IA 124:

INTRODUCTION TO IT SECURITY

LECTURE 03

PRACTICAL CRYPTOGRAPHY (a)

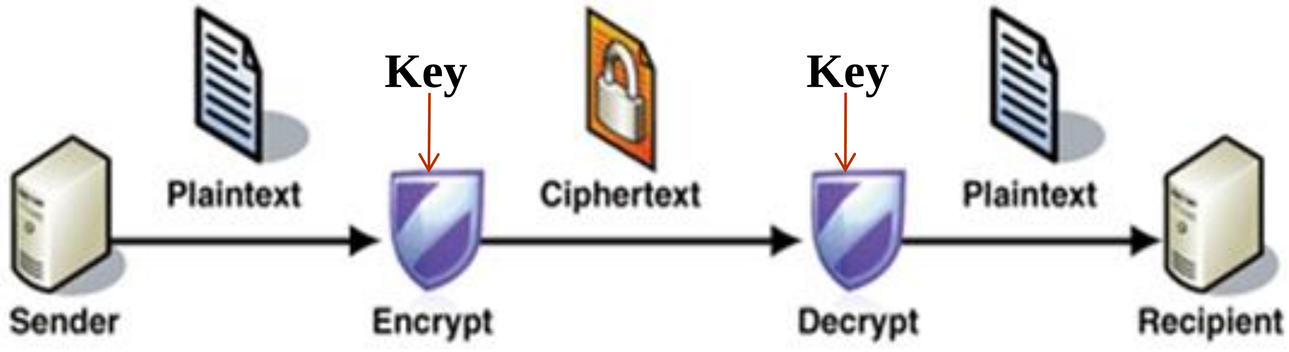
CRYPTOGRAPHY CONCEPTS

Cryptography

- Cryptography is the **conversion of data** into a scrambled code and send across a private or public network.
  - ✓ Original meaning: The art of secret writing.
  - ✓ Becoming a science that relies on mathematics (number theory, algebra)
    - ➢ The science of **encrypting**.
    - ➢ The science and art of designing **ciphers**.
    - ➢ **Cipher** are algorithms used to encrypt or decrypt the data.
- The purpose of cryptography is to **protect** data transmitted in the likely presence of an opponent.
  - ✓ **Protect** e-mail messages, credit card information, and corporate data.
- **Objectives of cryptography**

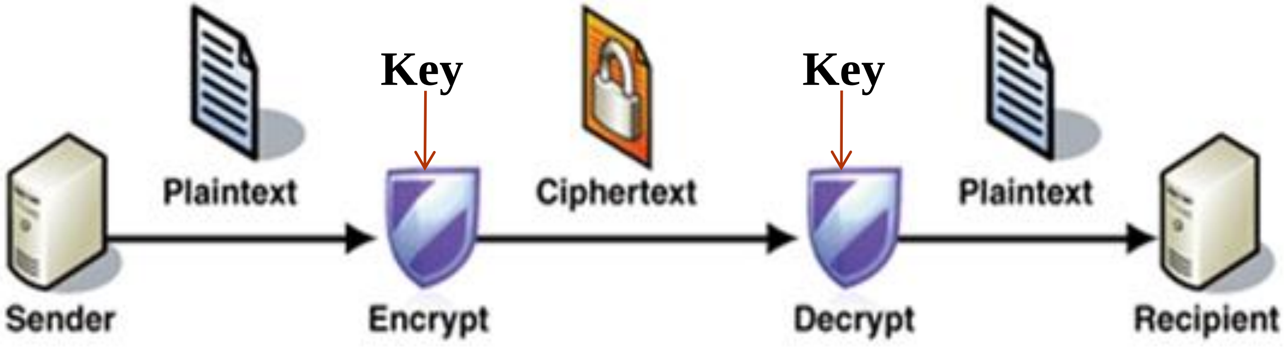
1. **Confidentiality**
2. **Integrity**
3. **Authentication**
4. **Non-repudiation**

Terminologies



- **Plaintext:** A message in its original form.
  - ✓ A **message** in cryptography can be any kind of data, such as images, audio, video, text, databases, files, or data streams.
- **Ciphertext:** A message in the transformed, unrecognized form. A scrambled message. It depends on the plaintext and the secret key.
  - ✓ Designed to protect the information from an unauthorized access.
- **Encryption:** The process that transforms a plaintext under the control of the **key** into a ciphertext; also known as **encode** and **encipher.**
- **Decryption:** The process that transforms an encrypted message (ciphertext) to the corresponding plaintext; also known as **decode** and **decipher.**

Terminologies



- **Key:** The value used to control encryption/decryption
- **Cipher** are algorithms used to encrypt or decrypt the data.
- **Cryptosystem:** A system for encryption and decryption
- **Cryptanalysis (technically):** Is a study of ciphers, ciphertext or cryptosystems and to find weakness in the encryption key so that message can be decrypted without knowing the key.
    - ✓ The science of **decrypting** messages or breaking codes and ciphers.
- **Cryptanalysis (In non-technical terms):** It is an unauthorized method of recovering the original message or breaking the message. It is a combination of science, art and luck used to break messages or the entire systems.
- **Cryptology:** is a study of both cryptography and cryptanalysis.

