

Lecture (02)

Classical Encryption Techniques (I)

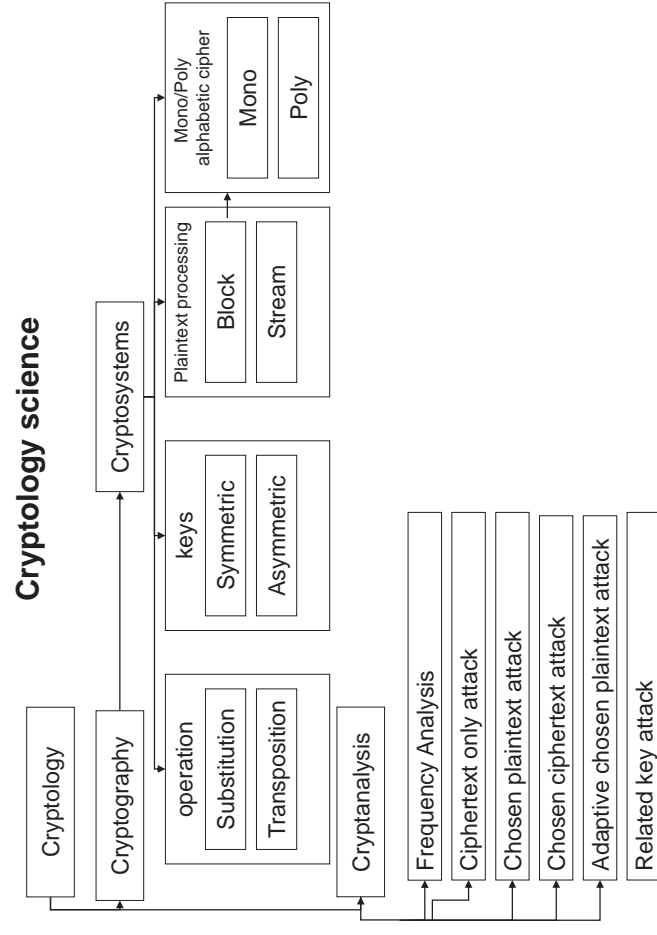
Dr. Ahmed M. ElShafee

Agenda

- Preface
- Cryptography
- Cryptanalysis
- Classical Ciphers

Preface

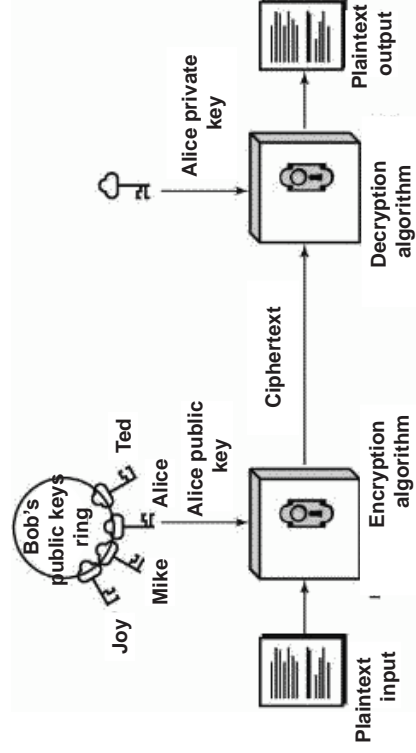
- **cryptology** - field of both cryptography and cryptanalysis
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key



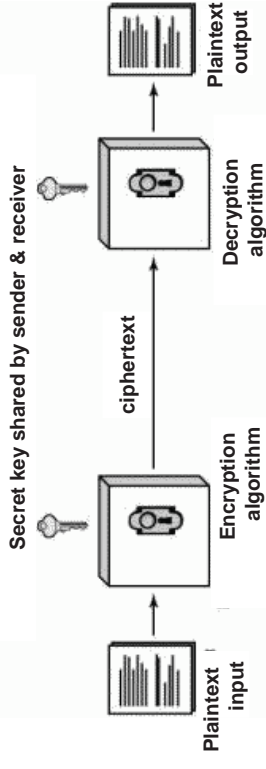
Cryptography

- Cryptographic systems can be characterized along these three independent dimensions.
 - type of encryption operations used
 - Substitution, permutation, or product (later)
 - number of keys used
 - single-key or private (symmetric)
 - two-key or public (Asymmetric)
 - way in which plaintext is processed
 - block / stream (later)

