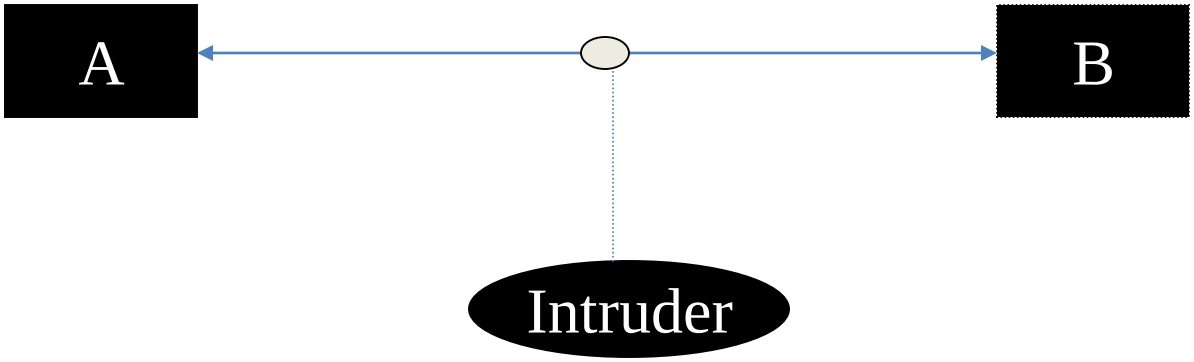
- **Availability**

  - Assure that systems work promptly and service is not denied to authorized users

The Basic Problem

- We consider the confidentiality goal:
  - Alice and Bob are Friends
  - Marvin is a rival
  - Alice wants to send secret messages (M_1,M_2,…) to Bob over the Internet
  - Rival Marvin wants to read the messages (M_1,M_2,…) - Alice and Bob want to prevent this!
  - Assumption: The network is OPEN: Marvin is able to eavesdrop and read all data sent from Alice to Bob.
  - Consequence: Alice must not send messages (M_1,M_2,…) directly – they must be "scrambled" or encrypted using a 'secret code' unknown to Marvin but known to Bob.

Why Study cryptology(1)



Communications security

What is Cryptography?

- Cryptography, a word with Greek origins, means "secret writing" However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks and to preserve confidentiality .
- Cryptography is a collection of mathematical techniques for protecting information.