CONVENTIONAL ENCRYPTION PRINCIPLES

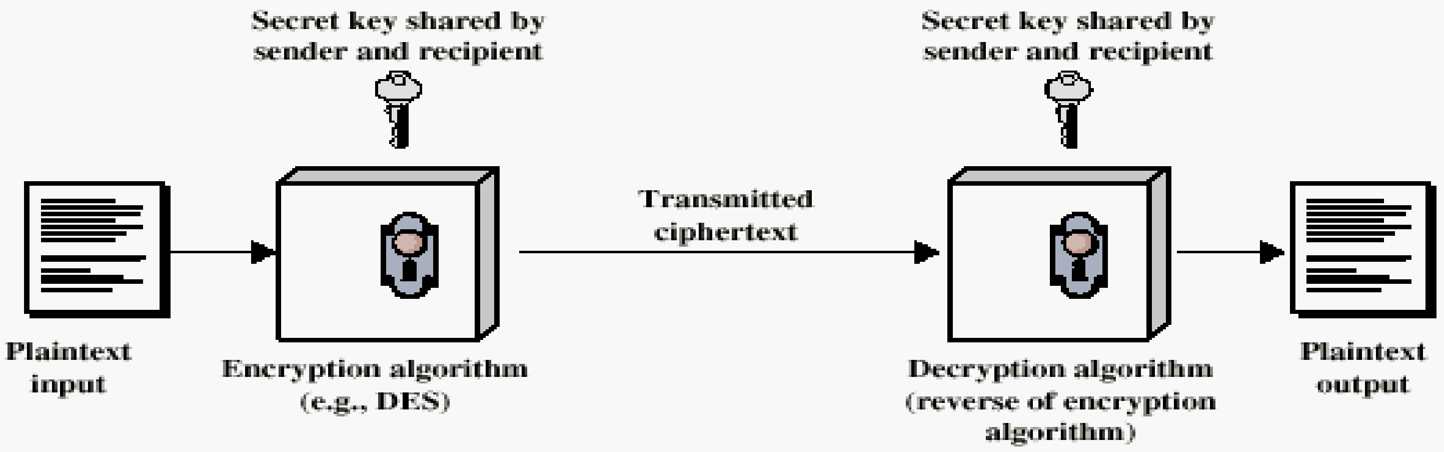

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Conventional Encryption

- An encryption scheme has five ingredients:

  1. **Plaintext**
  2. **Encryption algorithm**
  3. **Secret Key**
  4. **Ciphertext**
  5. **Decryption algorithm**

- **Note:** Security depends on the secrecy of the key, not the secrecy of the algorithm

CONVENTIONAL ENCRYPTION PRINCIPLES

- An encryption scheme has **five ingredients**:

1. **Plaintext:** This is the original intelligible message or data. Input to encryption algorithm.
2. **Encryption algorithm:** Performs various substitutions and transformations on the plaintext. It takes the plaintext and the secret key and produces the ciphertext.
3. **Private or Secret key:** Piece of secret data used to control encryption and decryption process.
4. **Ciphertext:** This is the scrambled/transformend message; An encrypted message. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

CRYPTOGRAPHY

Cryptographic systems are **characterized** along three independent dimensions

1. The type of **operations** used for transforming plaintext to ciphertext.
   - **(a)** Substitution cipher **(b)** Transposition cipher
2. The number of **keys** used.
   - **(a)** Symmetric encryption **(b)** Asymmetric encryption
3. The way in which the plaintext is **processed**.
   - **(a)** Block cipher **(b)** Stream cipher

Cryptographic Systems Classification

(1) The type of **operations** used for transforming plaintext to ciphertext

- **Substitution cipher:**

  In this technique the letters/numbers/ symbols of plaintext are replaced by other letters/numbers/symbols to form a ciphertext.

  ✓ Example: a→G, d→S

- It replaces bits, characters, or blocks of characters with different bits, characters or blocks. e.g. **Caesar cipher**, **hill cipher.**

Plaintext	Ciphertext
a	G
b	X
c	N
d	S
e	D
…	…
z	Q

SUBSTITUTION TECHNIQUES

- A **monoalphabetic substitution cipher** maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.
  - Example: Caesar cipher

plain:	**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**
CIPHER:	**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**

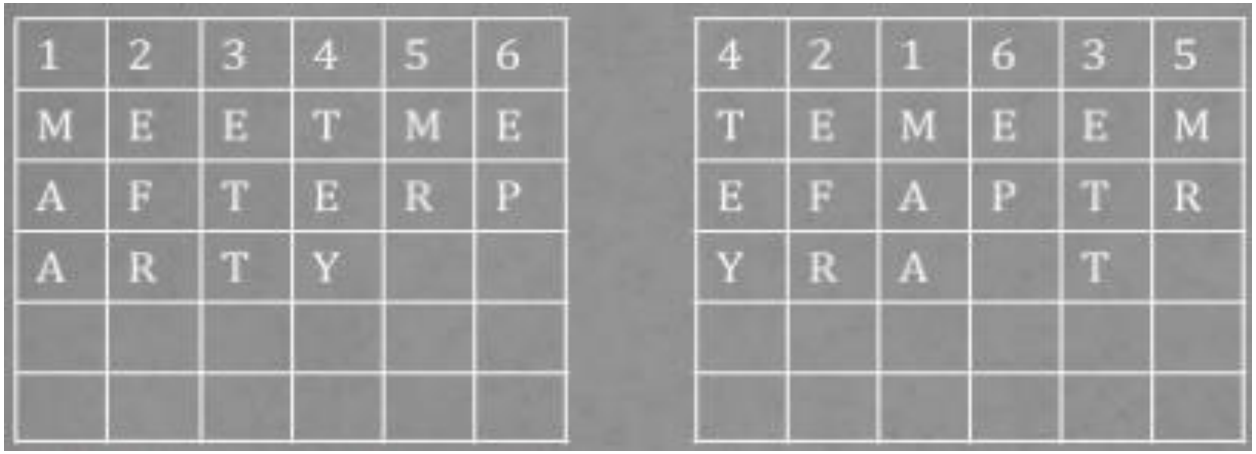
- **Polyalphabetic Ciphers**
  - In order to make substitution ciphers more secure, more than one alphabet can be used.
  - Such ciphers are called polyalphabetic, which means that the same letter of a message can be represented by different letters when encoded.
  - Example: Vigenère Cipher

Cryptographic Systems Classification

(1) The type of **operations** used for transforming plaintext to ciphertext

- **Transposition cipher:**

In this technique the position of letters/numbers/symbols in plaintext is changed with one another.



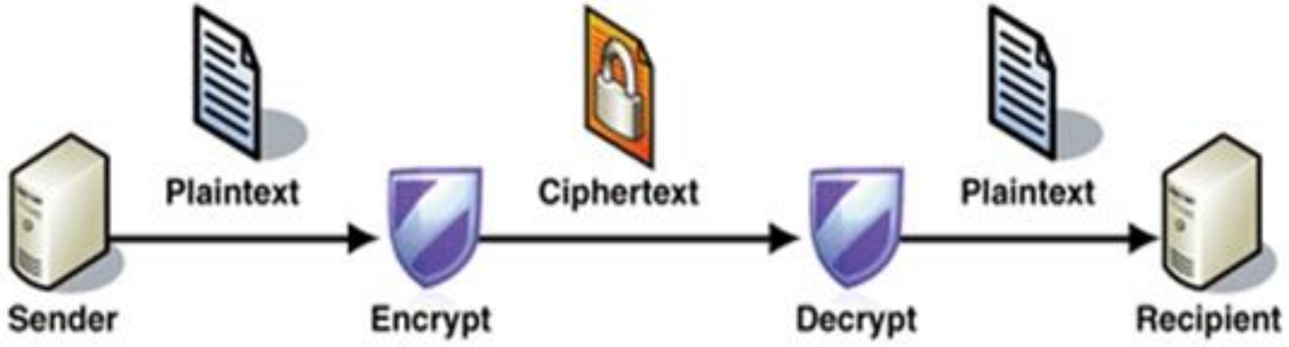
1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Plaintext: Meet me after party
Ciphertext: TEMEEMEFAPTRYRAT
Key: 421635

