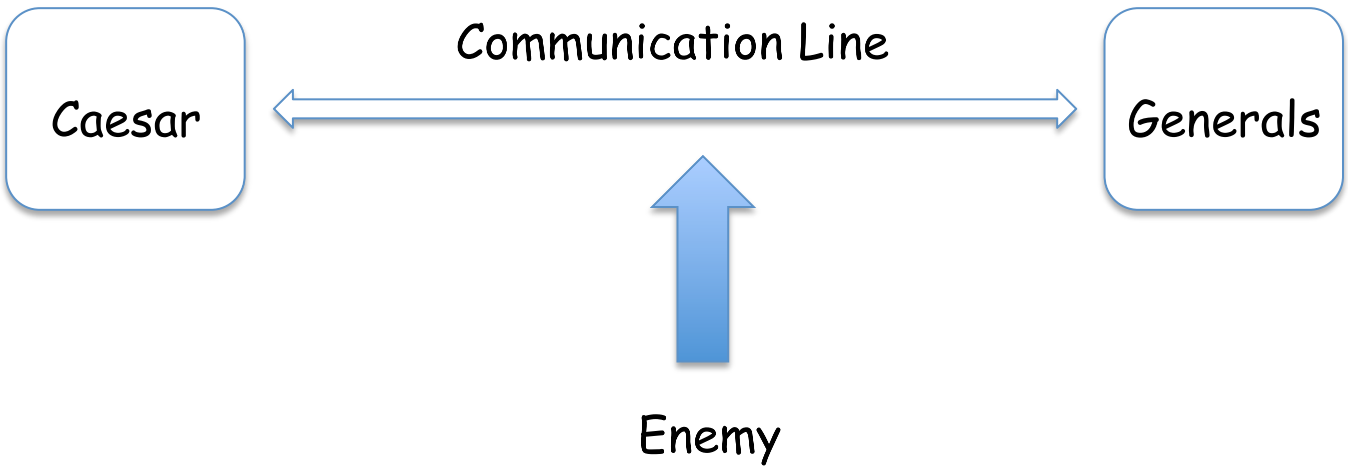
The War of Codemakers & Codebreakers

Çetin Kaya Koç   koc@cs.ucsb.edu

Since the time of Caesar or even earlier, people are interested in "secret communications"



To hide the content of his messages from the enemy, Caesar developed "an encryption method" = **Caesar Cipher**

Caesar Cipher

For every letter in the word, replace the letter with the letter 3 locations <u>ahead</u> in the alphabet

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

For example, if Caesar wants to send the order "attack", he encrypts it as:

attack -> **dwwdfn**

and sends it to his General.

The enemy also captures the message and sees "**dwwdfn**". But the enemy does not know what that means!! ☺

The General decrypts "dwwdfn" by replacing every letter with the letter 3 locations <u>back</u> in the alphabet. ☺

dwwdfn -> **attack**

Encryption

A transformation of the message such that

✧ your enemy captures the encrypted message
✧ your enemy should not be able to decrypt
✧ your friend receives the encrypted message
✧ your friend decrypts and obtains the message

✧ cryptography: science of making encryption methods
✧ cryptanalysis: science of breaking encryption methods
✧ cryptology: cryptography + cryptanalysis
✧ to encrypt, to decrypt; to encipher, to decipher
✧ cipher: cryptographic (crypto) algorithm
✧ message: meaningful text you are sending
✧ ciphertext: encrypted text

✧ There is "a civilized war" between cryptographers & cryptanalysts … codemakers & codebreakers

Exercises:

1. Encrypt “**wait**” using Caesar cipher

2. Encrypt “**yield**” using Caesar cipher

3. Encrypt “**return now**” using Caesar cipher

4. Decrypt “**uxq iru brxu olih**” using Caesar cipher

Representation

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

Every letter is represented as a number between 0 and 25
Instead of working with letters we work with numbers

Affine Cipher

Affine cipher encrypts or decrypts a number-represented letter using the formula

Encrypt using $\alpha = \alpha + k \bmod 26$
Decrypt using $\alpha = \alpha - k \bmod 26$

