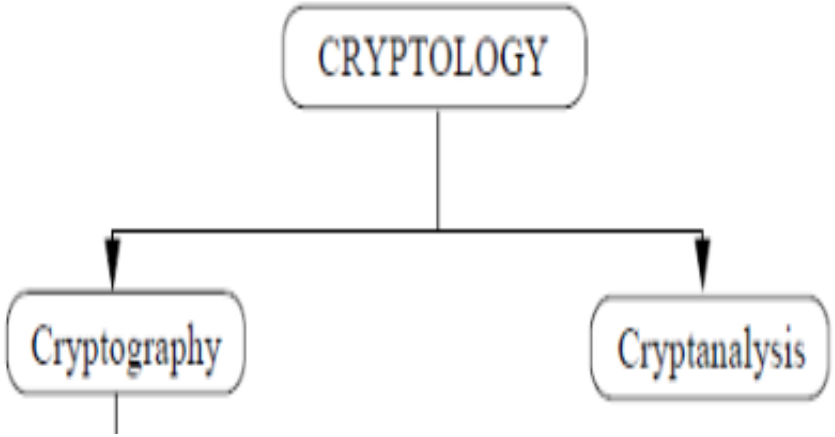
Cryptography

LECTURE-1

Cryptology

Cryptology: the branch of mathematic encompassing both **cryptography** and **cryptanalysis**.



Cryptography and Cryptanalysis

- **Cryptography**: comes from Greek words **kryptos** meaning **hidden or secret** and **graphos** meaning **writing**.
  - **Cryptography** defines as the science and study of secret writing.
  - Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

- **cryptography** is the science of using mathematics to encrypt and decrypt data.

Phil Zimmermann

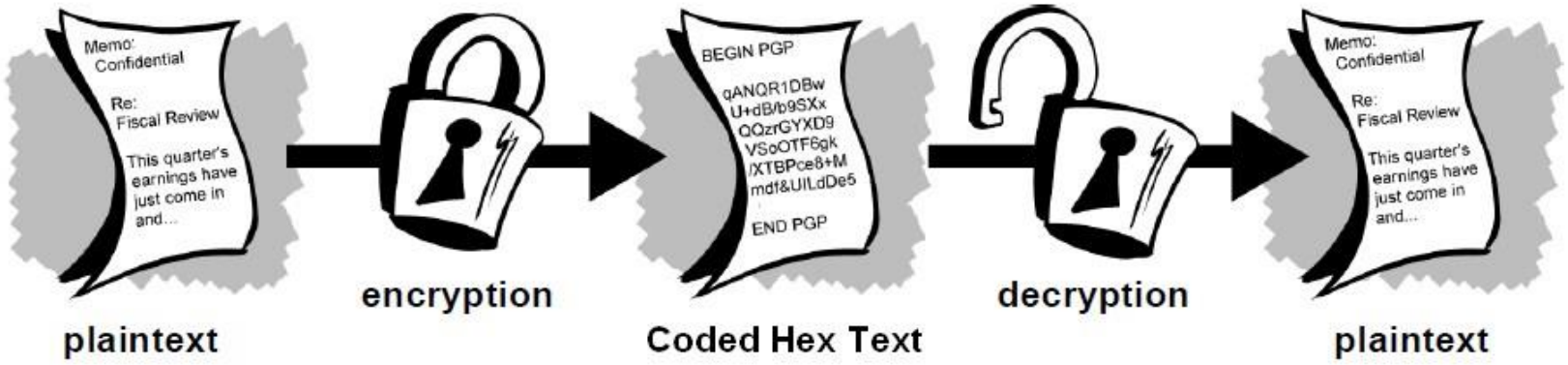
- **Cryptography** is the art and science of keeping messages secure**.**

Bruce Schneier

- **Cryptanalysis:** the science and study of methods of breaking ciphers.