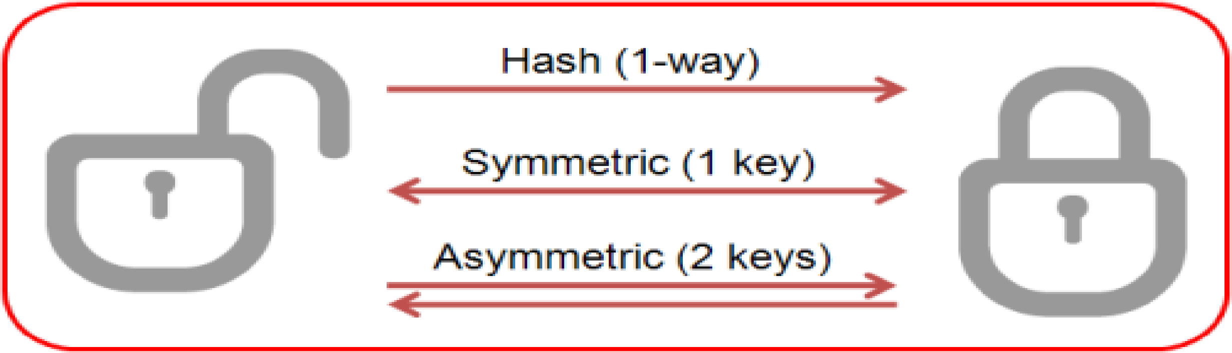
Cryptographic Systems Classification

(2) The number of **keys** used



❖ General there are **two** types of encryption :

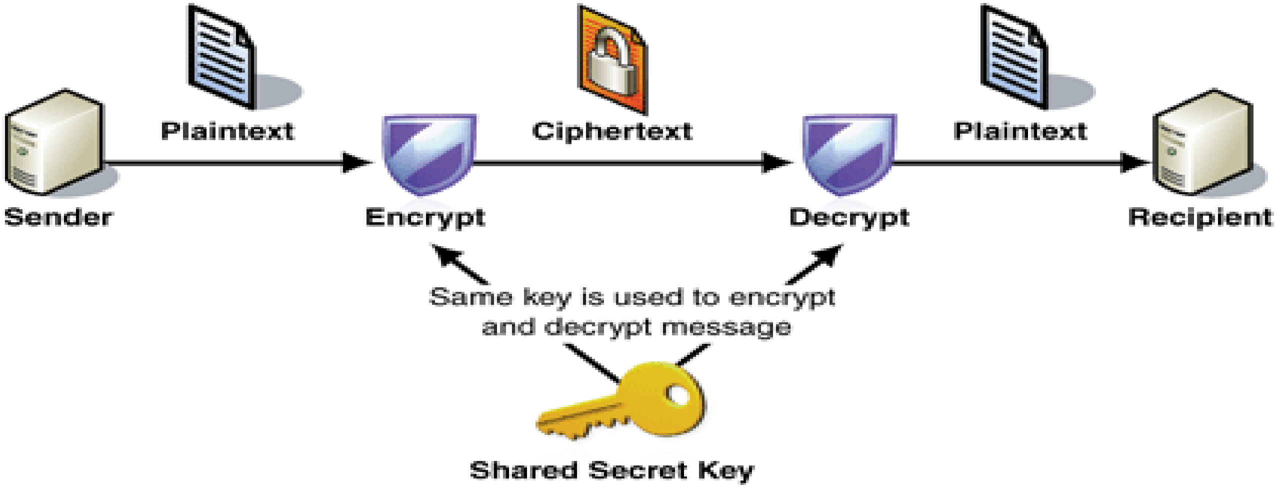
1. **Symmetric encryption (uses one secret key)**
2. **Asymmetric encryption (uses a private key and a public key)**
3. **Hash function (One-way encryption)**



Cryptographic Systems Classification

Symmetric encryption (uses one secret key)

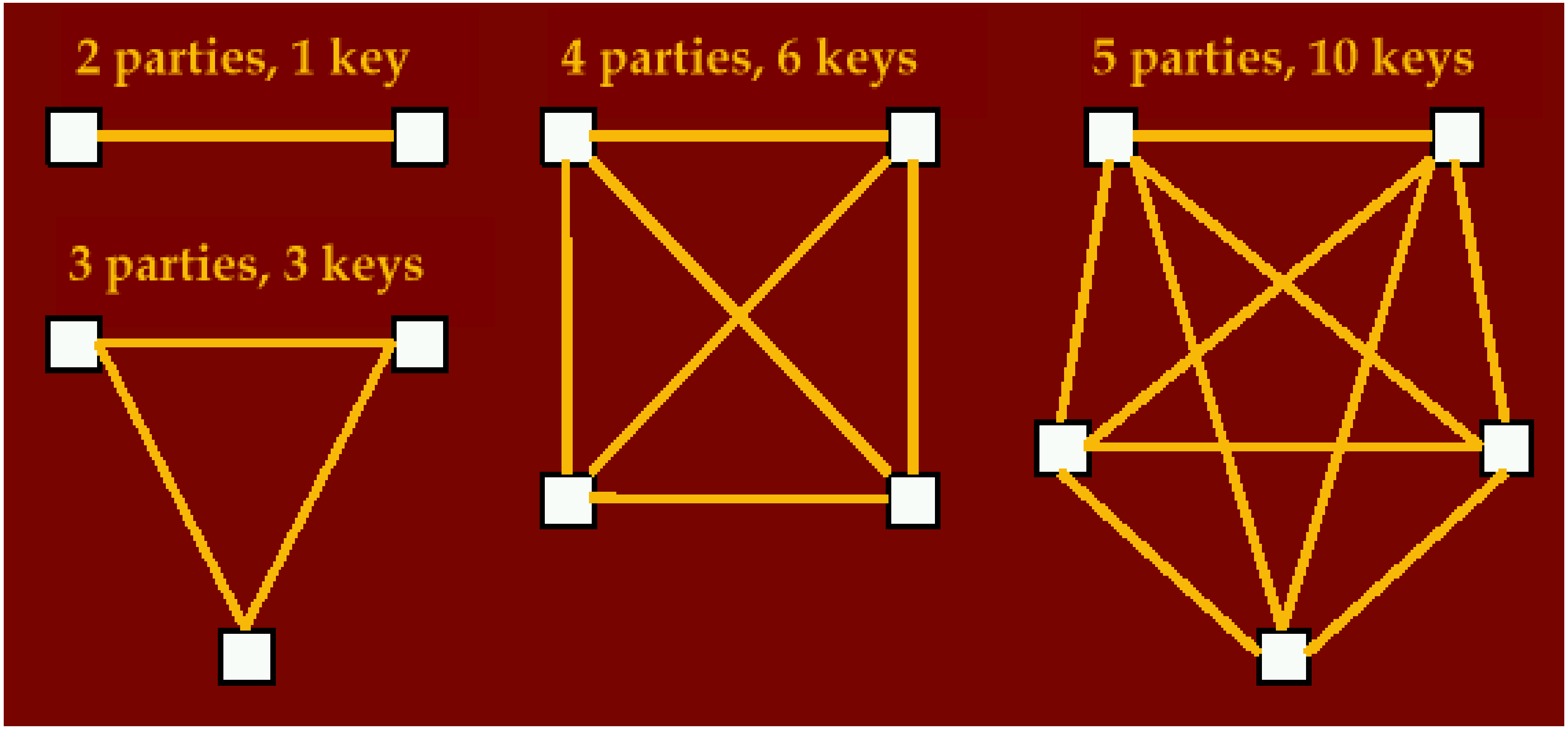
- **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the same key (**private/secret/single/shared key)**.
- If the key is disclosed communications are compromised
- Both parties are equal; Hence does not protect sender from receiver forging a message & claiming is sent by sender
- It is also known as conventional encryption