Here k is known to you and your friend
The enemy does not (should not) know k

k is called <u>the secret key</u>

<u>Caesar cipher</u> is an affine Cipher with $k = 3$

Encrypt using $\alpha = \alpha + 3 \bmod 26$
Decrypt using $\alpha = \alpha - 3 \bmod 26$

Affine Cipher Example

k = 11

Represent "**dinner**" using numbers "**3 8 13 13 4 17**"

Then encrypt "dinner" = "3 8 13 13 4 17" using k=11

$3 + 11 = 14 \bmod 26$ -> o
$8 + 11 = 19 \bmod 26$ -> t
$13 + 11 = 24 \bmod 26$ -> y
$13 + 11 = 24 \bmod 26$ -> y
$4 + 11 = 15 \bmod 26$ -> p
$17 + 11 = 28 = 2 \bmod 26$ -> c

"**dinner**" is encrypted as "**otyypc**"

Affine Cipher

Decryption **of "otyypc" = "14 19 24 24 15 2"**

Decryption method: $\alpha = \alpha - k \bmod 26$

14 - 11 = 3 mod 26	-> d
19 - 11 = 8 mod 26	-> i
24 - 11 = 13 mod 26	-> n
24 - 11 = 13 mod 26	-> n
15 - 11 = 4 mod 26	-> e
2 - 11 = -9 = 17 mod 26	-> r

The decrypted text is "**dinner**"

<u>Exercises</u>:

5. Encrypt "**avatar**" using the affine cipher with k=0

6. Encrypt "**rain**" using the affine cipher with k=10

7. Decrypt "**wtaad**" using the affine cipher with k=15

8. Decrypt "**cxeeh**" using affine cipher with k=19

Breaking Ciphers!!! ☺

Breaking or cryptanalysis of a cipher means

- ✧ <u>either</u>: decrypting without knowing the unknown key
- ✧ <u>or</u>: discovering the unknown key

Method 1: Try all possible keys

This encrypted message is given: “httpnj” and we don’t know k (key) … i.e., <u>we are the enemy</u>!! ☺

“**httpnj**” = “**7 19 19 15 13 9**”

Remember, decryption rule: $\alpha = \alpha - k \bmod 26$

But we don’t know k … so we will try all possible values for it

All possible values of k are 0, 1, 2, 3, …, 25

PS: No need to try k = 0, since k = 0 doesn’t hide the message

Method 1: Try all possible keys

"**httpnj**" = "**7 19 19 15 13 9**"

