CS 0111:
INTRODUCTION TO IT SECURITY

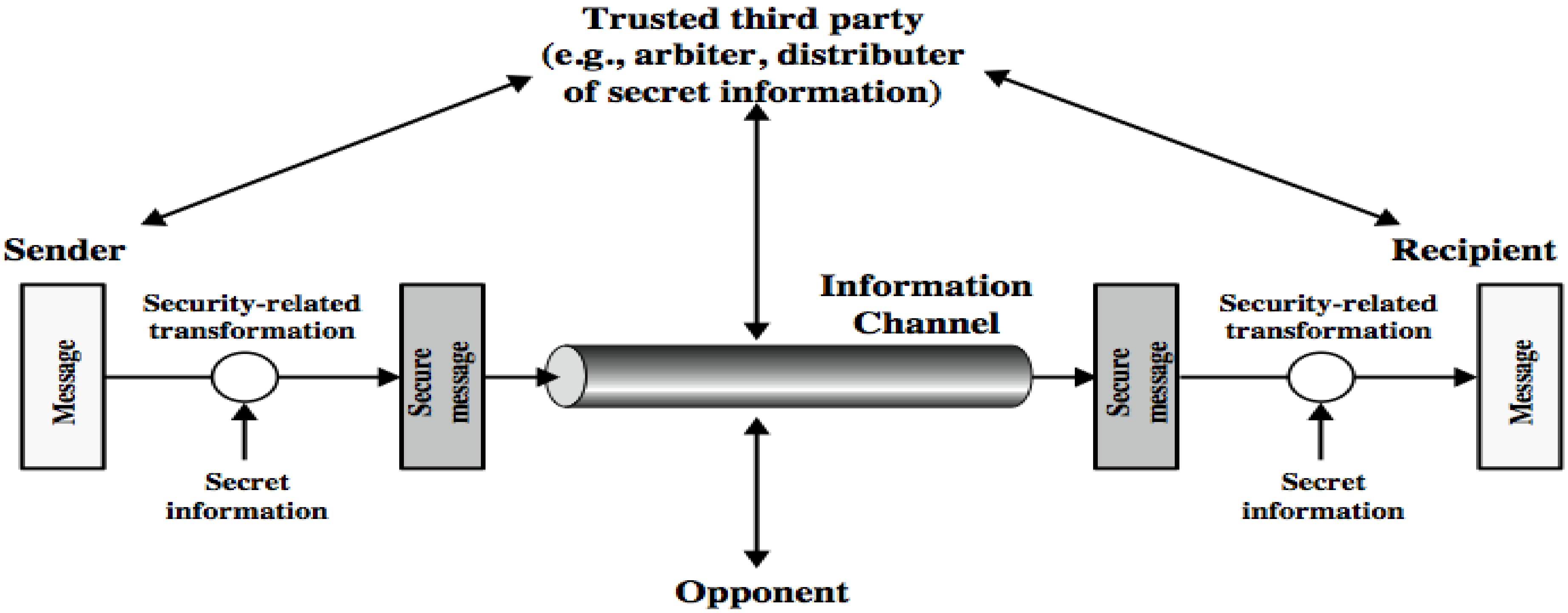
LECTURE 04
PRACTICAL CRYPTOGRAPHY (a)

Security Mechanism

- Is a method, tool, or procedure that provide a security services.
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use: **Cryptographic techniques**
- Hence our focus on this topic
- **Other Methods of Defense**
  - ✓ Software Controls (access limitations in a data base, in operating system protect each user from other users)
  - ✓ Hardware Controls (e.g. firewalls, smartcard)
  - ✓ Policies (e.g.. frequent changes of passwords)
  - ✓ Physical Controls (e.g. locked doors, guards)

Model for Network Security

- **Basic tasks**
  - ✓ Design an algorithm that opponent cannot defeat
  - ✓ Generate the secret information to be used with the algorithm
  - ✓ Develop methods for distributing secret information
  - ✓ Specify a protocol to be used
- May need a trusted third party to assist



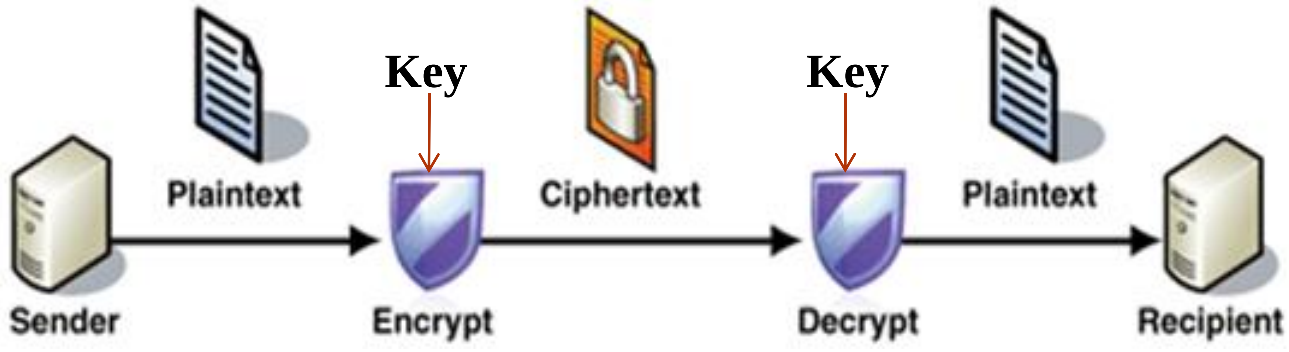
CRYPTOGRAPHY CONCEPTS

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**

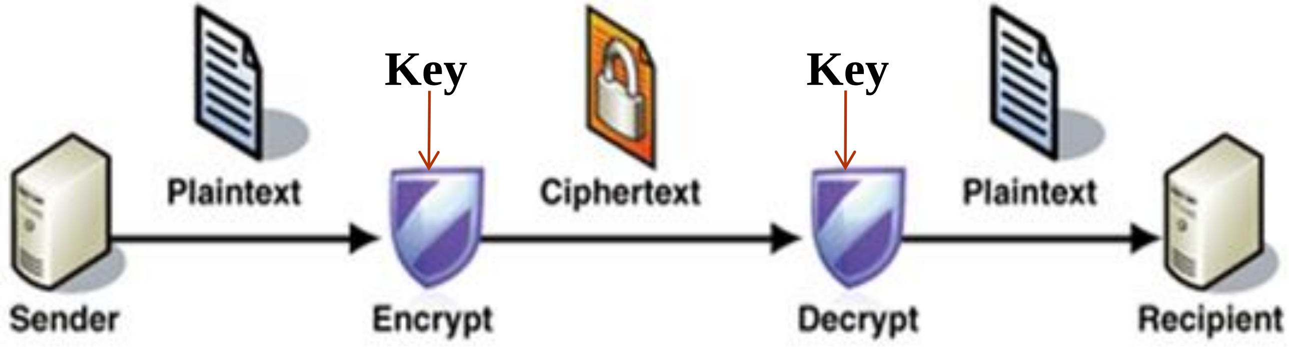
1. **Confidentiality**
2. **Integrity**
3. **Authentication**
4. **Non-repudiation**