Public key cryptosystem



Private key cryptosystem



Symmetric (private) key

- Symmetric encryption, also referred to as conventional encryption or single key encryption, was the only type of encryption in use prior to the development of public-key encryption in the 1970s.
- It remains by far the most widely used of the two types of encryption.
- *All traditional schemes are **symmetric / single key / private-key encryption algorithms, with a single key, used for both encryption and decryption.***
- *Since both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.*

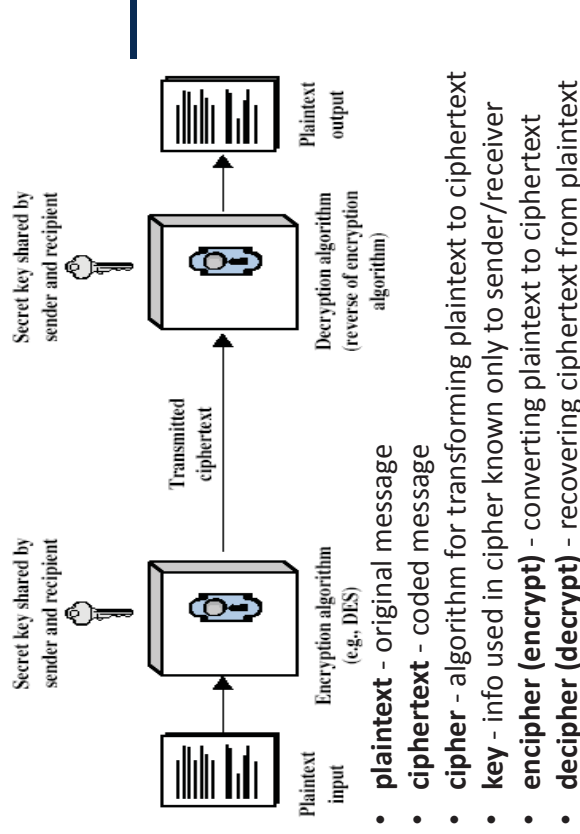
- two requirements for secure use of symmetric encryption:
 - a strong encryption algorithm
 - a secret key known only to sender / receiver
- We assume that it is impractical to decrypt a message on the basis of the cipher- text plus knowledge of the encryption/decryption algorithm, and do not need to keep the algorithm secret; rather we only need to keep the key secret.
- This feature of symmetric encryption is what makes it feasible for widespread use.
- It allows easy distribution of s/w and h/w implementations.

- mathematically have:

$$Y = E_K(X)$$

$$X = D_K(Y)$$

- assume encryption algorithm is known
- implies a secure channel to distribute key



Cryptanalysis

- objective is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.
- general approaches:
 - cryptanalytic attack
 - rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.

– brute-force attack

- try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success

17

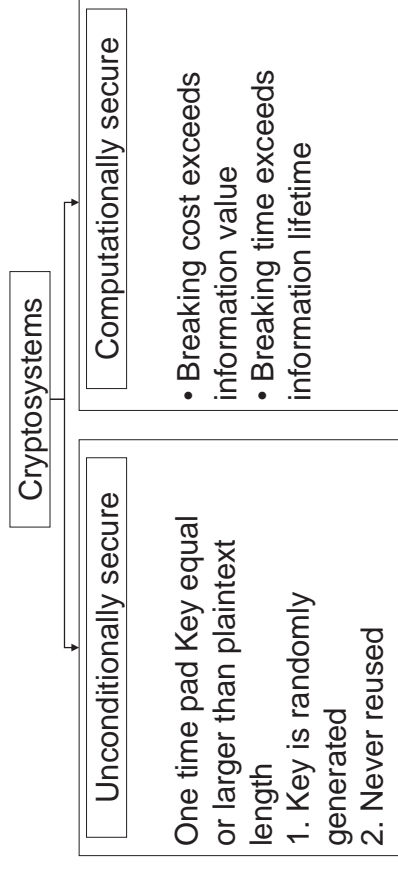
Cryptanalytic Attacks

- ciphertext only
only know algorithm & ciphertext, is statistical, know or can identify plaintext
- known plaintext
know/suspect plaintext & ciphertext
- chosen plaintext
select plaintext and obtain ciphertext
- chosen ciphertext
select ciphertext and obtain plaintext
- chosen text
select plaintext or ciphertext to en/decrypt