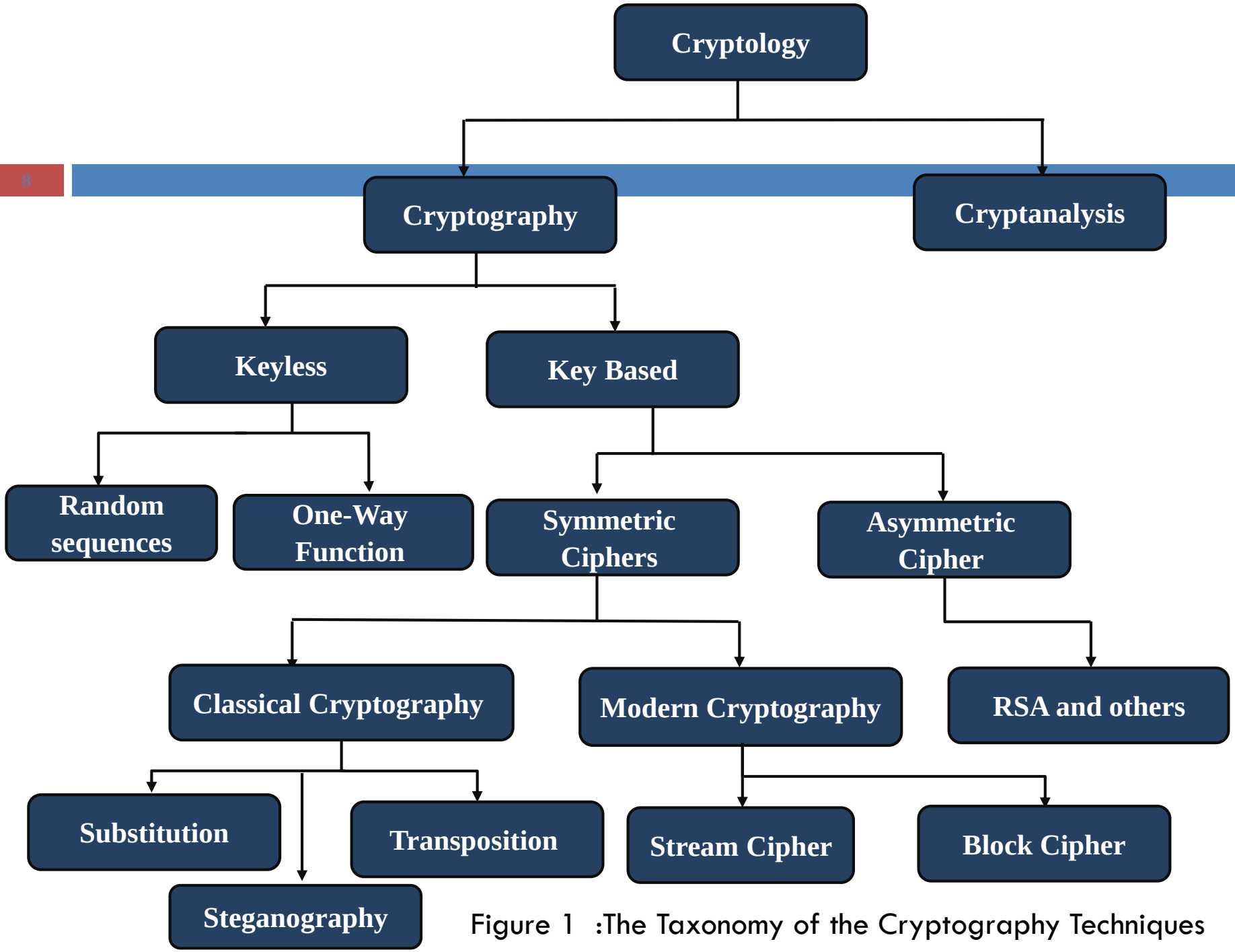


Figure 1 :The Taxonomy of the Cryptography Techniques

Basic Terms

- Cryptology (to be very precise)
  - Cryptography --- code designing
  - Cryptanalysis --- code breaking
- Cryptologist:
  - Cryptographer & cryptanalyst
- Encryption/encipherment :Scrambling data into unintelligible to unauthorised parties
- Decryption/decipherment: Un-scrambling
- Plaintext (P) : original message
- Ciphertext (C): encrypted or coded message
- Key (K): information used in cipher known only to sender/receiver
- Cipher: a particular algorithm (cryptographic system)

What is the Encryption / Decryption Process ?