Decryption rule : α = α - k mod 26

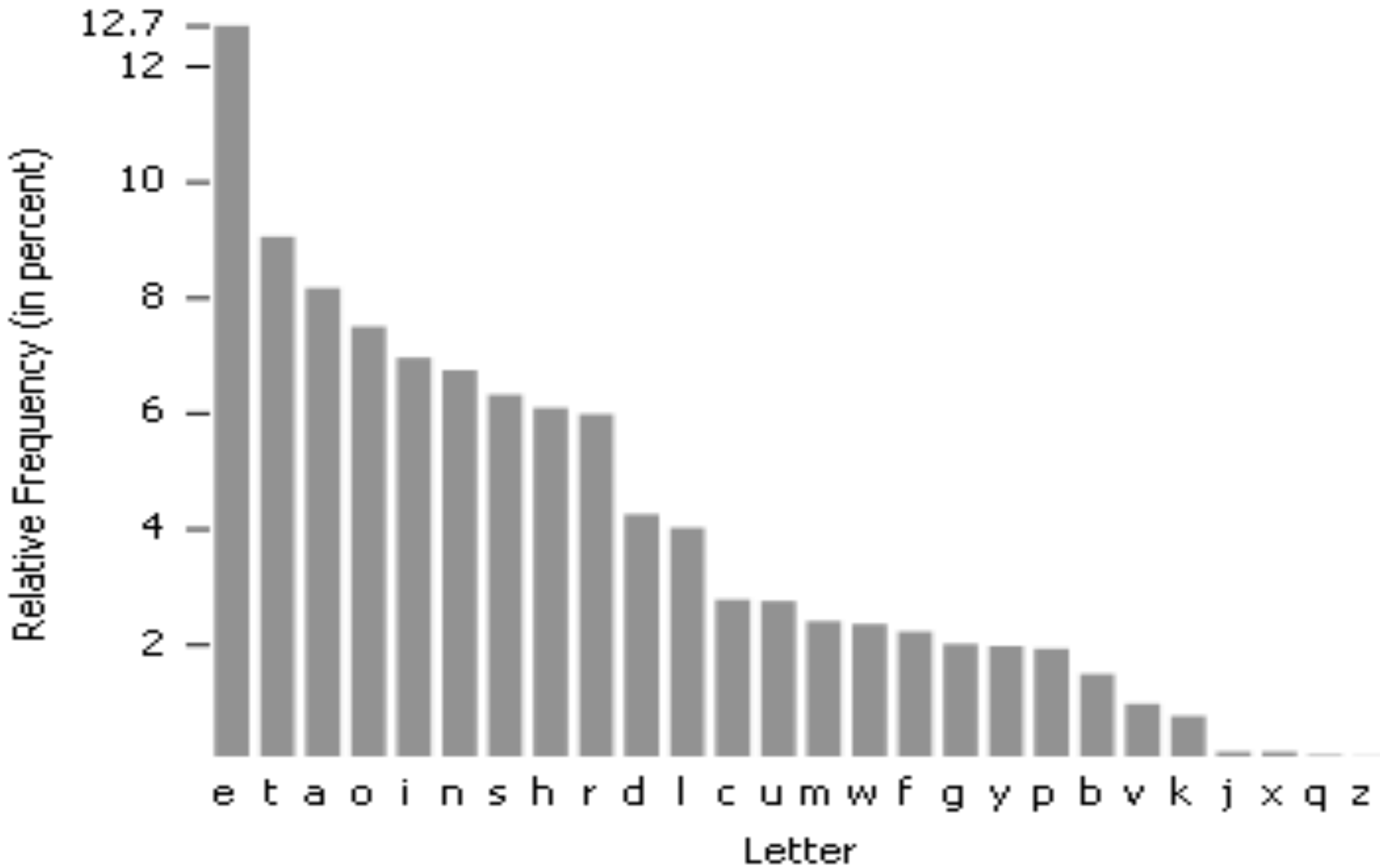
Try k = 1, 2, 3, …, 25

k=1 … "6 18 18 14 12 8" = "gssomi" ??
k=2 … "5 17 17 13 11 7" = "frrnlh" ??
k=3 … "4 16 16 12 10 6" = "eqqmkg" ??
k=4 … "3 15 15 11 9 5" = "dppljf" ??
k=5 … "2 14 14 10 8 4" = "**cookie**" ☺
k=6 … "1 13 13 9 7 3" = "bnnjhd" ??
k=7 … "0 12 12 8 6 2" = "ammigc" ??
k=8 … "25 11 11 7 5 1" = "zllhfb" ??
…

Fortunately, there are only 25 keys … ☺

Method 2: Frequency of Letters

In an arbitrary English text, some letters appear more often than others: letter e appears the most, then letter t, then letter a, … , letter z appears the least



Method 2: Frequency of Letters

Suppose the following encrypted sentence is given
"**tbxqebo fp dobxq ebob**"
and we are trying to find the key

In the encrypted text, the letter "b" appears the most often!!
Very likely "b" is the encryption of "e"

"b" = "e" + k mod 26
1 = 4 + k mod 26

This means k = 23 because 4 + 23 = 27 = 1 mod 26.

Using k = 23 in the above text, we decrypt it at once:
"**tbxqebo fp dnbxq ebnb**" -> "**weather is great here**"

Method 2 is better … we did not have to try all possible keys ☺

Exercises:

9. Break the encryption of "**xurq ue nqmgfurgx**"

10. Break the encryption of "**vhytqoi qhu jxu ruij**"

11. Break the encryption of "**tboub cbscbsb jt b gvo upxo**"

12. Break the encryption of "**cn hypyl luchm ch wufczilhcu**"