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

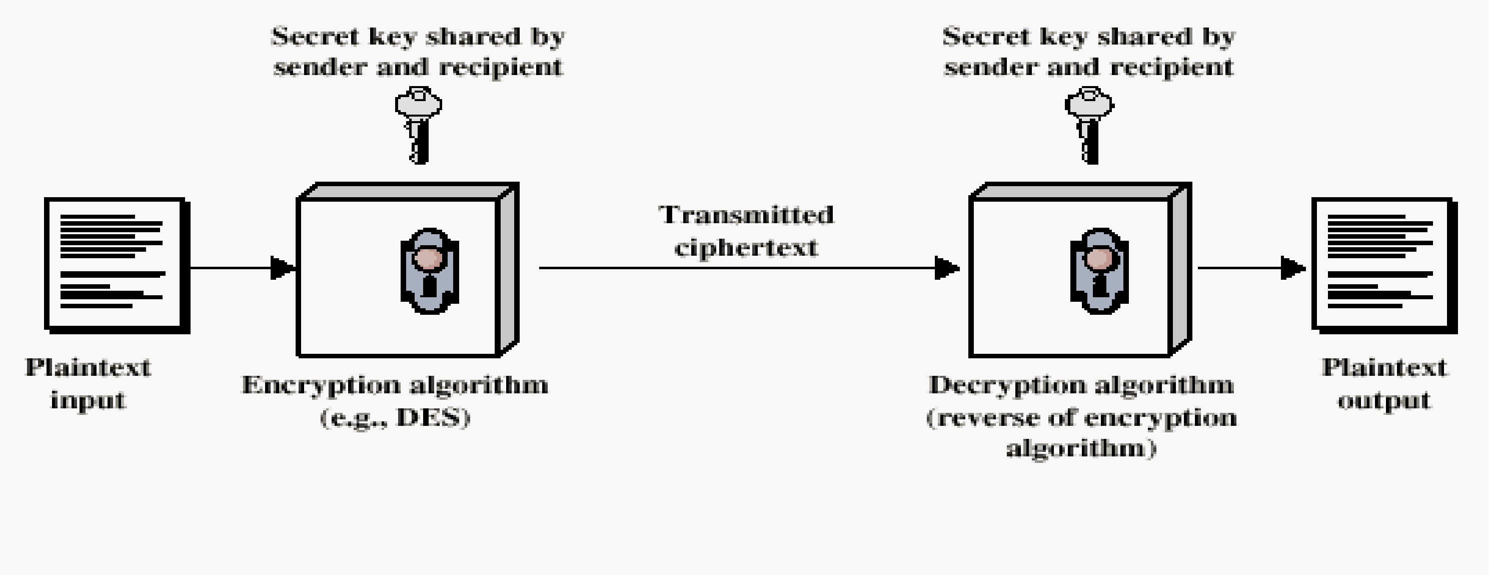

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

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**

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.
2. The number of **keys** used.
3. The way in which the plaintext is **processed**.

Cryptographic Systems Classification

(1) The type of **operations** used for transforming plaintext to ciphertext: All encryption algorithms are based on two general principles

- ✓ **Substitution cipher:** It replaces bits, characters, or blocks of characters with different bits, characters or blocks. e.g. Caesar cipher, hill cipher.
- ✓ **Transposition cipher:** The letters of the plaintext are shifted about to form the cryptogram. e.g. Rail fence.

(2) The number of **keys** used: General there are two types of encryption

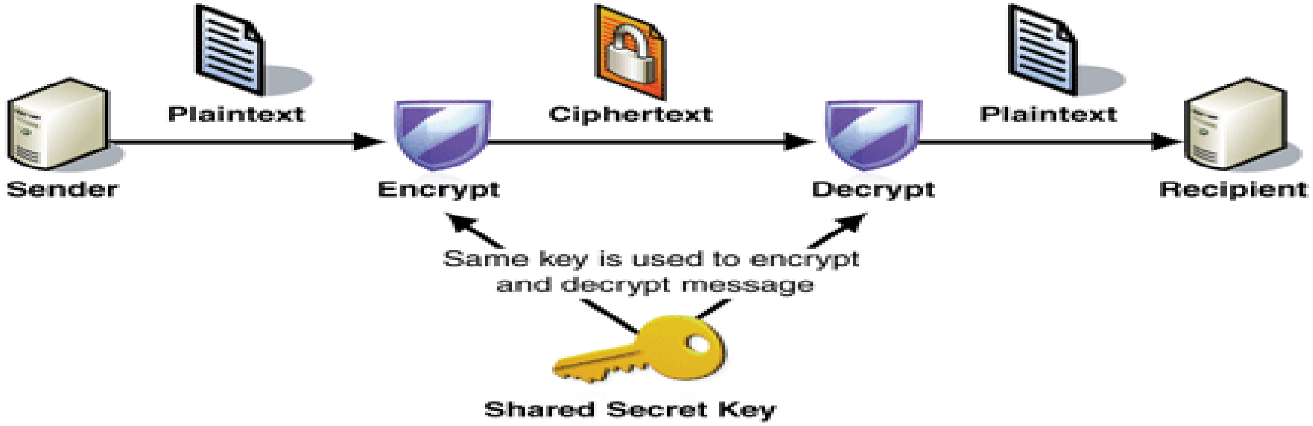
- ✓ **Symmetric**, single-key, secret-key, or conventional encryption.
  - If both sender and receiver use the same key.
  - Same key is used for encryption and decryption
- ✓ **Asymmetric**, two-key, or public-key encryption.
  - If the sender and receiver use different keys.
  - Different keys are used for encryption and decryption