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

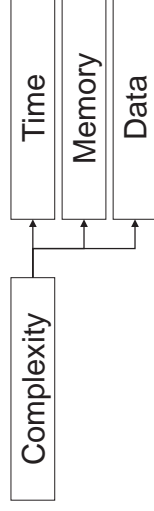
Shannon's theory

According to cryptanalytic attacks, we can classify cryptosystems into two types



18

Complexity & weakness



“Breaking cipher, means to find weakness can be exploited with complexity less than brute force attack”, Bruce a schneier

Brute Force attack (Excusive key search)

- A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ μ s	Time required at 10^6 decryptions/ μ s
32			
56			
128			
168			

Classical Ciphers

- The two basic building blocks of all encryption technique are substitution and transposition.

Substitution

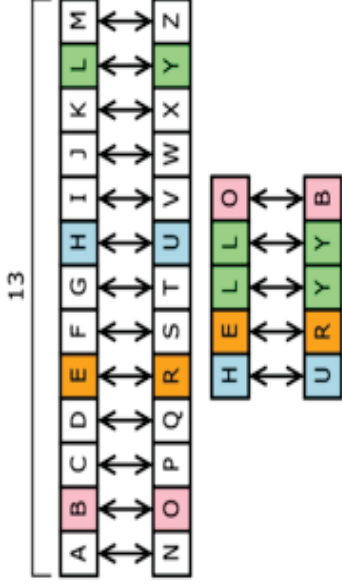
- where letters of plaintext are replaced by other letters or by numbers or symbols
- if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Brute Force attack (Excusive key search)

- A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

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	7.6×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu$ s = 5.9×10^{36} years	8.4×10^{30} years

Substitution ciphers



11

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

11

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first use in military affairs
- Example: replaces each letter by 3rd letter on

- Substitution box

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
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

- Mathematically

$$c = E(p) = (p + k) \bmod (26)$$

$$p = D(c) = (c - k) \bmod (26)$$

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	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
					0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5					

11

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

11

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

- This mathematical description uses **modulo (clock)** arithmetic.

- Here, when you reach Z you go back to A and start again.
- Mod 26 implies that when you reach 26, you use 0 instead (ie the letter after Z, or $25 + 1$ goes to A or 0).

Examples

- Encrypt the following message
“meet you at nine PM”,
- using the key
“k”

Y*

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

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
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

m	e	e	t	y	o	u	a	t	n	i	n	e	P	M
12	4	4	19	24	14	20	0	19	13	8	13	4	15	12

key

k
10

ciphertext

22	14	14	3	8	24	4	10	3	23	18	23	14	25	22
w	o	o	d	i	y	e	k	d	x	s	x	o	z	w

Y*

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

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
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

m	e	e	t	y	o	u	a	t	n	i	n	e	P	M
12	4	4	19	24	14	20	0	19	13	8	13	4	15	12

key

k
10

ciphertext

Y*

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

Example

- Decrypt the following message
“nhfsstyrjjydtzfysnsjqjyxrfrfpjnyjs”
- using the key
“F”

Y*

Dr. Ahmed ElShafee, ACU Spring 2014, Information Security

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
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

G	C	U	A	V	Q	D	T	G	C	M
6	2	20	0	21	16	3	19	6	2	12

Key

plaintext

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
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

G	C	U	A	V	Q	D	T	G	C	M
6	2	20	0	21	16	3	19	6	2	12

Key

c
2

plaintext

4	0	18	24	19	14	1	17	4	0	10
e	a	s	y	t	o	b	r	e	a	k

Thanks,..
See you next week (ISA),...