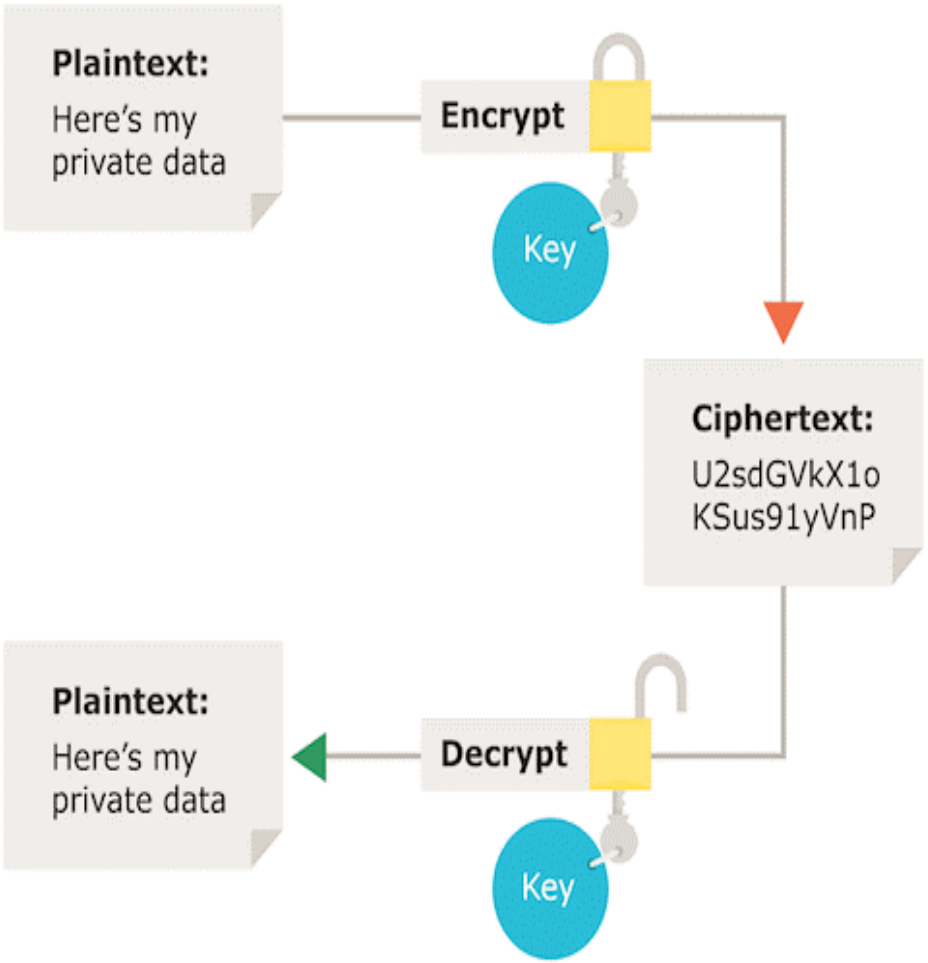
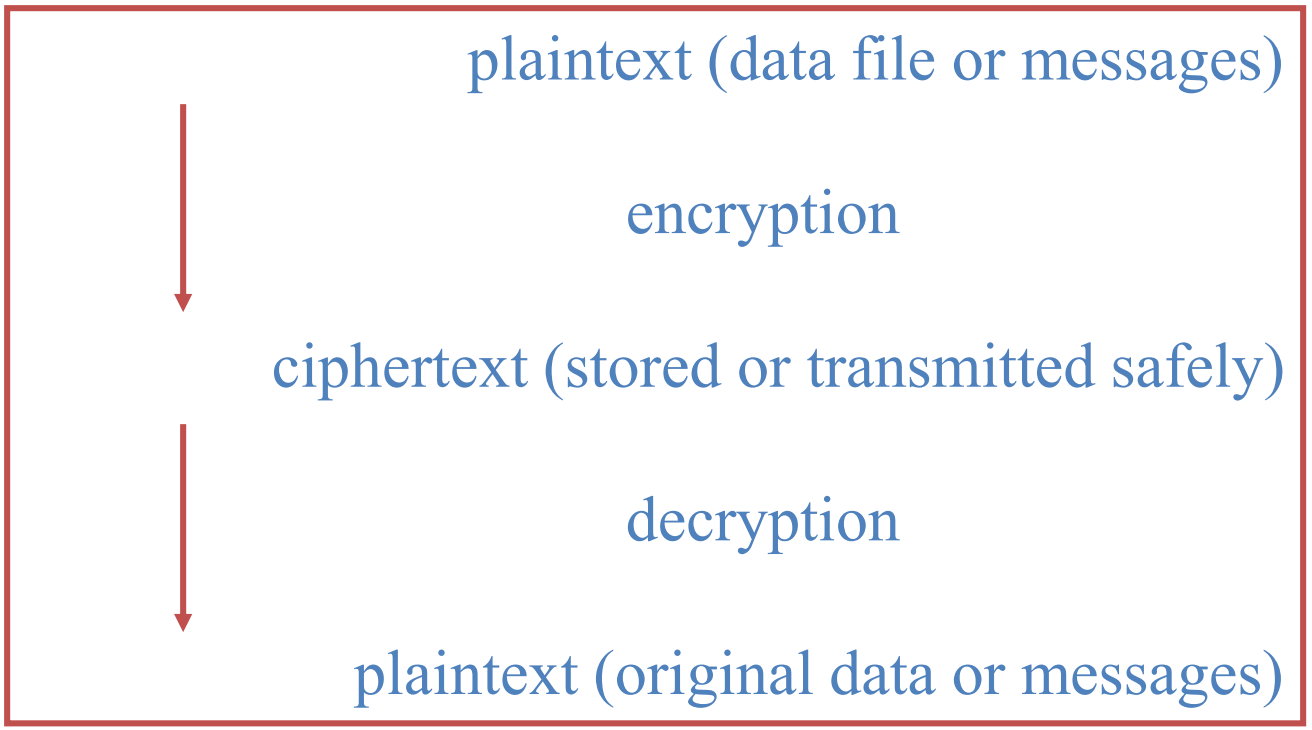