(3) The way in which the plaintext is processed

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

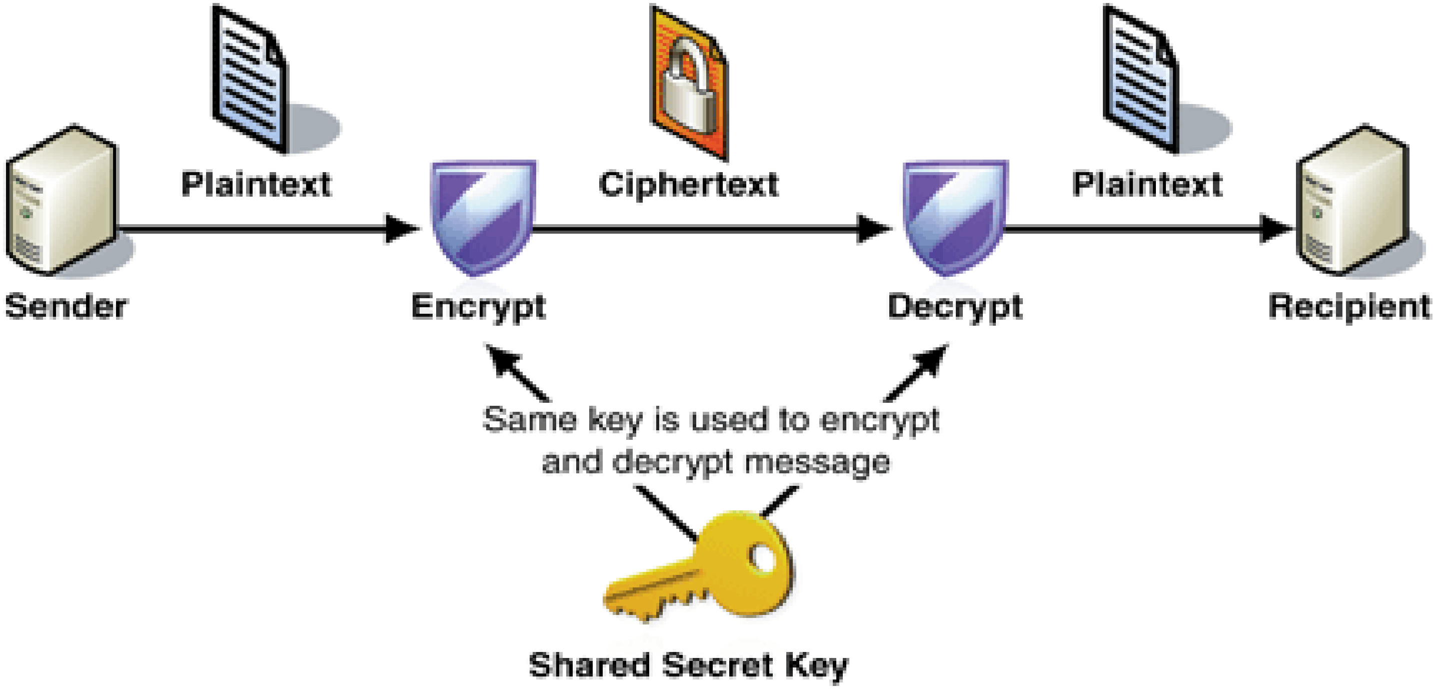
Cryptographic Systems Classification: number of keys used

- **Symmetric encryption**
- ✓ **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the same key.
- ✓ This key is known as **private/secret/single/shared key.**
- ✓ **Symmetric encryption** is also known as private-key /secret-key /single-key /shared-key encryption or conventional encryption .
- ✓ If the key is disclosed communications are compromised
- ✓ In **symmetric encryption**, both parties are equal
  - ❑ Hence does not protect sender from receiver forging a message & claiming is sent by sender



Symmetric Encryption

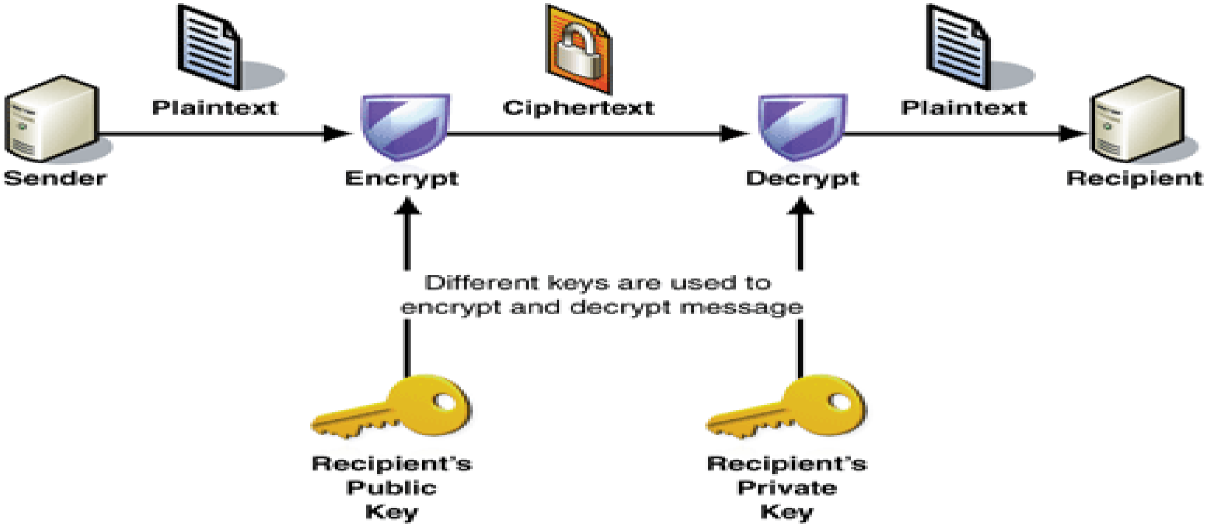
- Insufficiencies with **Symmetric Encryption**
  - ✓ **Key distribution:** how to have secure communications in general without having to trust a Key Distribution Centre (KDC) with your key.
  - ✓ **Digital signatures:** how to verify a message comes intact from the claimed sender