Symmetric Encryption

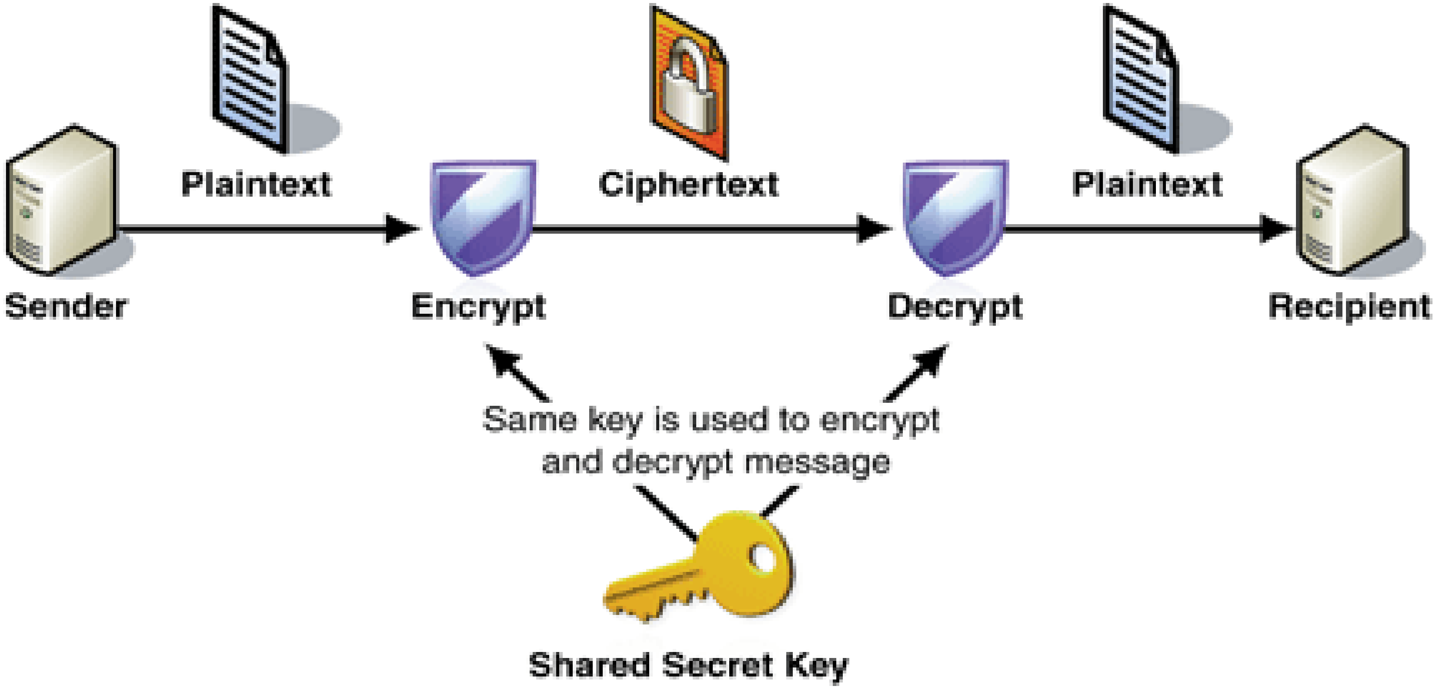
- **Symmetric Key – Issues**
  - ✓ Key management, keys required = (p*(p-1))/2

Note: P=number of parties in communications network



Symmetric Encryption

- Insufficiencies with **Symmetric Encryption**
  - ✓ **Key distribution:** how to have secure communications in general without having to trust a Key Distribution Centre (KDC) with your key.
  - ✓ **Digital signatures:** how to verify a message comes intact from the claimed sender

