

Introduction to Cryptography

Lecture 1: Functions and Principles of Cryptography

CYB 650

Cybersecurity Fundamentals

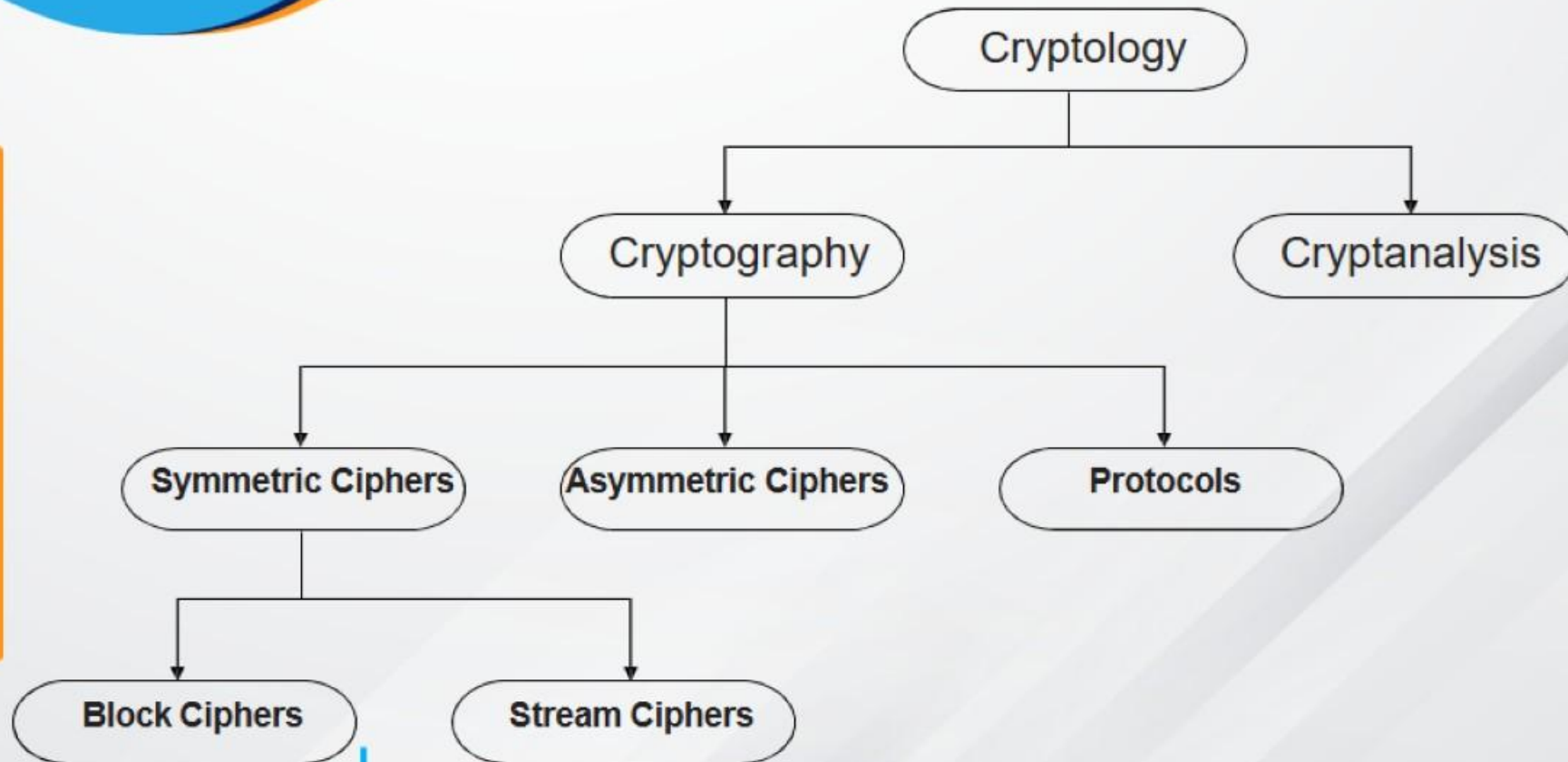
Presented by

Dr. Mohammad Alkhatib

Module 1

Functions and Principles of Cryptography

- Overview on the field of cryptology
- Principles and Functions
- Basics of symmetric cryptography
- Classical Cryptography



❑ **Cryptography**- the science of secret writing with the goal of hiding the meaning of a message.