Terminologies

- A message is **plaintext (sometimes called cleartext).**
- The process of disguising a message in such away as to hide its substance is **encryption.**
- An encrypted message is **ciphertext.**
- The process of turning ciphertext back into plaintext is **decryption.**



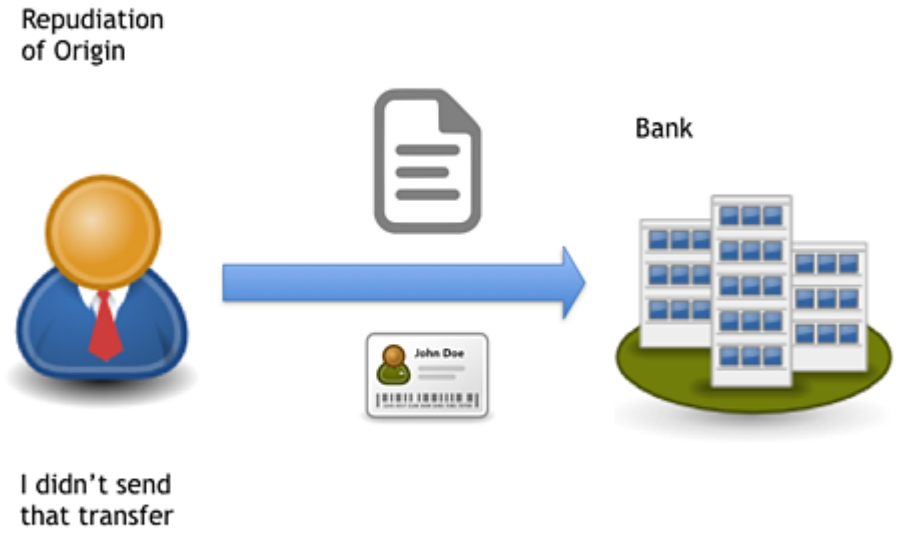
Cryptosystem

- **Cryptosystem**: a method for encoding and decoding messages
- A **cryptosystem** is also referred to as a cipher system
- The various components of a basic cryptosystem are as follows −
  - *Plaintext (P)*
  - *Ciphertext (C)*.
  - *Encryption (E)*
  - *Decryption (D)*
  - *Keys (K):* controller for E and D.

Cryptography Services

Cryptography can be directly used to help ensure these security properties:

- **Confidentiality:** the information cannot be understood by anyone for whom it was unintended
- **Integrity**: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
- **Non-repudiation** : the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
- **Authentication:** verification of identity