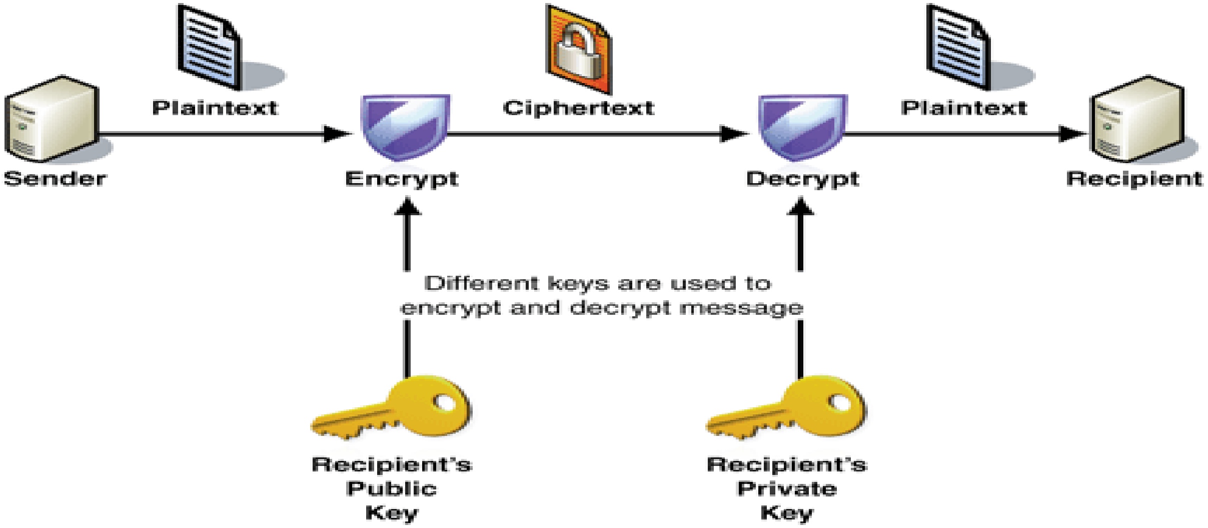


Cryptographic Systems Classification

❖ Asymmetric encryption

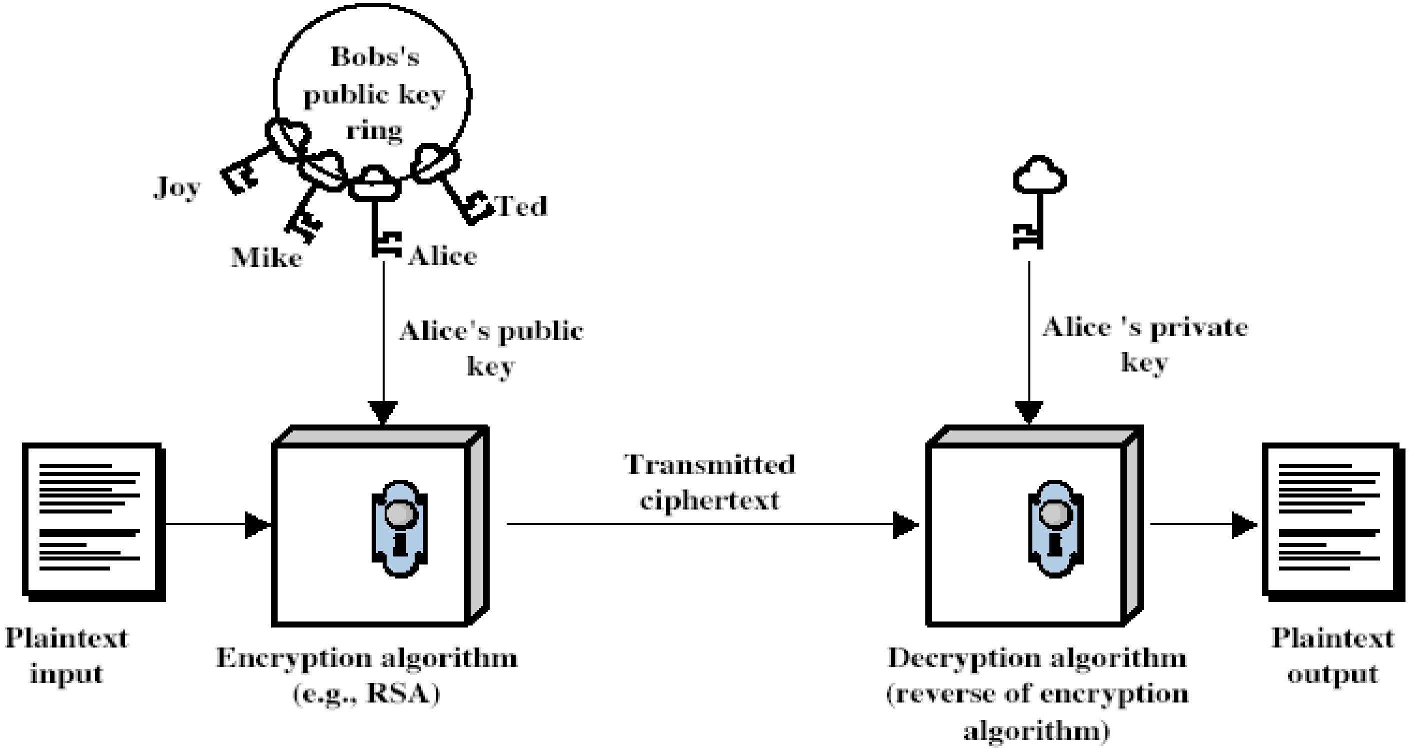
- ✓ Asymmetric encryption (public-key) uses deferent encryption keys for encryption and decryption. These keys are known as public and private keys.
- ✓ **Public-key/two-key/asymmetric** cryptography involves the use of **two** keys:

1. **Public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures.**
2. **Private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures.**

