Lecture 9

Cryptography is the practice and study of hiding information.

There is a sender-receiver team on one side and a kibitzer on the other side.

Definition 1: *Plaintext* is the original message from the sender.

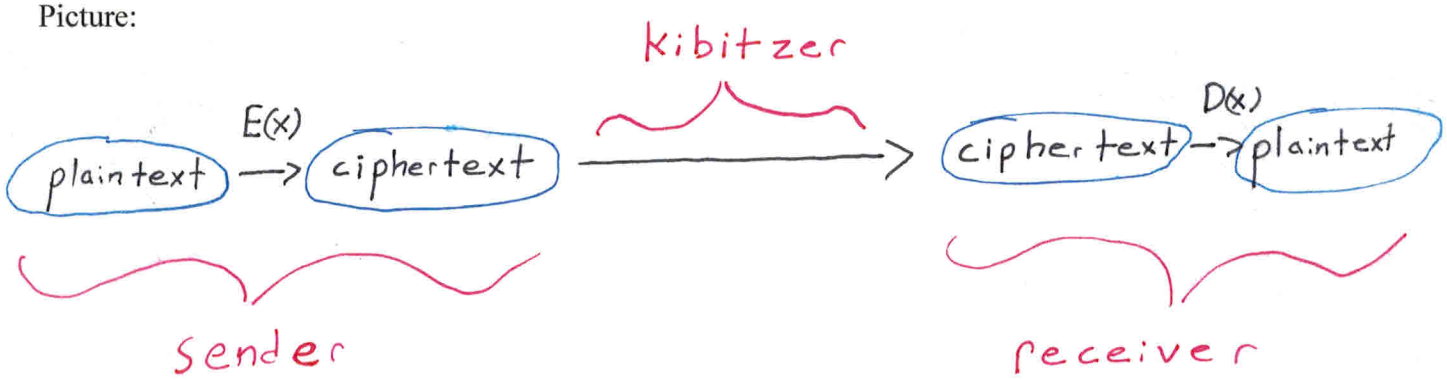
Definition 2: The sender knows an *encoding function* $E(x)$, which turns plaintext into gibberish.

Definition 3: The gibberish from $E(x)$, is called *ciphertext*.

Definition 4: The *kibitzer* is someone trying to obtain the original message from gibberish without $E(x)$.

Definition 5: The receiver knows a *decoding function* $D(x)$, which turns the gibberish back into the original message. So we have $D(E(x)) = x$ for any message x.

Picture:



We encode letters as numbers using mod 26:

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

Generalized Caesar's Code

a. The sender picks a value k and then shifts each letter in the plaintext with the encoding function:

$$E(x) \equiv x + k \bmod 26$$

b. The receiver can find the plaintext by using the decoding function:

$$D(x) \equiv x - k \bmod 26$$

c. The kibitzer can shift each letter in the ciphertext down the alphabet one by one until a word makes sense

Example 1:

a) Play the role of the sender. With $k \equiv 3$ use the generalized Caesar's code to encipher the word:

LET

M F U
N G V
O H W

b) Play the role of the receiver. With $k \equiv 3$ decipher the following word which was encoded using the generalized Caesar's code.

I T
J U
K V
LW

c) Play the role of the kibitzer. Find the plaintext from the following ciphertext which was encoded using the generalized Caesar's code.

B E
C F
D G
E H
F I
G J
H K

Note: the answer is not "EH" or "OR" since the message is "Let it BE".

GROUP 1

Koymncihm uly nby wlyuncpy uwnm iz chnyffcayhwy. - Zluhe Echaxih

GROUP 2

Dolu avsk "Spml pz ohyk." Cvsahpyl hzrlk "Jvtwhylk av doha?"