Asymmetric encryption

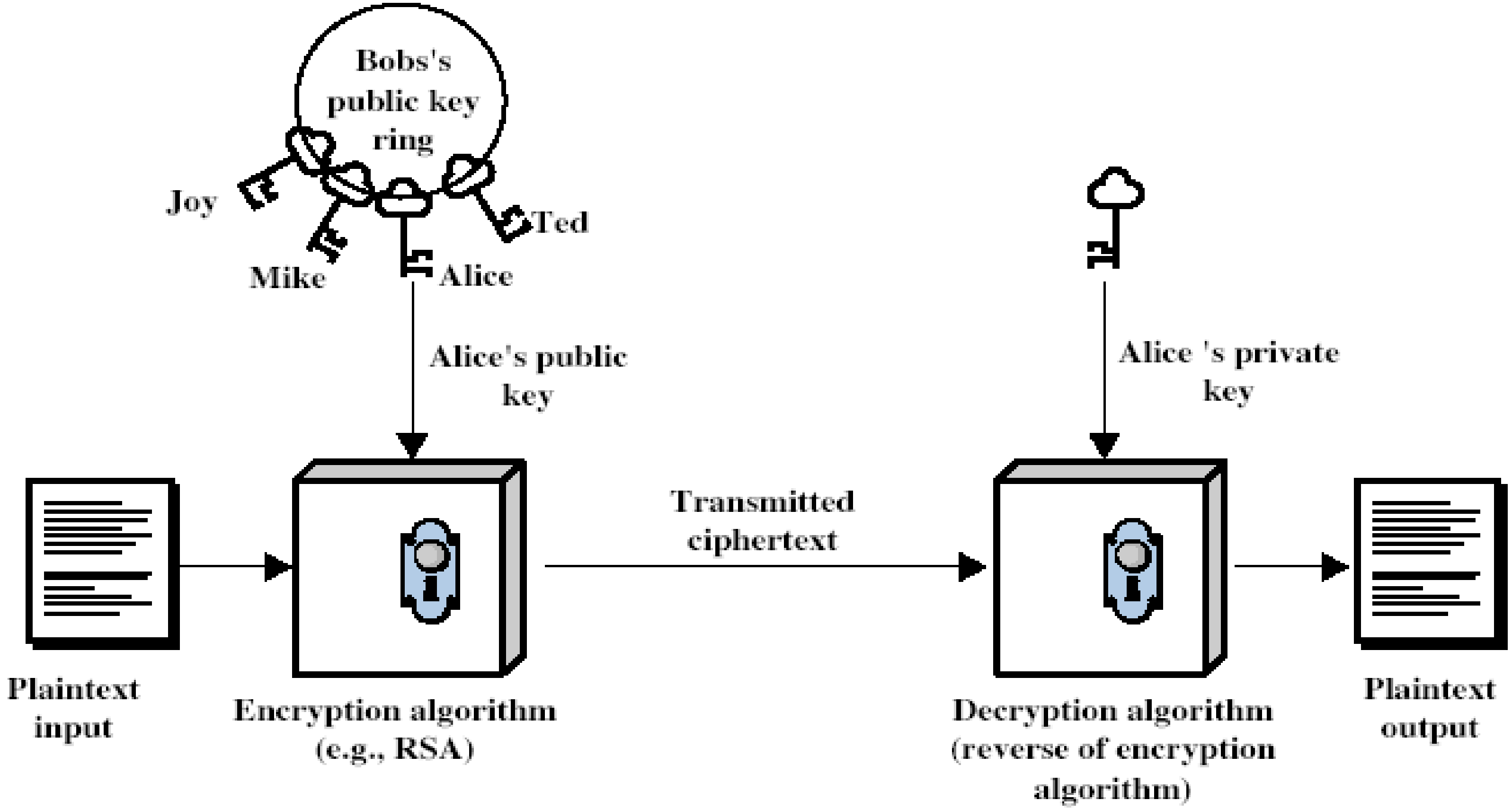
- ✓ **Asymmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using deferent keys
- ✓ These keys are known as public and private keys.
- ✓ **Asymmetric encryption** is also known as **Public-key / two-key** encryption involves the use of **two** keys:

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.**

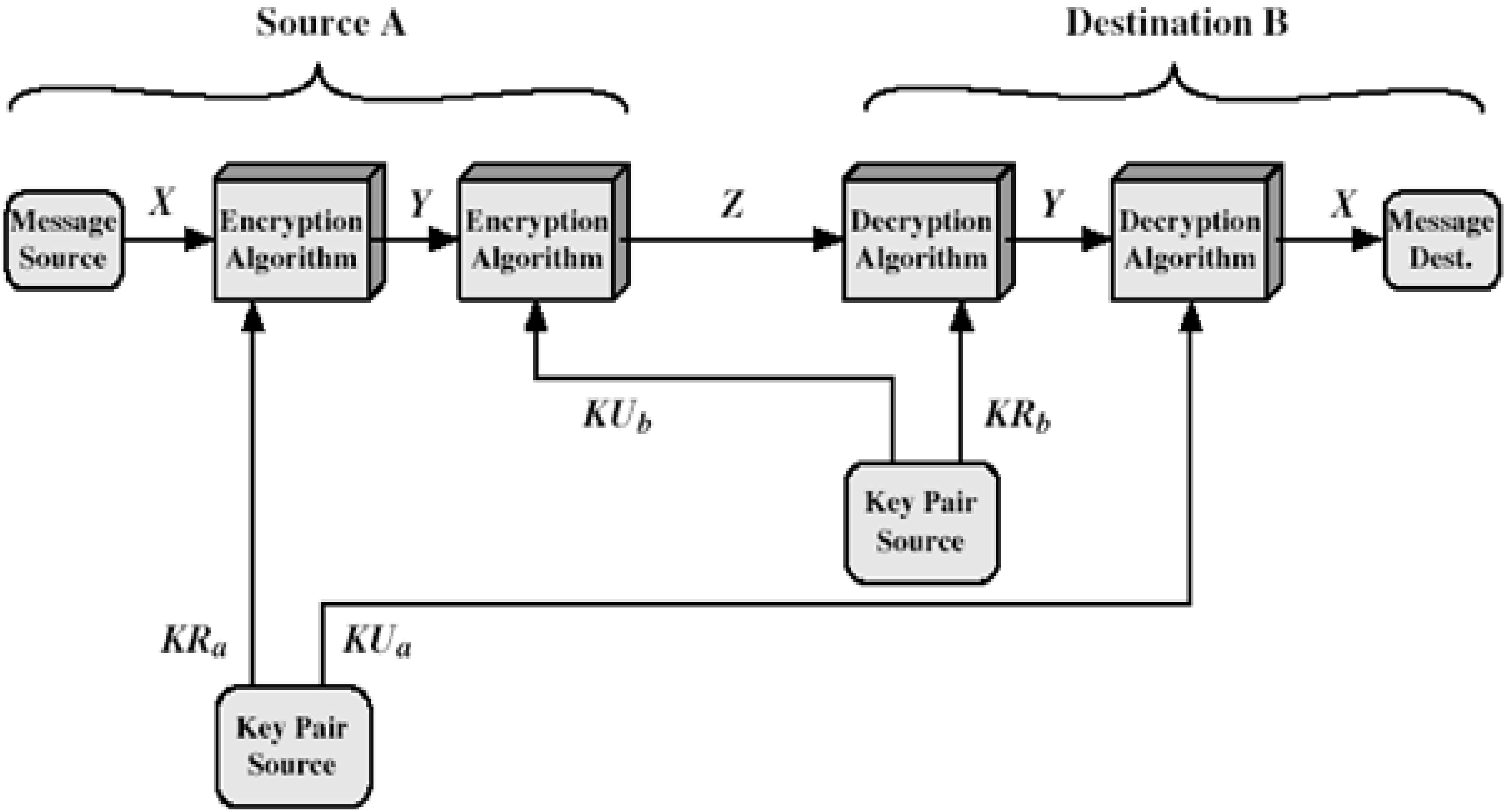


Asymmetric Encryption

- 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

- The type of **operations** used for transforming plaintext to ciphertext
- **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.
  - ✓ A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.
- **Key points**
  - ✓ Plaintext is always in **lowercase**
  - ✓ Ciphertext is in **uppercase**
  - ✓ Key values are **italicized lowercase**

CAESAR CIPHER

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

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) mod 26 {Arithmetic Modular}

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

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

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

The decryption algorithm is simple:

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

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

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"**

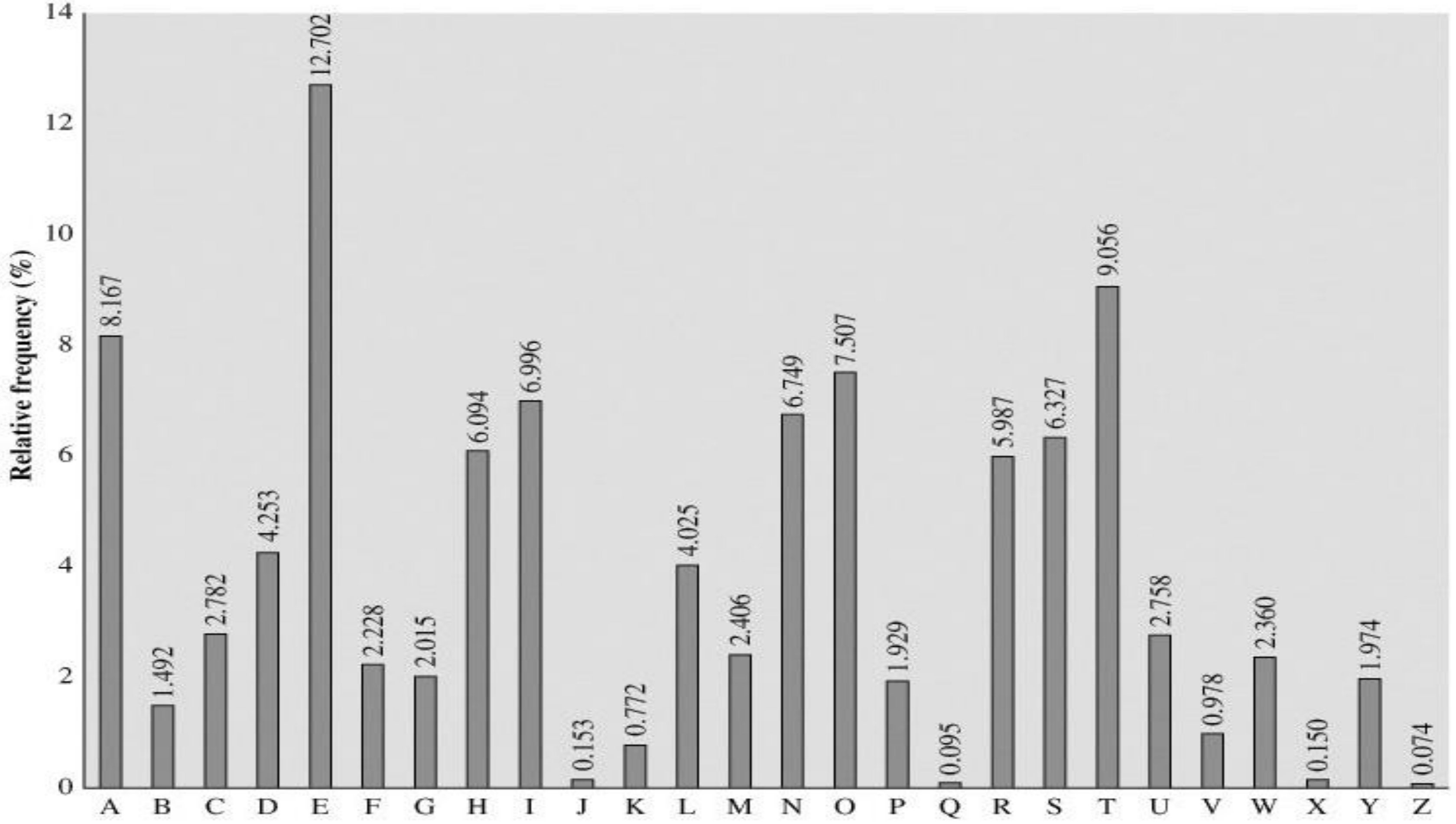
ANOTHER LINE OF ATTACK

- 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.