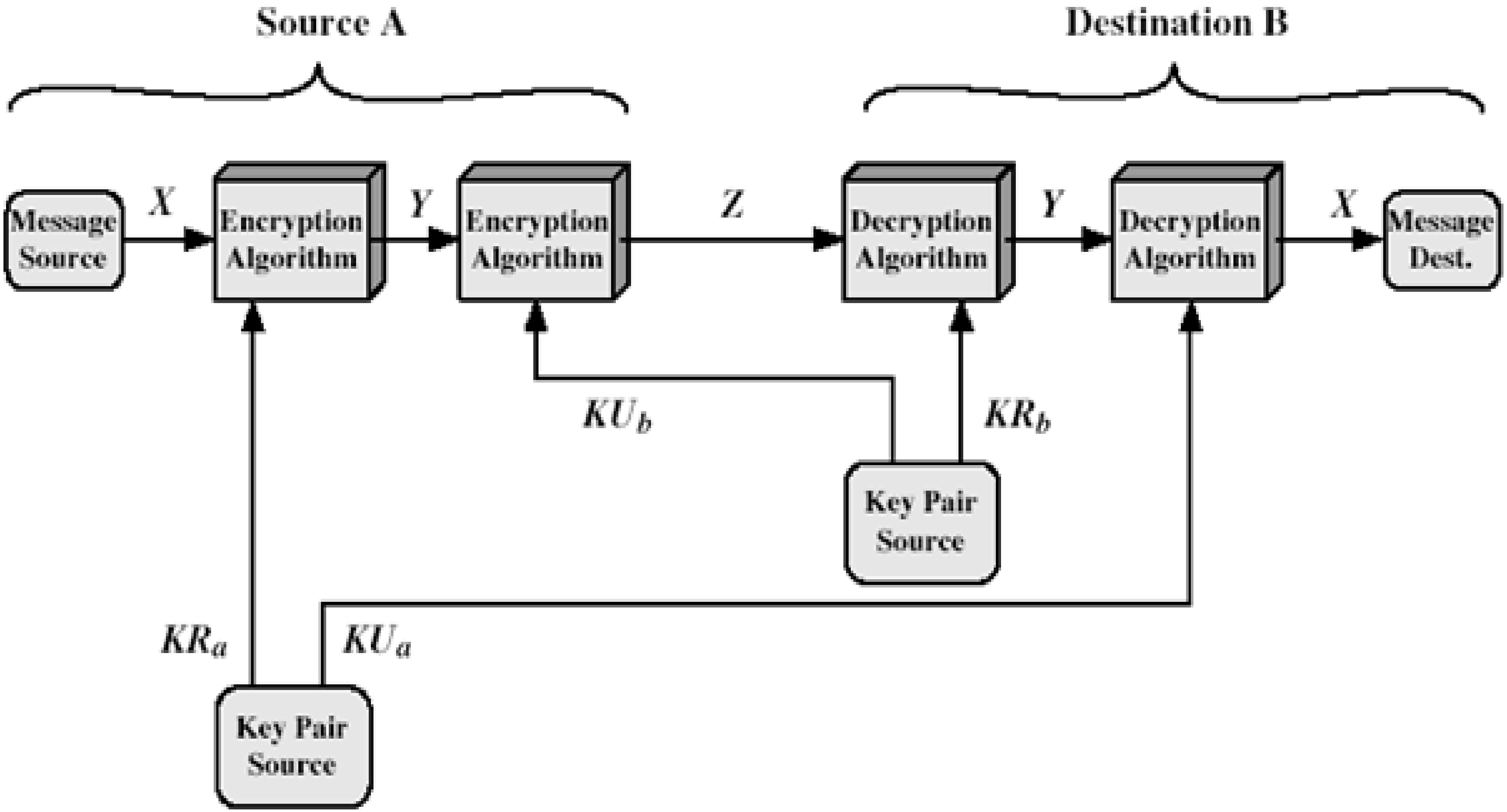


Asymmetric Encryption

- Is **asymmetric** encryption because
  - ✓The key used to encrypt messages or verify signatures **cannot** decrypt messages or create signatures
- Complements **rather than** replaces private key cryptography



Asymmetric Cryptosystems

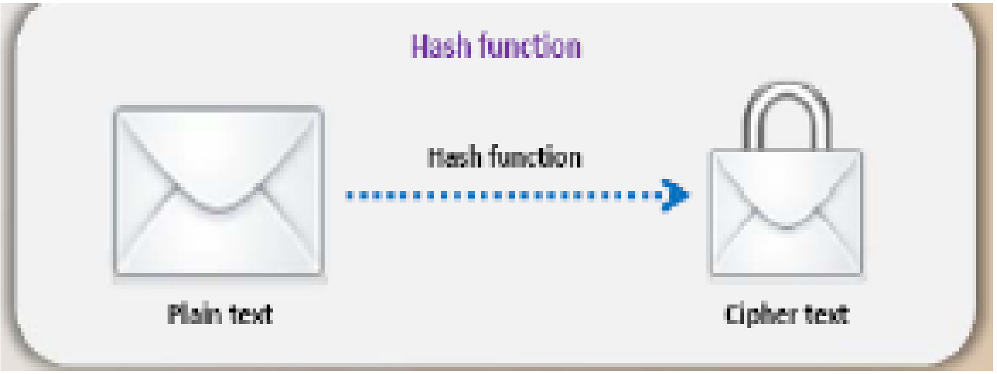


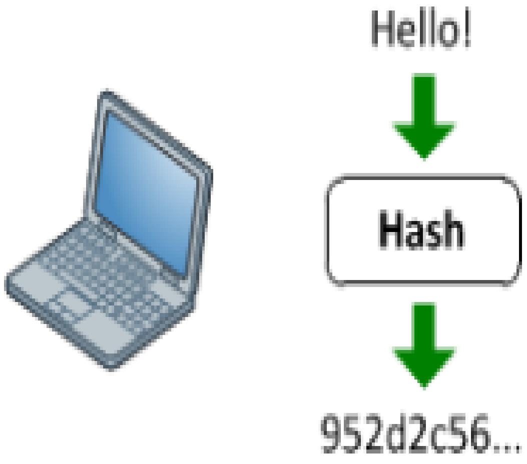
- KR-Private Key : Create Signatures, Decrypt Messages
- KU-Public Key: Encrypt Messages, Verify Signature