Figure 2 : Encryption / Decryption Process

- **Encryption**
  - Input: plaintext and key
  - Output: cipher text
- **Decryption**
  - Input: cipher text and a key
  - Output: original plaintext

Structure of cryptography



Notations

- Encrypt a plaintext (P) using a key (K) & an encryption algorithm (E)

  C = E(K,P)

- Decrypt a ciphertext (C) using the same key (K) and the matching decryption algorithm (D)

  P = D(K,C)

- Note: P = D(K,C) = D(K, E(K,P))

Examples of “Messages”

- Types of secret “Messages” Alice might want to send Bob (in increasing length):
  - Text : Decision (yes/no), eg. as answer to the question “Are we meeting tomorrow?”
  - Numerical Value, eg. as answer to the question “at what hour are we meeting?”
  - Document
  - Software
  - Images, etc.

Types of Ciphers

1. Public key cryptosystems/ciphers(Asymmetric Key Cryptography)
   - The secret key is not shared and two parties can still communicate using their public keys

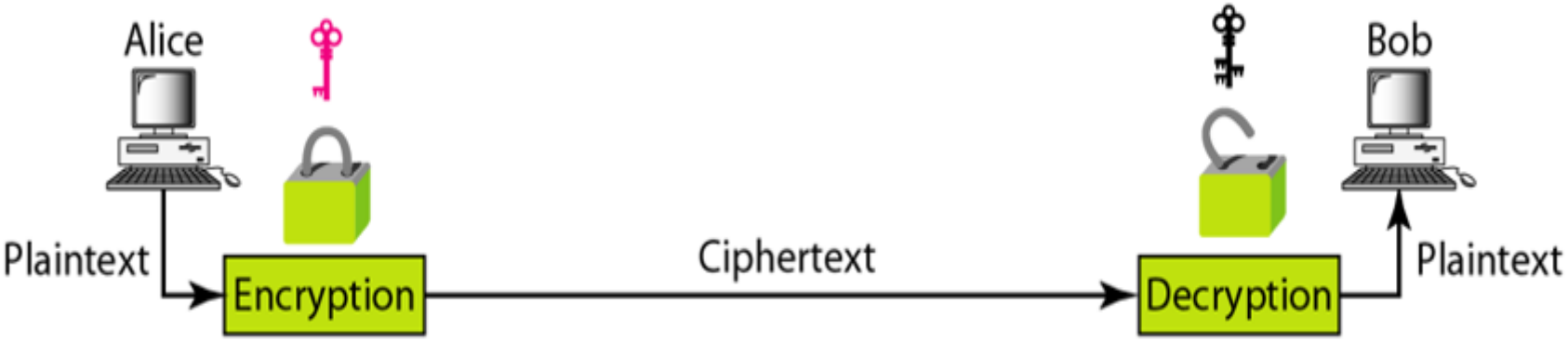


Figure 3: Asymmetric Key Cryptography

Types of Ciphers

2. Private key cryptosystems/ciphers (Symmetric Key Cryptography) :is composed of two algorithms

- encryption algorithm (E)
- decryption algorithm (D)

