Lecture 10

Definition 1: A *mono-alphabetic cipher* uses the same substitution across the entire message.

Definition 2: In a *poly-alphabetic cipher*, the substitution may change throughout the message.

Key Phrase Cipher

- Also called the Vigenère cipher.
- Consists of using several Caesar ciphers in sequence with different shift values. These shift values are determined by a key phrase.

For example, suppose we choose the key phrase "HAM". The sender repeats it until it matches the length of the plaintext.

Each letter is encoded by finding the intersection in the grid between the plaintext letter and keyword letter.

Example 1:
To encode the plaintext "student" we would:

H A M H A M H
S T U D E N T

Z T G K E Z A

Now to decode the ciphertext "JEZAEDLD" we would:

H A M H A M H A
J E Z A E D L D

C E N T E R E D

encode →

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

← decode

Activity:

a	P	I	N	E	A	P	P	L	E
b	q	j	o	f	b	q	q	m	f
c	r	k	p	g	c	r	r	n	g
d	s	l	q	h	d	s	s	o	h
e	t	m	r	i	e	t	t	p	i
f	u	n	s	j	f	u	u	q	j
g	v	o	t	k	g	v	v	r	k
h	w	p	u	l	h	w	w	s	l
i	x	q	v	m	i	x	x	t	m
j	y	r	w	n	j	y	y	u	n
k	z	s	x	o	k	z	z	v	o
l	a	t	y	p	l	a	a	w	p
m	b	u	z	q	m	b	b	x	q
n	c	v	a	r	n	c	c	y	r
o	d	w	b	s	o	d	d	z	s
p	e	x	c	t	p	e	e	a	t
q	f	y	d	u	q	f	f	b	u
r	g	z	e	v	r	g	g	c	v
s	h	a	f	w	s	h	h	d	w
t	i	b	g	x	t	i	i	e	x
u	j	c	h	y	u	j	j	f	y
v	k	d	i	z	v	k	k	g	z
w	l	e	j	a	w	l	l	h	a
x	m	f	k	b	x	m	m	i	b
y	n	g	l	c	y	n	n	j	c
z	o	h	m	d	z	o	o	k	d

a	P	E	P	P	E	R	O	N	I
b	q	f	q	q	f	s	p	o	j
c	r	g	r	r	g	t	q	p	k
d	s	h	s	s	h	u	r	q	l
e	t	i	t	t	i	v	s	r	m
f	u	j	u	u	j	w	t	s	n
g	v	k	v	v	k	x	u	t	o
h	w	l	w	w	l	y	v	u	p
i	x	m	x	x	m	z	w	v	q
j	y	n	y	y	n	a	x	w	r
k	z	o	z	z	o	b	y	x	s
l	a	p	a	a	p	c	z	y	t
m	b	q	b	b	q	d	a	z	u
n	c	r	c	c	r	e	b	a	v
o	d	s	d	d	s	f	c	b	w
p	e	t	e	e	t	g	d	c	x
q	f	u	f	f	u	h	e	d	y
r	g	v	g	g	v	i	f	e	z
s	h	w	h	h	w	j	g	f	a
t	i	x	i	i	x	k	h	g	b
u	j	y	j	j	y	l	i	h	c
v	k	z	k	k	z	m	j	i	d
w	l	a	l	l	a	n	k	j	e
x	m	b	m	m	b	o	l	k	f
y	n	c	n	n	c	p	m	l	g
z	o	d	o	o	d	q	n	m	h

Using the key phrase “PINEAPPLE” decrypt the ciphertext:

PINEAPPLE PINE

WIJEIXPY TXHME

HAWAIIAN PIZZA

Using the key phrase “PEPPERONI” decrypt the ciphertext:

PEPPE RONIP EPPER ONIPE

RLXRE XCFBN PTSIV DQQHL

CHICAGO STYLE DEEP DISH

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

a	M	U	S	H	R	O	O	M
b	n	v	t	i	s	p	p	n
c	o	w	u	j	t	q	q	o
d	p	x	v	k	u	r	r	p
e	q	y	w	l	v	s	s	q
f	r	z	x	m	w	t	t	r
g	s	a	y	n	x	u	u	s
h	t	b	z	o	y	v	v	t
i	u	c	a	p	z	w	w	u
j	v	d	b	q	a	x	x	v
k	w	e	c	r	b	y	y	w
l	x	f	d	s	c	z	z	x
m	y	g	e	t	d	a	a	y
n	z	h	f	u	e	b	b	z
o	a	i	g	v	f	c	c	a
p	b	j	h	w	g	d	d	b
q	c	k	i	x	h	e	e	c
r	d	l	j	y	i	f	f	d
s	e	m	k	z	j	g	g	e
t	f	n	l	a	k	h	h	f
u	g	o	m	b	l	i	i	g
v	h	p	n	c	m	j	j	h
w	i	q	o	d	n	k	k	i
x	j	r	p	e	o	l	l	j
y	k	s	q	f	p	m	m	k
z	l	t	r	g	q	n	n	l

Using the key phrase "BEEF" decrypt the ciphertext:

BEEF BEEFBE

NIEY MSZJSW

MEAT LOVERS

Using the key phrase "MUSHROOM" decrypt the ciphertext:

MUSHROOMMUSH

BUFHXCDAGFGZ

PANAGOPOULOS

Hill Ciphers

- Plaintext is split up into n letter blocks.
- For this course we will only do hill ciphers for 2 letter blocks.
- If the number of plaintext letters is not a multiple of 2 we add an x. For example, the plaintext "Pizza" is split up into "Pi zz ax".
- Given a, b, c, d in mod 26 and a block "x y" in the plaintext, our encoding function is:

$$E(x) \equiv a \cdot x + b \cdot y \pmod{26}$$

$$E(y) \equiv c \cdot x + d \cdot y \pmod{26}$$

- If $ad - bc$ inverse in (mod 26) is δ then the inverse of the 2×2 matrix:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \equiv \delta \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

gives the decoding function for each block:

$$D(x) \equiv \delta d \cdot x - \delta b \cdot y \pmod{26}$$

$$D(y) \equiv -\delta c \cdot x + \delta a \cdot y \pmod{26}$$

Example 2: Consider the Hill Cipher with $a = 2, b = 1, c = 1, d = 1$ and

a) encode the plaintext "Pizza".
b) decode the cipher text "IBJQ".

a)
$E(P) \equiv 2(15) + (8) \equiv 12$ M
$E(I) \equiv (15) + (8) \equiv 23$ X

$E(Z) \equiv 2(-1) + (-1) \equiv 23$ X
$E(Z) \equiv (-1) + (-1) \equiv 24$ Y

$E(A) \equiv 2(0) + (-3) \equiv 23$ X
$E(x) \equiv (0) + (-3) \equiv 23$ X

b) $\delta \equiv (2 \cdot 1 - 1 \cdot 1)^{-1} \equiv 1^{-1} \equiv 1$

$D(I) \equiv (8) - (1) \equiv 7$ H
$D(B) \equiv -(8) + 2(1) \equiv -6$ U

$D(J) \equiv (9) - (-10) \equiv 19$ T
$D(Q) \equiv -(9) + 2(-10) \equiv -3$ X

Activity:

Decrypt the ciphertext message:

I I	W O	E Z	M D	M T	U H	O F	S P
8 8	-4 14	4 -1	12 3	12 -7	-6 7	14 5	-8 15

which was encrypted using Hill cipher with the encoding function:

$$E(x) \equiv 1 \cdot x + 2 \cdot y \mod 26$$
$$E(y) \equiv 1 \cdot x + 3 \cdot y \mod 26$$

$D(x) \equiv 3x - 2y$

$D(y) \equiv -x + y$

since $\delta^{-1} \equiv (3-2)^{-1} \equiv 1$

$D(8) \equiv 8$

$D(8) \equiv 0$

$D(-4) \equiv 12$

$D(14) \equiv -8$

$D(4) \equiv 14$

$D(-1) \equiv -5$

$D(12) \equiv 5$

$D(3) \equiv -9$

$D(12) \equiv -2$

$D(-7) \equiv 7$

$D(-6) \equiv -6$

$D(7) \equiv 13$

$D(14) \equiv 6$

$D(5) \equiv -9$

$D(-8) \equiv -2$

$D(15) \equiv -3$

(mod 26)