Cryptographic Systems Classification

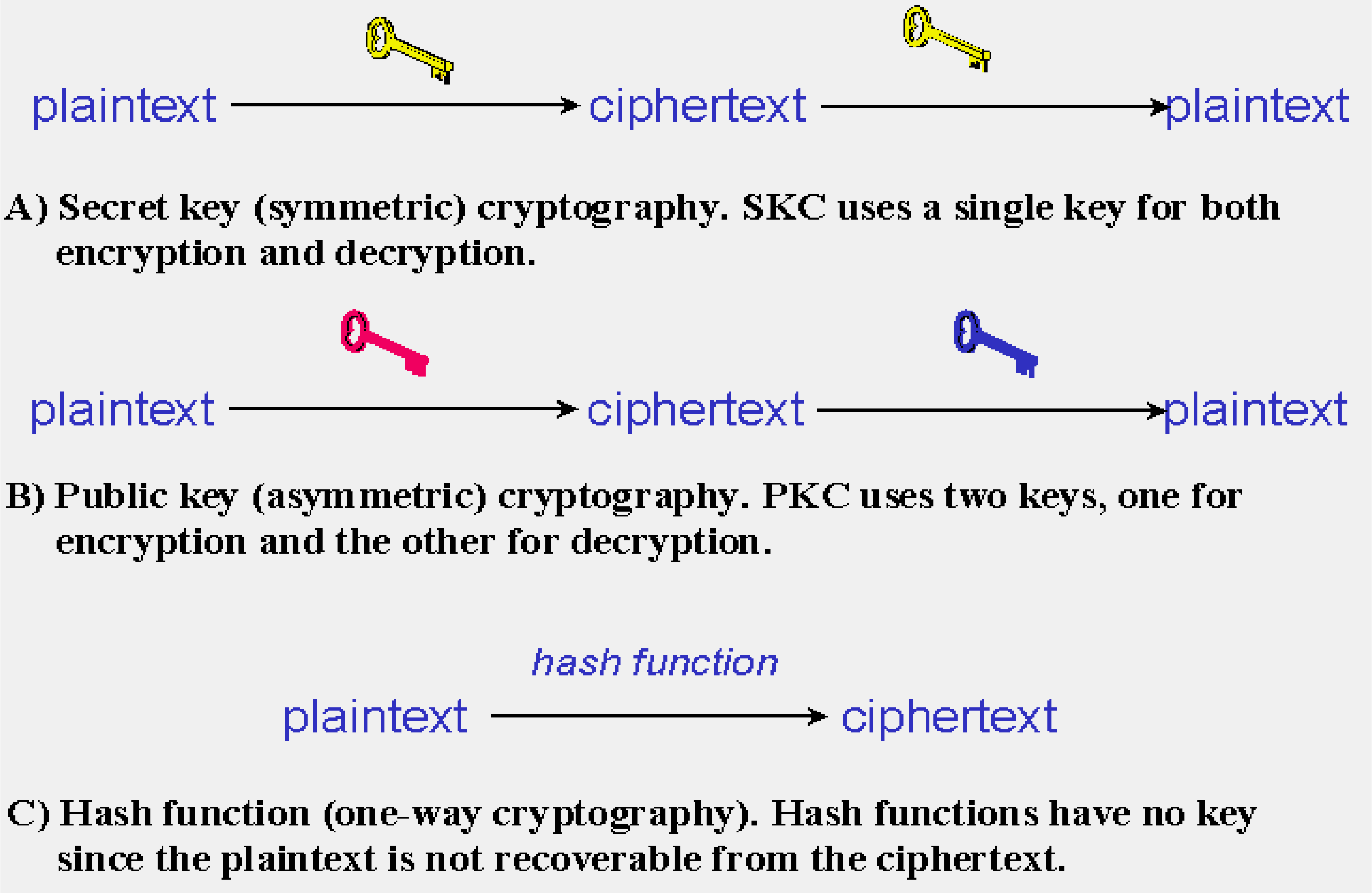
❖Hash function

✓Hash function (massage digests or one – way encryption) uses no key for encryption and decryption





THE LEXICON OF CRYPTOGRAPHY



plaintext → ciphertext → plaintext

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

plaintext → ciphertext → plaintext

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

hash function

plaintext → ciphertext

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Cryptographic Systems Classification

(3) The way in which the plaintext is processed

- Two types

1. **Block cipher:** Encrypts block of data of fixed size.
2. **Stream cipher:** Encrypts continuous streams of data (one bit or one byte at a time).

ENCRYPTION ALGORITHMS

Encryption Algorithms

- **Cipher** are algorithms used to encrypt or decrypt the data.

Two Categories

- **Classical cryptography**
  - ✓Encryption/decryption done by hand
  - ✓**Examples:** Caesar Cipher, Hill Cipher, Vigenère Cipher
- **Modern cryptography**
  - ✓Computers to encrypt and decrypt
  - ✓Same principles, but automation allows ciphers to beco me much more complex

CAESAR CIPHER

- **Original meaning:** The Caesar cipher involves replacing each letter of alphabet with the letter standing three places further down the alphabet.
- **General Caesar algorithm:** The Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

Plain	meet	me	after	the	toga	party
Cipher	PHHW	PH	DIWHU	WKH	WRJD	SDUWB

plain:	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
CIPHER:	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

Encryption Algorithms

- **KEY POINTS**
  - Plaintext is always in **lowercase**
  - Ciphertext is in **uppercase**
  - Key values are **italicized lowercase**

CAESAR CIPHER

- Let us assign numerical equivalent to each letter:

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 algorithm can be expressed as follows:

$$C=E(3, p) = (p+3) \bmod 26$$ {Arithmetic Modular}

- The shift may be of any amount, so that the general Caesar algorithm:

$$\mathbf{c = E(\mathit{k}, p) = (p + \mathit{k}\ ) \bmod 26}$$

c = (p+k) mod 26

Where k takes the value in the range 1 to 25.

The decryption algorithm is simple:

$$\mathbf{p = D(\mathit{k}, C) = (c - \mathit{k}) \bmod 26}$$

p = (c-k) mod 26

CLASS ACTIVITY

- Caesar Cipher examples

STRONG CRYPTOGRAPHY

- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of **ciphertext** with the **plaintext** that produced each cipher text.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.
- **Assumptions**
  - ✓ We do not need to keep the algorithm secret, we need to keep only the key secret.
  - ✓ We assume that it is impractical to decrypt a message on the basis of the cipher text plus knowledge of encryption/decryption algorithm.

STRONG CRYPTOGRAPHY

- An encryption scheme is **unconditionally secure** if
  - ✓ The ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
- An encryption scheme is said to be **computationally secure** if:
  1. The cost of breaking the cipher exceeds the value of the encrypted information, and
  2. The time required to break the cipher exceeds the useful lifetime of the information.

Attacks in Cryptosystems

- The objective of attacking encryption system is to recover the key in use rather that simply to recover the plaintext of a single ciphertext.
- Two general approaches:
  - ✓ **Cryptanalysis**
    - ❑ This type of attack exploits the characteristics of algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
  - ✓ **Brute-Force Attack**
    - ❑ The attacker tries every possible key on a piece of ciphertext until intelligible translation into plain text is obtained.

BRUTE-FORCE: CAESAR CIPHER

- Simply try all the 25 possible keys:
- Assumptions:
  - ✓The encryption and decryption algorithms are known;
  - ✓There are only25 keys to try;
  - ✓The language of the plaintext is known and easily recognizable.

EXAMPLE OF BRUTE-FORCE CRYPTANALYSIS

	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
Key						
1	oggy	og	chvgt	vjg	vgic	rctva
2	nffu	nf	bgufs	uif	uphb	qbauz
3	**meet**	**me**	**after**	**the**	**toga**	**party**
4	idda	id	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	juins
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlg
12	dvvk	dv	rwkvi	kyv	kfxr	qrikp
13	cuuj	cu	qvjuh	jxu	jweq	fghjo
14	assh	as	othsf	hvs	hcuo	dofhm
15	btti	bt	pultg	iwt	idvp	epgin
16	zrrg	zr	nsrge	gur	gbtn	cnegl
17	yggf	yg	mrfgd	ftq	faam	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwol	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	qlzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

CAESAR CIPHER

- Advantages and Disadvantages of the Caesar Cipher
- **Advantage:** Easy to use
- **Disadvantage**
  - ✓ The only problem with this cryptosystem is that it is easly broken. That is, it is possible for unuathorized person to convert the ciphetext back to plaintext.