- A private key cipher The same key K is used for encryption & decryption
- The secret key K has to be distributed (shared) between two parties before hand.

Private key cipher

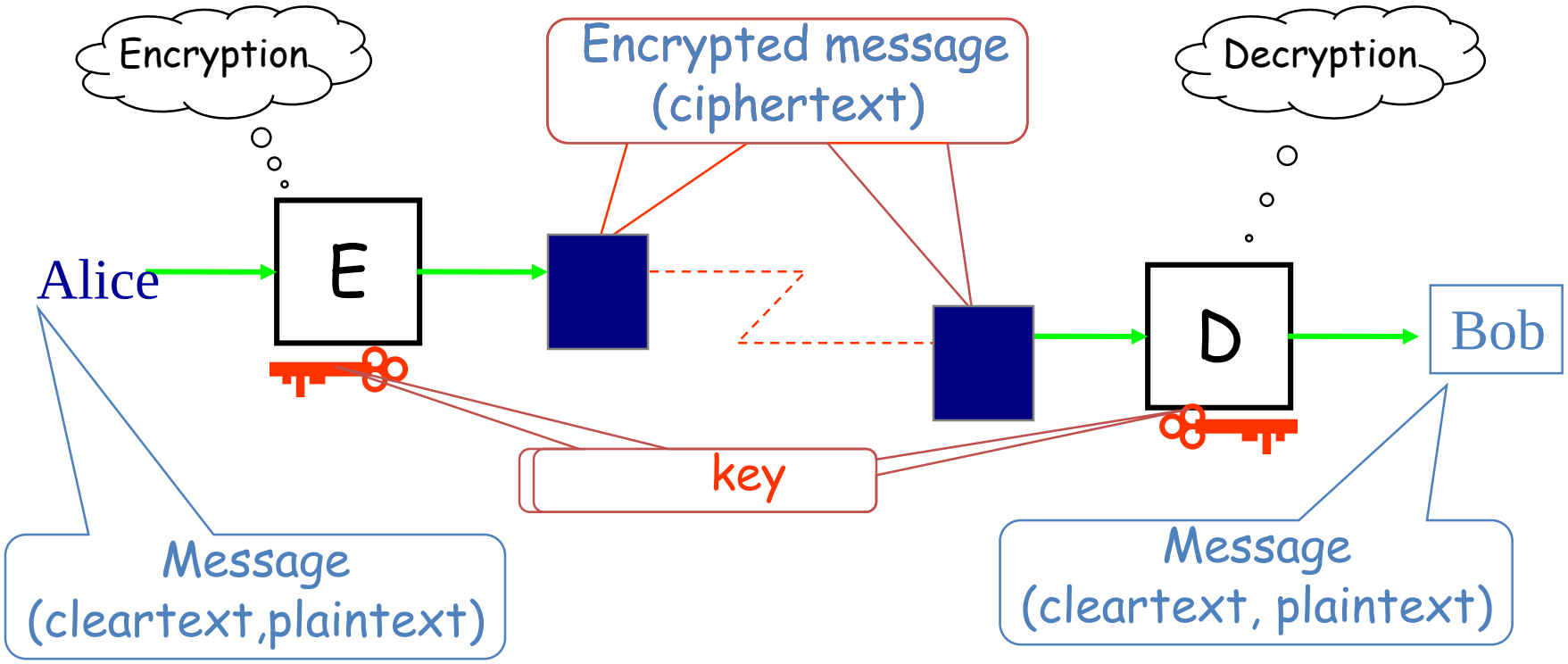


Figure 4 : Symmetric Key Cryptography

Classical Cryptographic Techniques

- Have two basic components of classical: Substitution and Transposition

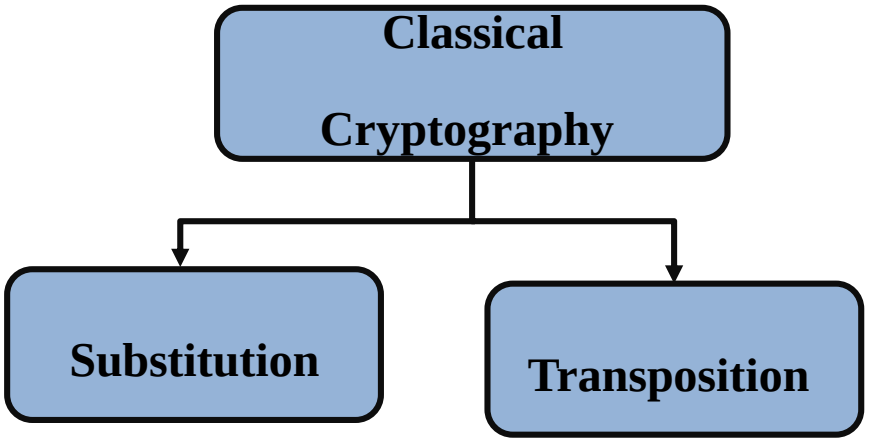


Figure 5 : **Classical Cryptography Classification**

Classical Cryptographic Techniques

- **Substitution Ciphering**: It is a process of replacing characters or symbols in the plain text or data by other characters or symbols in the encryption process. For example, replace the letter A for the letter D and letter T with letter Z.
- **Transposition Ciphering**: It is the process of reorders the letters, numbers and symbols in the plain text or data to be encrypted and placed in a different of location from its original on in the plain text or data. A symbol in first position of the plaintext may appear in the tenth position in the ciphertext.

Substitution Ciphers System

Substitution Ciphers System

1. Monoalphabetic Substitution Cipher (Simple substitution system)
2. Homophonic substitution system
3. Polyalphabetic substitution system

1. Simple Substitution System \ Mono Substitution System

- Additive Cipher (The Caesar Cipher)
- Multiplicative Cipher
- Affine Cipher
- Reverse Cipher

The Caesar Cipher (e.g)

- The Caesar cipher is a substitution cipher, named after Julius Caesar.
- Operation principle: each letter is translated into the letter *a fixed number of positions* after it in the alphabet table.
- The fixed number of positions is a key both for encryption and decryption.

The Caesar Cipher

- Encryption of a letter by a shift n can be described mathematically as:
- Encryption Phase with shift k