STRONG CRYPTOGRAPHY

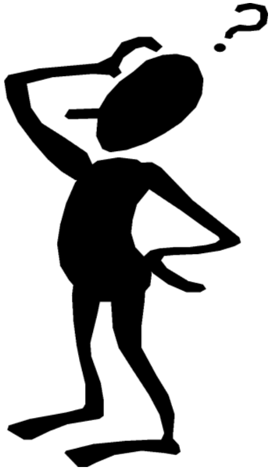
- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of **ciphertext** with the **plaintext** that produced each cipher text.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key 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.

CLASS ACTIVITY

1. What is the effect if either of the attack succeeds in deducing the key?
2. Why ciphertext-only attack is the easiest to defend against hacker?



END

CS 0111 LECTURE 04

CS 0111:

INTRODUCTION TO IT SECURITY

LECTURE 05

PRACTICAL CRYPTOGRAPHY (b)

OUTLINE

1. Vigenere Cipher
2. Hill Cipher
3. Rail Fence

SUBSTITUTION CIPHER

❖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.
- ✓Such a **one-to-many** correspondence makes the use of frequency analysis much more difficult in order to crack the code.
- ✓We describe one such cipher named for Blaise de Vigenere a 16-th century Frenchman.

VIGENERE CIPHER

- The Vigenere cipher is a polyalphabetic cipher based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters.
- The procedure is based on the tableau and the use of a **keyword**.
- The **letters of the keyword** determine the **shifted alphabets** used in the encoding process.

- A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

VIGENERE TABLEAU

PLAINTEXT LETTERS

KEYWORD LETTERS

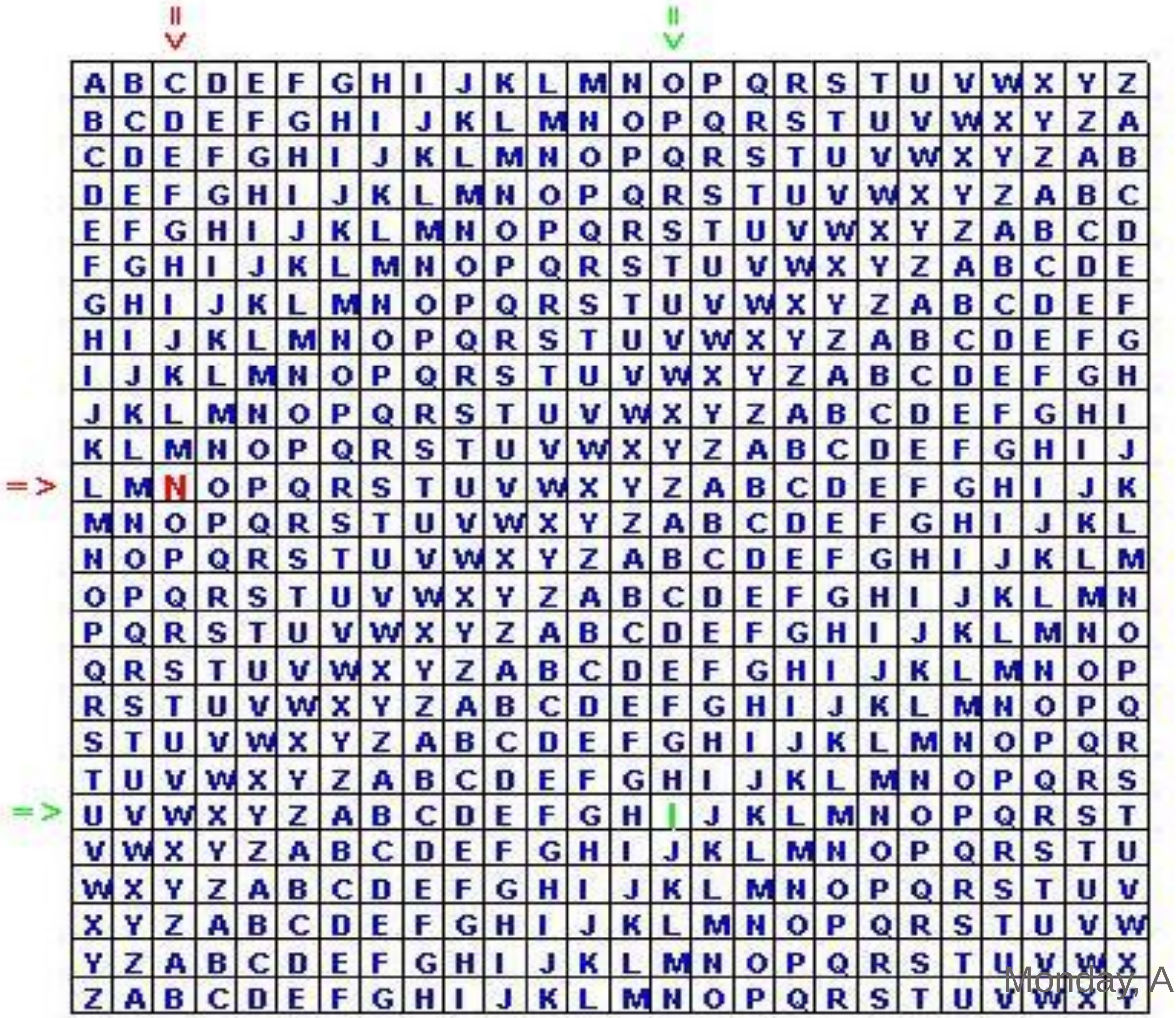
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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

VIGENERE CIPHER

- **For example** the message “computing gives insight” and keyword “*lucky*” we proceed by repeating the keyword as many times as needed above the message, as follows.

plaintext	**c**	**o**	**m**	**p**	**u**	**t**	**i**	**n**	**g**	**g**	**i**	**v**	**e**	**s**	**i**	**n**	**s**	**i**	**g**	**h**	**t**
key	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***

1. For each letter of the message use the letter of the keyword to determine a row and go across the row to the column headed by the corresponding letter of the message.
   - ✓ It follows that the first two letters "CO" in the message are encoded as "NI".