❑ **Cryptanalysis**- the science and sometimes art of breaking cryptosystems

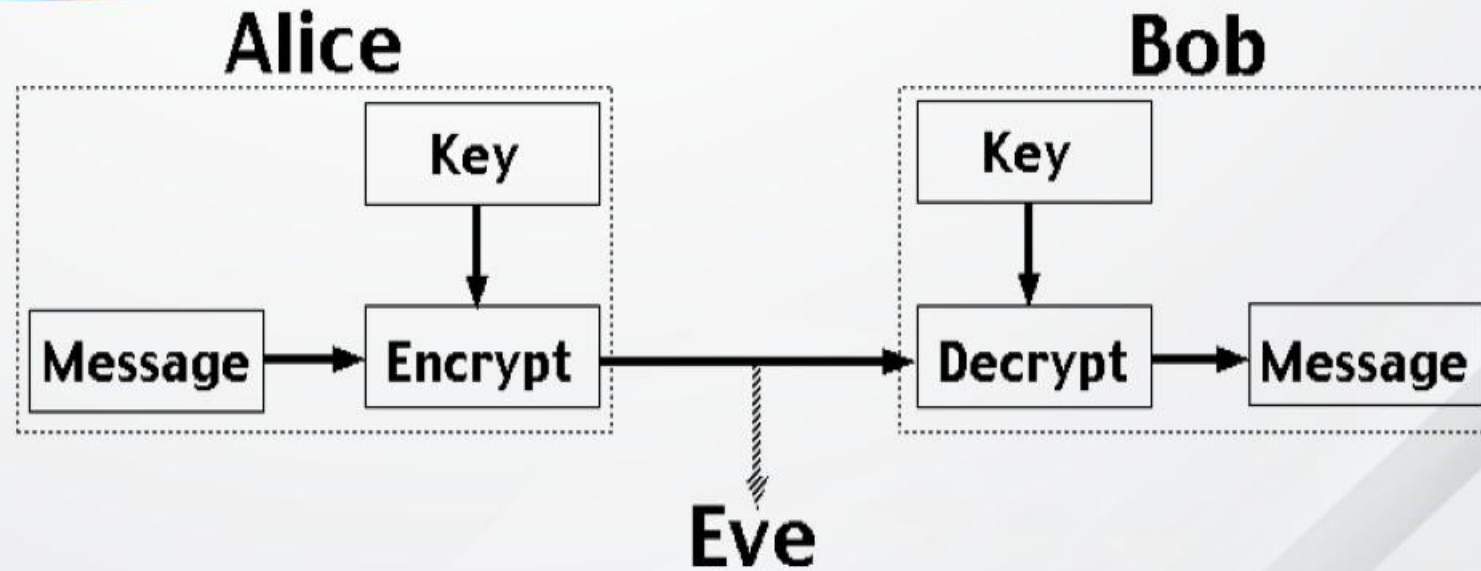
❑ **plaintext** - the original text or message to be hidden (encrypted)

❑ **ciphertext** - the coded (encrypted) message

- ❑ **key** - information used in cryptographic algorithm known only to sender/receiver
- ❑ **Encryption**- converting plaintext to ciphertext
- ❑ **Decryption**- recovering plaintext from ciphertext

- ❑ In a **transposition cipher**, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged.
- ❑ By contrast, in a **substitution cipher**, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

❑ A **monoalphabetic cipher** uses fixed substitution over the entire message, whereas a **polyalphabetic cipher** uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa



- **Cryptography** is the science that enables Alice and Bob to communicate securely in the presence of Eve.