$$E(m) = (m + k) \; mod \; 26$$

- Decryption Phase with shift k

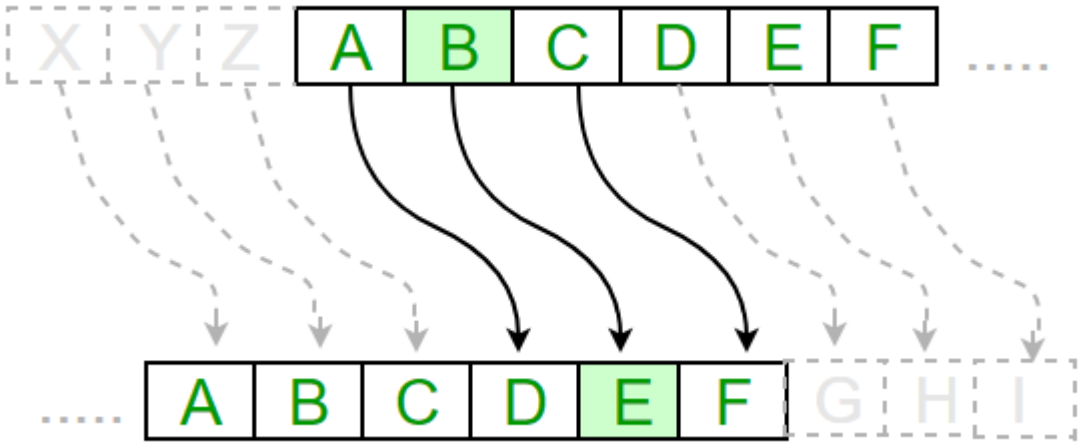
$$D(m) = (m - k) \; mod \; 26$$

- In Encryption / decryption equations used mod 26 or n where 26 is English alphabetic

The Caesar Cipher

- Each letter of a given text is replaced by a letter some fixed number of positions down the 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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



The Caesar cipher (cnt'd)

K=3

Outer: plaintext

Inner: ciphertext

Example

- If K=3 ,

$$E(m) = (m + k) \, mod \, 26$$

A full translation chart of the Caesar cipher is shown here.

Plaintext	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	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

Using this encryption, the message

TREATY IMPOSSIBLE

would be encoded as

T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

Example

- Ex: If k =5 and message(m) = hello … Encryption/ decryption Using Caser cipher;
- Sol: 1- Encryption Phase

$$E(m) = (m + k)\ mod\ 26$$

- Decryption Phase

$$D(m) = (m - k)\ mod\ 26$$

- Cont. …

Example

P=m	E(m)	E(m)	Result	C	D(m)	D(m)	Result	P=m
H	E(H)=H+k mod 26	E(H) = 7 +5 mod 26	12	M	D(M)=M-k mod 26	D(M)=12-5 mod 26	7	H
E	E(E) = E+ k mod 26	E(E)= 4+5 mod 26	9	J	D(J)=J-k mod 26	D(J)=9-5 mod 26	4	E
L	E (L) = L + k mod 26	E(L)=11+5 mod 26	16	Q	D(Q)= Q-k mod 26	D(Q)=16-5 mod 26	11	L
L	E (L) = L + k mod 26	E(L)=11+5 mod 26	16	Q	D(Q)= Q-k mod 26	D(Q)=16-5 mod 26	11	L
O	E(O) = O+k mod 26	E(O) = 14+5 mod 26	19	T	D(T)=T-k mod 26	D(T)=19-5 mod 26	14	O

Which p or m =plain text/message , c= cipher text, E(m) = Encryption for m, D(m) = Decryption for m

Example

Plaintext Letter	Plaintext Number	+	Key	Result	Subtract 26?	Result	Ciphertext Letter
H	7	+	13	= 20		= 20	20 = U
E	4	+	13	= 17		= 17	17 = R
L	11	+	13	= 24		= 24	24 = Y
L	11	+	13	= 24		= 24	24 = Y
O	14	+	13	= 27	- 26	= 1	1 = B
H	7	+	13	= 20		= 20	20 = U
O	14	+	13	= 27	- 26	= 1	1 = B
W	22	+	13	= 35	- 26	= 9	9 = J
A	0	+	13	= 13		= 13	13 = N
R	17	+	13	= 30	- 26	= 4	4 = E
E	4	+	13	= 17		= 17	17 = R
Y	24	+	13	= 37	- 26	= 11	11 = L
O	14	+	13	= 27	- 26	= 1	1 = B
U	20	+	13	= 33	- 26	= 7	7 = H

Breaking classic ciphers

- With the help of fast computers, 99.99% ciphers used before 1976 are breakable by using one of the 4 types of attacks (described later).
- Modern cluster computers and future quantum computers can break several existing ciphers due to the power of such computers.

Breaking the Caesar cipher

- By trial-and error
- By using statistics on letters
  - **frequency distributions** of letters

letter	percent
A	7.49%
B	1.29%
C	3.54%
D	3.62%
E	14.00%

.....