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

PLAINTEXT LETTERS

KEYWORD LETTERS

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

It follows that the first letter “c" in the message is encoded as "N"

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

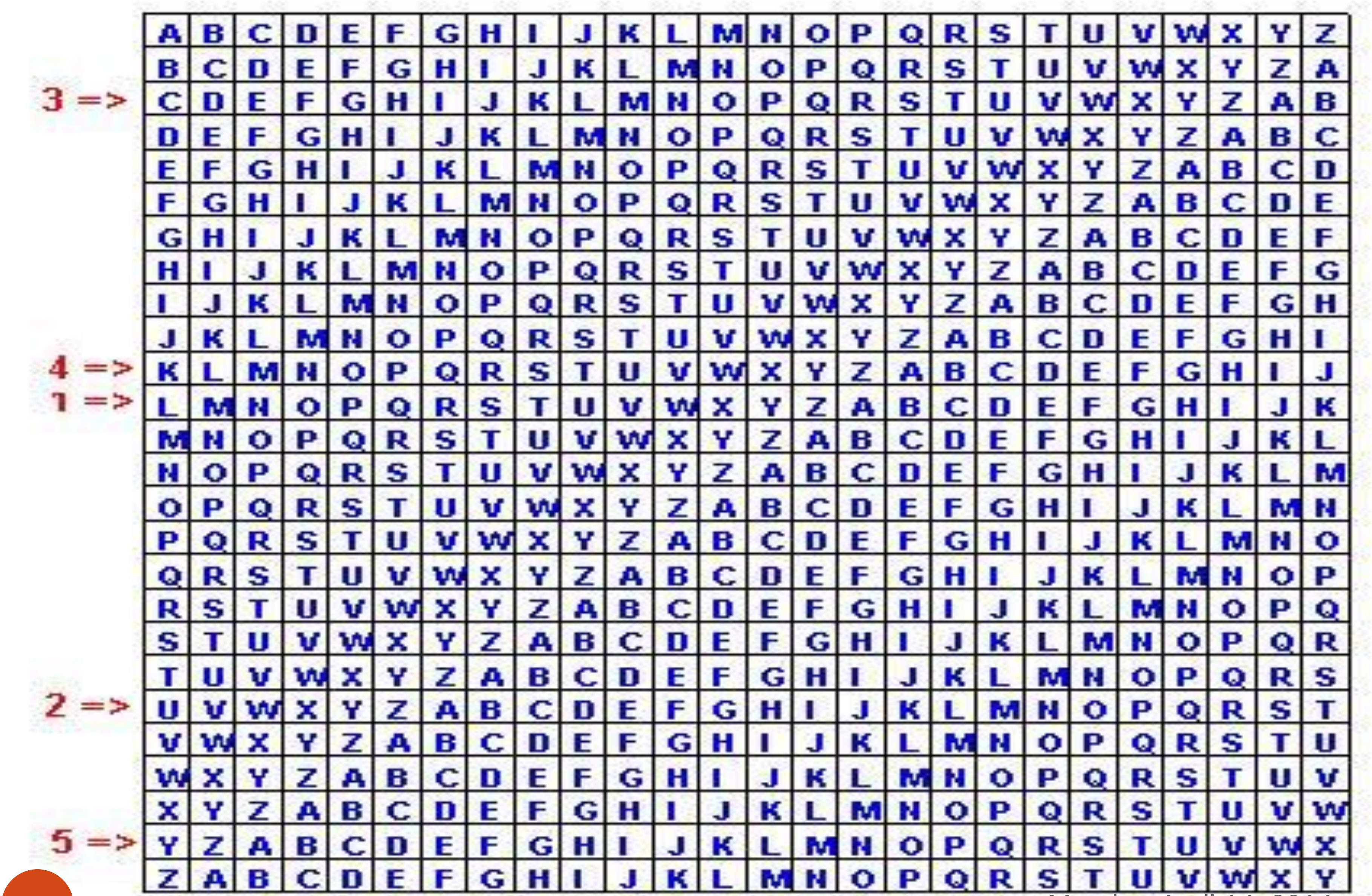
It follows that the first letter “o" in the message is encoded as “I"

VIGENERE CIPHER

2. We use the shifted alphabets that start with the letters of the keyword in the order indicated by the numbered arrows. This group of alphabets is repeated as many times as needed to assign an alphabet to each letter of the message. We append a standard alphabet at the top of this set of shifted alphabets to produce the **Vigenere Code Table**

VIGENERE CIPHER

lucky



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

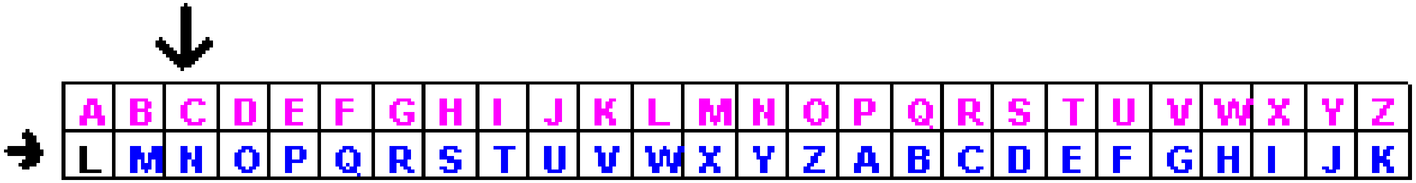
VIGENERE CIPHER

CODE TABLE

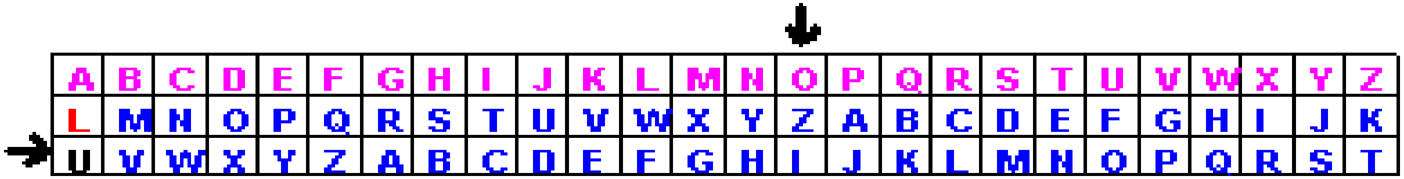
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S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

VIGENERE CIPHER

- Using the letters of the message in order we substitute the letter in the shifted alphabet associated with the letter of the keyword that appears immediately above it by going across to the column headed by that letter in the code table. To encode the first letter C we use the row of the code indicated by the arrow and the column indicated by the arrow. Hence the letter N is substituted for C.
- Use the same procedures for other letters on the message.