- Confidentiality
 - Keeping information secret from non authorized entities
- Data Integrity
 - Ensure the information not being altered
- Authentication
 - Identification between parties
- Non-repudiation
 - Prevent an entity from denying previous actions

classified along three independent dimensions

The type of operations used for transforming plaintext to ciphertext

- **Substitution** – each element in the plaintext is mapped into another element
- **Transposition** – elements in plaintext are rearranged

The number of keys used

- Sender and receiver use same key – **symmetric**
- Sender and receiver each use a different key - **asymmetric**

The way in which the plaintext is processed

- **Block cipher** – processes input one block of elements at a time
- **Stream cipher** – processes the input elements continuously

Cryptosystem is computationally **secure if:**

- Cost of breaking cipher exceeds value of information
- Time required to break cipher exceeds the useful lifetime of the information
- If the best known attack is to try all possible keys

- Cryptosystem is **insecure** if any shortcut attack is known
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack

- Trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ μ s	Time required at 10^6 decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu$ s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu$ s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu$ s = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu$ s = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu$ s = 6.4×10^{12} years	6.4×10^6 years

- Information security is a big topic
 - Crypto, Access control, Protocols, Software
 - Real world info security problems abound
- Cryptography is the part of information security that works best
- Using crypto correctly is important
- The more we make other parts of security behave like crypto, the better

- ❑ **Symmetric Algorithms**- two parties have an encryption and decryption method for which they share a secret key.
- ❑ All cryptography from ancient times until 1976 was exclusively based on symmetric methods.

- ❑ Symmetric ciphers are still in widespread use, especially for data encryption and integrity check of messages (Confidentiality and Integrity).
- ❑ Symmetric Algorithms are called single key algorithms since they use one key for both encryption and decryption operations

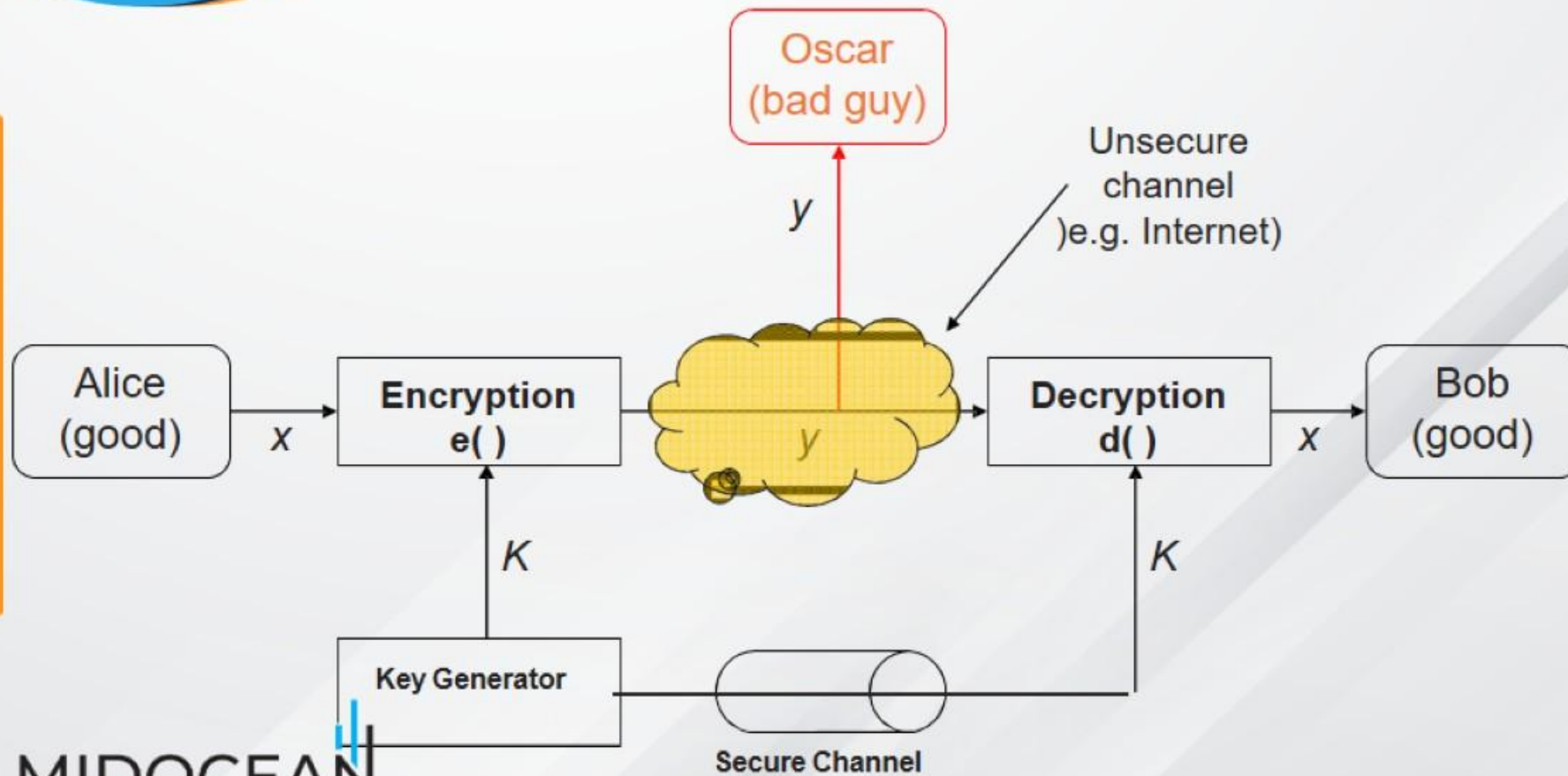
- ❑ **Asymmetric (also called Public-Key) Algorithms**- a user possesses a secret key (*for decryption*) as in symmetric cryptography but also a public key (for encryption).
- ❑ Asymmetric algorithms can be used for applications such as *digital signatures* and *key establishment*, and also for classical data encryption.