GROUP 3

Nby vynnyl juln iz ihy'm fczy wihmcmnm iz bcm zlcyhxmbcjm. --Uvlubug Fchwifh

GROUP 4

B phnew ktmaxk ux otznxer kbzam matg ikxvblxer pkhgz. – Dxrgxl

GROUP 5

“Mh uxebxox t mabgz bl bfihllbuex bl mh ftdx bm lh.” - Ykxgva ikhoxku

GROUP 6

"N zna pna or qrfgeblrq ohg abg qrsrngrq." - Rearfg Urzvatjnl

GROUP 7

"hmttxj yt gj tuynrnxynh, ny kjjqx gjyyjw." - Ifqn Qfrf

GROUP 1

Questions are the creative acts of intelligence. - Frank Kingdon

GROUP 2

When told "Life is hard." Voltaire asked "Compared to what?"

GROUP 3

The better part of one's life consists of his friendships. --Abraham Lincoln

GROUP 4

I would rather be vaguely right than precisely wrong. - Keynes

GROUP 5

"To believe a thing is impossible is to make it so." - French proverb

GROUP 6

"A man can be destroyed but not defeated." - Ernest Hemingway

GROUP 7

"Choose to be optimistic, it feels better." - Dali Lama

Linear Codes

a. The sender can encode plaintext with the function

$$E(x) \equiv ax + k \bmod 26$$

where a is relatively prime with 26.

b. The receiver can decode the ciphertext with the function:

$$D(x) \equiv a^{-1}(x - k) \bmod 26$$

where a^{-1} is the multiplicative inverse of a.

c. The kibitzer has to work harder to decipher a linear code than a Caesar's code. Though (s)he can use the following strategies:

1. By using frequency analysis for very long passages of English text, the following letter-use percentages have been observed:

Letter	% Frequency
E	12.02
T	9.1
A	8.12
O	7.68
I	7.31
N	6.95
S	6.28
R	6.02
H	5.92
D	4.32
L	3.98
U	2.88
C	2.71

Letter	% Frequency
M	2.61
F	2.3
Y	2.11
W	2.09
G	2.03
P	1.82
B	1.49
V	1.11
K	0.69
X	0.17
Q	0.11
J	0.1
Z	0.07

2. By using educated guesses/trial and error, the kibitzer may be able to find a common word in the ciphertext.

3. If the kibitzer can figure out two letters in the ciphertext, say $D(x_1) \equiv x_2$ and $D(y_1) \equiv y_2$, (s)he may be able to figure out the decoding function $D(x) \equiv bx + c$ by solving the system:

$$x_2 \equiv bx_1 + c \pmod{26}$$
$$y_2 \equiv by_1 + c \pmod{26}$$

Example 2:

a) Play the role of the sender. With $a \equiv 5,\ k \equiv 5$ use the linear code to encode the word:

THIS

$E(T) \equiv 5(19) + 5 \equiv -4 \equiv W$

$E(H) \equiv 5(7) + 5 \equiv 14 \equiv O$

$E(I) \equiv 5(8) + 5 \equiv -7 \equiv T$

$E(S) \equiv 5(18) + 5 \equiv -9 \equiv R$

WOTR

b) Play the role of the receiver. With $a \equiv 5, k \equiv 5$ use the linear code to decipher the word:

LTII

$-5 \cdot 5 \equiv 1$

$\therefore a^{-1} \equiv -5$

$D(L) \equiv -5(11-5) \equiv -4 \equiv W$

$D(T) \equiv -5(19-5) \equiv 8 \equiv I$

$D(I) \equiv -5(8-5) \equiv -15 \equiv L$

WILL

c) Play the role of the kibitzer. The ciphertext below was taken from a very long passage of ciphertext in which the letter Z appeared most often and the letter W appeared the second most often. Given that the very long passage of ciphertext was encoded using a linear code, find the plaintext.

CFRR

Let $D(x) = bx + c$ and guess that $D(Z) \equiv E$, $D(W) \equiv T$.

Solve:

$4 \equiv b(-1) + c$

$-7 \equiv b(-4) + c$

$11 \equiv 3b$

$\Rightarrow b \equiv 9 \cdot 11 \equiv -5$

$\Rightarrow c \equiv 4 + b \equiv -1$

$D(C) \equiv -5(2) - 1 \equiv -11 \equiv P$

$D(F) \equiv -5(5) - 1 \equiv -26 \equiv A$

$D(R) \equiv -5(-9) - 1 \equiv -8 \equiv S$

PASS

(mod 26)