Principles of Private Key Encryption

- Devise cryptographic algorithms:
  - a set of fast functions (E1, E2, E3, ..En) that when in turn applied to an input (initial or intermediate input) will produce a more potentially scrambled output.
  - and a set of functions (D1,D2,D3, .. Dn) that when in turn applied to the cipher text (final or intermediate) will produce the original input text.

- Devise algorithms, tests and proofs to validate your cryptographic algorithms
  - Analysing algorithms.
  - Tests with powerful computers such as specialised, parallel, cluster, or quantum computers.
  - Mathematical proofs.

Toy example of public key cryptography

- Definition: **The multiplicative inverse** of *x* with modulo *n* is *y* such that (*x***y*) mod *n* = 1

  E.g:x=3; n=10, => y=7; since (3*7) mod 10 = 1

- The above multiplicative inverse can be used to create a simple public key cipher: either *x* or *y* can be thought of as a secret key and the other is the public key. Let *x* = 3, *y* = 7, *n* = 10, and M be the message:

  - M = 4 ;
    - 3*4 mod 10 = 2; (ciphertext) - encrypting
    - 2*7 mod 10 = 4 = M ; (message) – decrypting
  - M =6 ;
    - 3*6 mod 10 = 8;
    - 8*7 mod 10 = 6 = M (message)

What is PKE used for?

Private Key Encryption (PKE) can be used:

- Transmitting data over an insecure channel
- Secure stored data (encrypt & store)
- Provide integrity check:
  - (Key + Mes.) -> MAC (message authentication code)

Morden Cryptography applications

- Not just about confidentiality!
- Integrity
  - Digital signatures
  - Hash functions
- Fair exchange
  - Contract signing
- Anonymity
  - Electronic cash
  - Electronic voting
- Etc.

Modern private key ciphers

- DES (US, 1977) (3DES)
  - key -- 56 bits, plaintext/ciphertext -- 64 bits
- LOKI (ADFA, Australia, 1989)
  - key, plaintext/ciphertext -- 64 bits
- FEAL (NTT, Japan, 1990)
  - key -- 128 bits, plaintext/ciphertext -- 64 bits
- IDEA (Lai & Massey, Swiss, 1991)
  - key -- 128 bits, plaintext/ciphertext -- 64 bits
- SPEED (Y Zheng in 1996)
  - Key/(plaintext/ciphertext) -- 48,64,80,…,256 bits
- AES (Joan Daemen & Vincent Rijmen 2000)
  - Key/(plaintext/ciphertext) -- 128, 192 and 256 bits

General approaches to Cryptography

- There are two general encryption methods: Block ciphers & Stream ciphers

- Block ciphers
  - Slice message M into (fixed size blocks) m_1, …, m_n
    - Add padding to last block
  - Use E_k to produce (cipher text blocks) x_1, …, x_n
  - Use D_k to recover M from m_1, …, m_n

  - E.g: DES, etc.

- Stream ciphers
  - Generate a long random string (or pseudo random) called *one-time pad*.

  - Message $\oplus$ *one-time pad* (exclusive or)
    - E.g: EC4

4 types of cryptanalysis

- Depending on what a cryptanalyst has to work with, attacks can be classified into
  - ciphertext only attack
  - known plaintext attack
  - chosen plaintext attack
  - chosen ciphertext attack (most severe)

4 types of attacks

- Ciphertext only attack
  - the only data available is a target ciphertext
- Known plaintext attack
  - a target ciphertext
  - pairs of other ciphertext and plaintext (say, previously broken or guessing)

4 types of attacks

- Chosen plaintext attacks
  - a target ciphertext
  - can feed encryption algorithm with plaintexts and obtain the matching ciphertexts
- Chosen ciphertext attack
  - a target ciphertext
  - can feed decryption algorithm with ciphertexts and obtain the matching plaintexts

Thank You