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



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

VIGENERE CIPHER

- Ciphertext encoded of the message from the table is: NIOZSECPQETPGCGYMKQFE

plaintext	**c**	**o**	**m**	**p**	**u**	**t**	**i**	**n**	**g**	**g**	**i**	**v**	**e**	**s**	**i**	**n**	**s**	**i**	**g**	**h**	**t**
key	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***	***u***	***c***	***k***	***y***	***l***
CIPHERTEXT	**N**	**I**	**O**	**Z**	**S**	**E**	**C**	**P**	**Q**	**E**	**T**	**P**	**G**	**C**	**G**	**Y**	**M**	**K**	**Q**	**F**	**E**

VIGENERE CIPHER

Example Two

- Uses Caesar's cipher with various different shifts, in order to hide the distribution of the letters. The key defines the shift used in each letter in the text. A key word is repeated as many times as required to become the same length as the plaintext. The result is added to the plaintext as follows:

plaintext	**v**	**e**	**g**	**e**	**n**	**e**	**r**	**e**	**s**	**c**	**i**	**p**	**h**	**e**	**r**
key	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***

Calculate Ciphertext.

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

VIGENERE CIPHER

- Ciphertext encoded of the message from the table is: **FMEORCBIQMMNRIP**

plaintext	**v**	**e**	**g**	**e**	**n**	**e**	**r**	**e**	**s**	**c**	**i**	**p**	**h**	**e**	**r**
key	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***	***k***	***e***	***y***
CIPHERTEXT	**F**	**M**	**E**	**O**	**R**	**C**	**B**	**I**	**Q**	**M**	**M**	**N**	**R**	**I**	**P**

CLASS ACTIVITY

1. Explain what relationship the Vigenere cipher has to the Caesar cipher.
2. The following ciphertext "OOWL KG HZGFBAJSUI" was created using a Vigenere cipher with the keyword "*code*". Use the table below to decode it.

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

HILL CIPHER

HILL CIPHER

- The Hill cipher was developed by the mathematician Lester Hill in 1929.
- The substitution is determined by *m* liner equations in which each character is assigned a numerical value (a=0, b=1,…z=25). For *m* =3, the system can be described as follows:

$$C_1 = (k_{11}p_1 + K_{12}p_2 + k_{13}p_3) \bmod 26$$
$$C_2 = (k_{21}p_1 + K_{22}p_2 + k_{23}p_3) \bmod 26$$
$$C_3 = (k_{31}p_1 + K_{32}p_2 + k_{33}p_3) \bmod 26$$

HILL CIPHER

- This can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} mod\ 26$$

Where C and P are column vectors of length 3, representing plaintext and ciphertext and **k** is 3x3 matrix representing the encryption key.

In general terms, the Hill system can be expressed as follows:

$$C = E(K, P) = KP \bmod 26$$

$$P = D(K, P) = K^{-1}C \bmod 26 = K^{-1}KP = P$$

HILL CIPHER

- Suppose that Alice wants to send a message to Bob and they have decided to use the Hill cipher.
- First, the plaintext is divided into blocks p0,p1,p2, . . ., each consisting of n letters.
- Alice then chooses an n x n invertible matrix A, with the entries reduced modulo 26, which acts as the key.
- Encryption is accomplished by computing the ciphertextas C_i= AP_i (mod 26) for each plaintext block pi.
- Bob decrypts the message by computing A-1ci(mod 26),for each ciphertextblock ci, where A-1is the inverse of A, modulo 26.

HILL CIPHER (example 1)

- Let n = 2 and $A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$

- Plaintext: meetmehere = (12,4,4,19,12,4,7,4,17,4)

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
	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

- Then $p_0 = \begin{bmatrix} 12 \\ 4 \end{bmatrix}, p_1 = \begin{bmatrix} 4 \\ 19 \end{bmatrix}, p_2 = \begin{bmatrix} 12 \\ 4 \end{bmatrix}, p_3 = \begin{bmatrix} 7 \\ 4 \end{bmatrix}, p_4 = \begin{bmatrix} 17 \\ 4 \end{bmatrix}$

- And $c_0 = \begin{bmatrix} 4 \\ 22 \end{bmatrix}, c_1 = \begin{bmatrix} 23 \\ 9 \end{bmatrix}, c_2 = \begin{bmatrix} 4 \\ 22 \end{bmatrix}, c_3 = \begin{bmatrix} 24 \\ 19 \end{bmatrix}, c_4 = \begin{bmatrix} 10 \\ 25 \end{bmatrix}$

- Ciphertext: (4,22,23,9,4,22,24,19,10,25) = EWXJEWYTKZ

HILL CIPHER (example 2)

- Consider the plaintext “paymoremoney” and use the encryption key:

$$k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

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**
	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 first three letters “pay” are presented as (15, 0, 24)

$$\mathbf{C} = \mathbf{KP} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix}$$

So **C= “LNS” when P= “pay”**

Continue in this fashion the entire ciphetext is deduced as: LNSHDLEWMTRW

Class activity

- Decipher the message SQGKC PQTYJ using the Hill cipher with the inverse key $\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$. Show your calculations and the result.

HILL CIPHER (example 3)

$$P = D(K, P) = K^{-1}C \bmod 26$$

- Recall how the inverse of a matrix is constructed. Here is an example using a encryption key 2×2
- Say, the encryption key is $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}$$

TRANSPOSITION CIPHER

RAIL FENCE

TRANSPOSITION TECHNIQUES

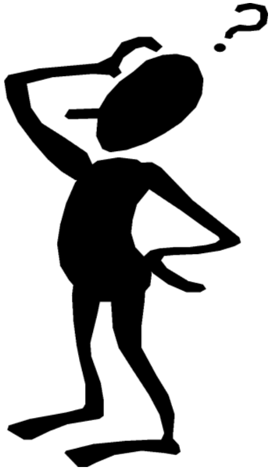
- Transposition is mapping which is achieved by performing some of permutation on the plaintext letters.
  - A **transposition cipher** involves a permutation of the plaintext letters.

RAIL FENCE

- The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows:
- For example , encipher the message " meet me after the toga party" with a rail fence of **depth** 2.
- The encryption message is :

MEMATRHTGPRYETEFETEOAAT

m	**e**	**m**	**a**	**t**	**r**	**h**	**t**	**g**	**p**	**r**	**y**
	e	t	e	f	e	t	e	o	a	a	t



END

CS 0111 LECTURE 05