MONOALPHABETIC CIPHER

- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.

plain:	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
CIPHER:	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

- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters then there are 26! Or greater than 4x10^{26} possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. This is referred to **“monoalphabetic substitution cipher”**

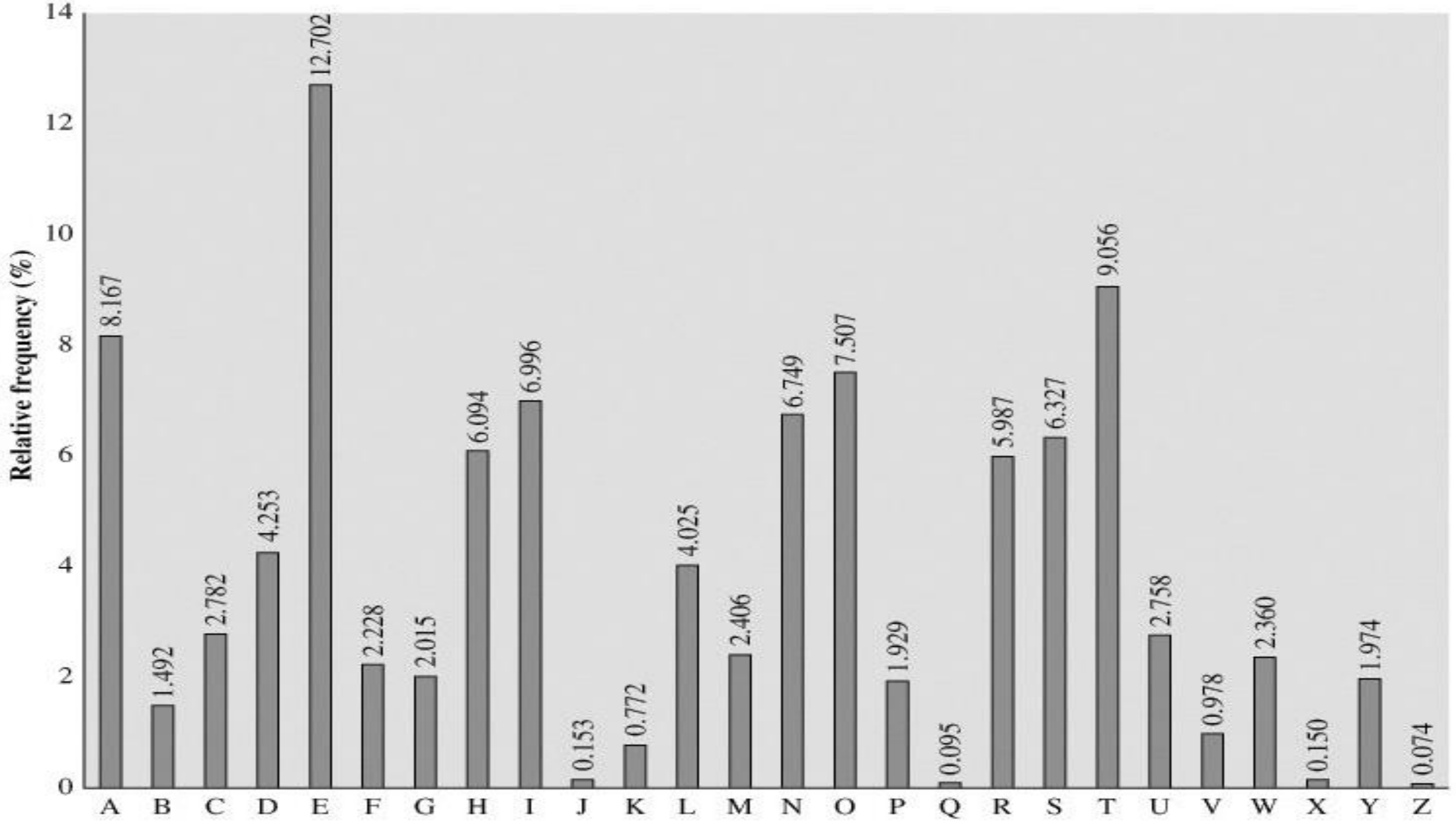
ANOTHER LINE OF ATTACK

- If the cryptanalyst knows the nature of the plain text (eg. Noncompressed English text), then the analyst can exploit the regularities of the language **(Cryptanalysis using frequency table).**

The frequencies of occurrence of letters constitute an elementary characteristic of a natural language.

In English, the most frequent letters are E, T, A, O, N, R, I, S, and H.
Roughly 13% of the letters in a large sample of English text should be E’s.

Relative Frequency of Letters in English Text



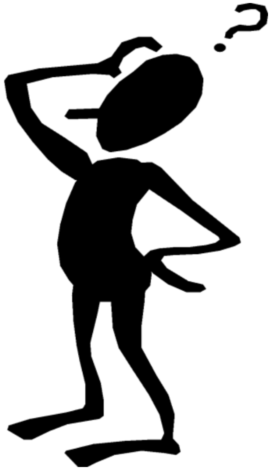
- In English, the most frequent letters are E, T, A, O, N, R, I, S, and H.

Types of Attacks on Encrypted Messages

- **Ciphertext only**
  - ✓ In this attack the attacker knows only the ciphertext to be decoded. The attacker will try to find the key or decrypt one or more pieces of ciphertext (only relatively weak algorithms fail to withstand a ciphertext-only attack).
- **Known plaintext**
  - ✓ The attacker has a collection of plaintext-ciphertext pairs and is trying to find the key or to decrypt some other ciphertext that has been encrypted with the same key.
- **Chosen plaintext**
  - ✓ This is a known plaintext attack in which the attacker can choose the plaintext to be encrypted and read the corresponding ciphertext.
- **Chosen ciphertext**
  - ✓ The attacker has the able to select any ciphertext and study the plaintext produced by decrypting them.

Cryptography Tools

- communiCrypt File Encryption Tool: http://www.communicrypt.com
- Steganos LockNote: http://www.steganos.com
- AxCrypt: http://www.axantum.com
- AutoKrypt: http://www.hiteksoftware.com
- CryptoForge: http://www.cryptoforge.com
- Ncrypt XL: http://www.littlelite.net
- ccrypt: http://www.sourceforge.net
- Cypherix: http://www.cypherix.com



END

IA 124 LECTURE 03