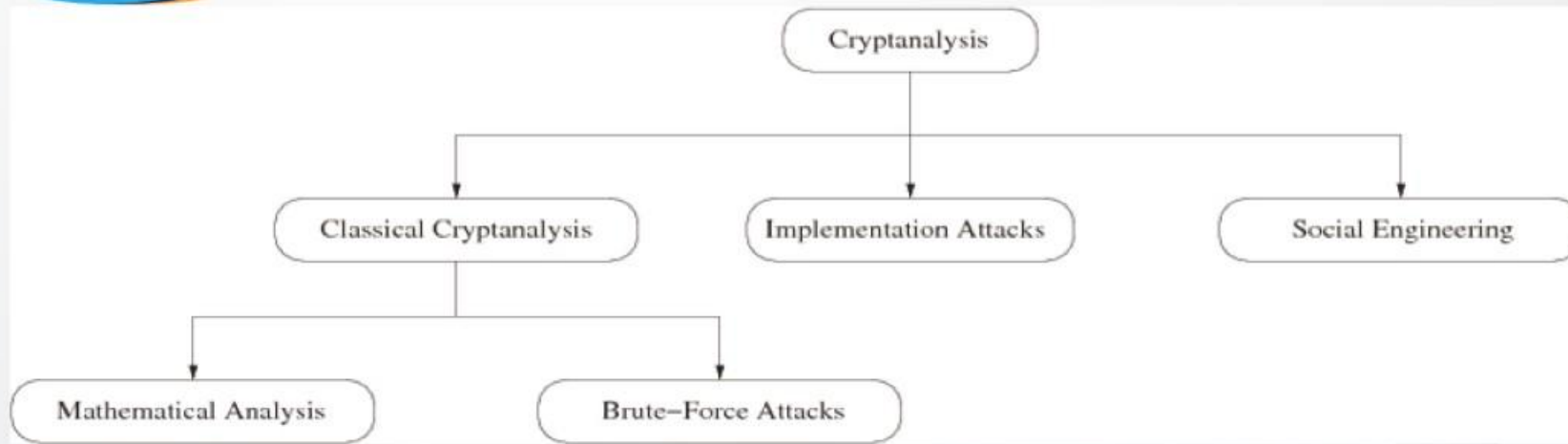
- ❑ Asymmetric algorithms were introduced In 1976 an entirely different type of cipher was introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle.
- ❑ Examples: RSA, ElGamal, ECC

- ❑ In the majority of cryptographic applications in practical systems, symmetric and asymmetric algorithms are all used together.
- ❑ This is referred to as hybrid schemes. The reason for using both families of algorithms is that each has specific strengths and weaknesses
- ❑ In particular, Public-key algorithms are used for key distribution process, while symmetric algorithms are used for usual message encryption and decryption processes

Module 01

Basics of Symmetric Cryptography





- ☐ **Classical Cryptanalysis**
- ☐ **Implementation Attacks**
- ☐ **Social Engineering Attacks**

- Definition
 - $a \bmod n = r$ q.s.t $a = qn + r$
where $0 \leq r \leq n-1$;
 - The integer modulo m , denoted by Z_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ where addition, subtraction and multiplication is performed modulo m .
 - Example
 - $7 \bmod 3 = 1$
 - $-7 \bmod 3 = 2$
 - In Z_{25} ,
 - $13 + 16 = 4$, since $13+16=29 \equiv 4 \pmod{25}$
 - $13 \cdot 16 = 8$, since $13 \cdot 16=208 \equiv 8 \pmod{25}$

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

- Replacing each letter of the alphabet with the letter standing p places further down the alphabet

$$C = E(k, p) = (p + k) \bmod 26$$

$$p = D(k, C) = (C - k) \bmod 26$$

- Brute-force cryptanalysis is easy (only 25 keys)

Example 1. Let the key be $k = 17$, and the plaintext is:

ATTACK = $x_1, x_2, \dots, x_6 = 0, 19, 19, 0, 2, 10$.

The ciphertext is then computed as:

$ek(0) \equiv 0 + 17 \pmod{26} = 17 \rightarrow \mathbf{A}$ becomes **r**

$ek(19) \equiv 19 + 17 \pmod{26} = 10 \rightarrow \mathbf{T}$ becomes **k**

$y_1, y_2, \dots, y_6 = 17, 10, 10, 17, 19, 1 =$ The ciphertext is **rkkrtb**

Example 1. continue, the ciphertext is:

rkkrtb = $y_1, y_2, \dots, y_6 = 17, 10, 10, 17, 19, 1$

The plaintext is then obtained as:

$dk(17) \equiv 17 - 17 \pmod{26} = 0 \rightarrow r$ becomes **A**

$dk(10) \equiv 10 - 17 \pmod{26} = 19 \rightarrow k$ becomes **T**

The plaintext is: ATTACK

Bob needs to send the following message to Alice over a communication channel.

Plaintext: "hide the gold in the safe"

❑ Encrypt and then decrypt the message using the playfair cipher using the key "system"

❑ *Step 1:* Break the message into digrams (groups of 2 letters). If needed, append an uncommon monogram to complete the final digram.

❑ Hi de th eg ol di nt he sa fe

❑ Note: If both letters are the same add a "z" after the first letter

Step 2: Construct the playfair table, as following:

- ❑ First, fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters).
- ❑ Fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "J" or "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space).
- ❑ The key can be written in the top rows of the table, from left to right.
- ❑ The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key

S	y	t	e	m
a	b	c	d	F
g	h	i/j	k	L
N	o	p	q	R
u	v	w	x	Z

Step 3: Start encrypting the plaintext pairs (every two letters), via applying the following rules:

- ❑ If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
- ❑ If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
- ❑ If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

- ❑ hi → ik
- ❑ de → kd
- ❑ th → yi

S	y	t	e	m
a	b	c	d	F
g	h	i/j	k	L
N	o	p	q	R
u	v	w	x	Z

Module 01

Playfair Cipher

□eg → sk

□ol → rh

□di → ck

□nt → ps

□he → ky

□sa → ag

□fe → dm

s	y	t	e	m
a	b	c	d	f
g	h	i/j	k	l
n	o	p	q	r
u	v	w	x	z

□Therefore, the encrypted text:

□ik kd yi sk rh ck ps ky ag dm

Module 01

Playfair Cipher

❑ To decrypt the ciphertext, reverse the previous steps, as follows:

❑ ik → hi

❑ kd → de

❑ yi → th

❑ sk → eg

❑ rh → ol

❑ ck → di

❑ ps → nt

❑ ky → he

❑ ag → sa

❑ dm → fe

s	y	t	e	m
a	b	c	d	f
g	h	i/j	k	l
n	o	p	q	r
u	v	w	x	z

❑ The plaintext: **hide the gold in the safe**



Thank You