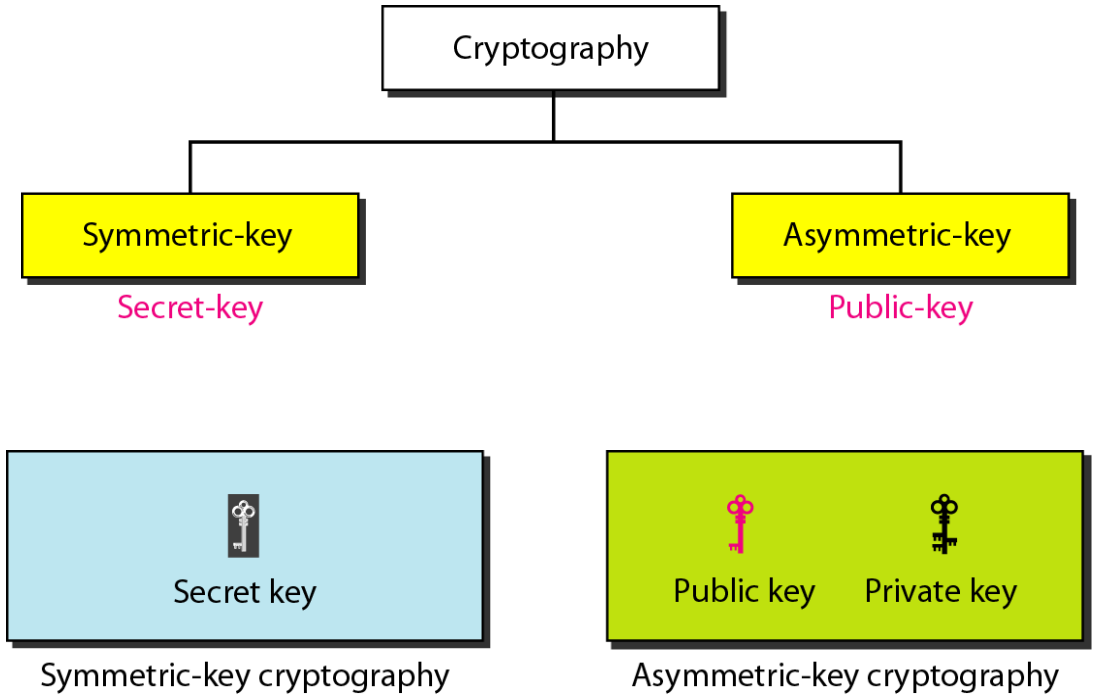

Repudiation
of Origin
Bank
John Doe
I didn't send
that transfer

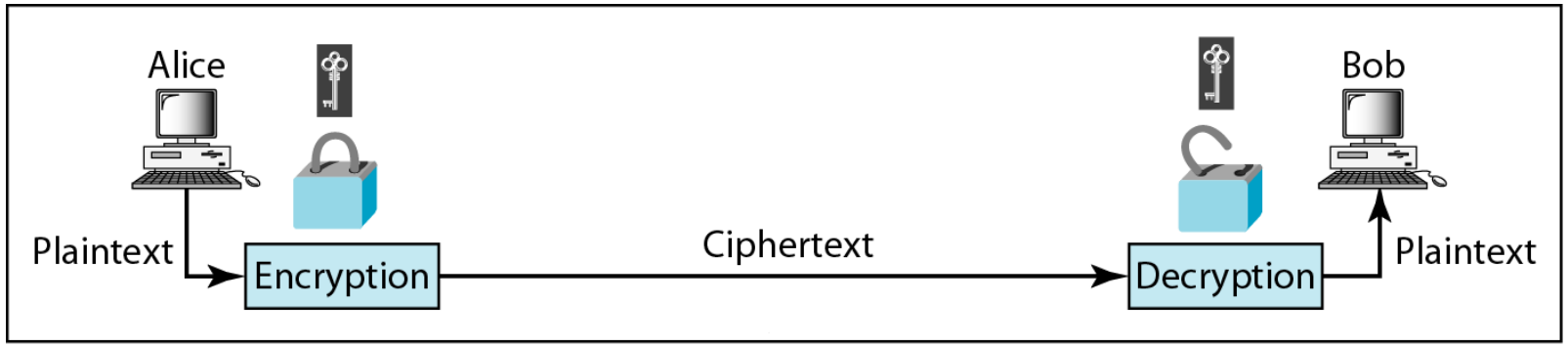
Type of cryptography

The type of cryptography can be classified according to the number of keys used.

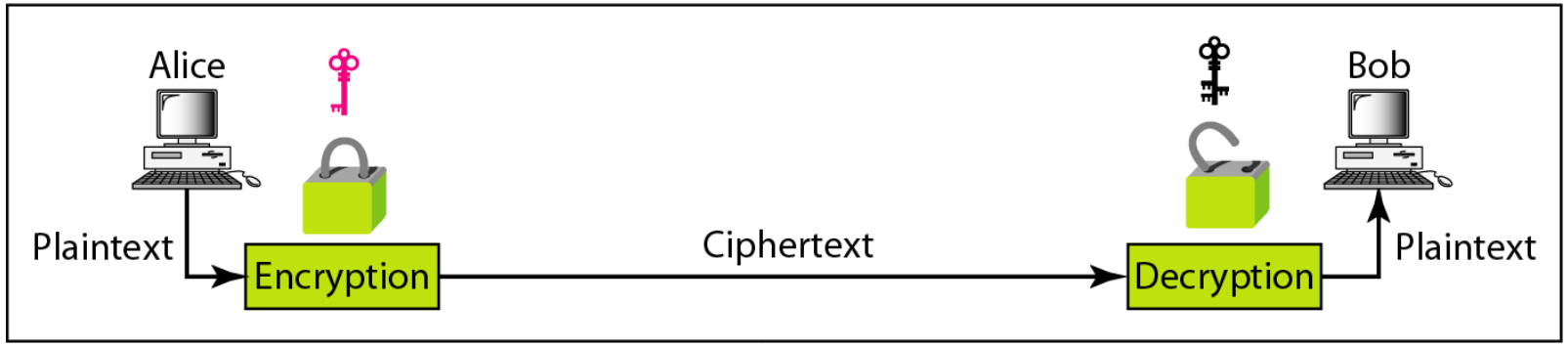
- **Symmetric** or **single-key**: both sender and receiver use the same key.

- **Asymmetric** or **public key :** if both sender and receiver each uses a different key





a. Symmetric-key cryptography



b. Asymmetric-key cryptography

Types of Cryptography

Cryptography can characterize by the type of operations used for transforming plaintext to ciphertext

- **Substitution**
  - involves the replacement of the letters by other letters and symbols to hide the actual meaning of the message.

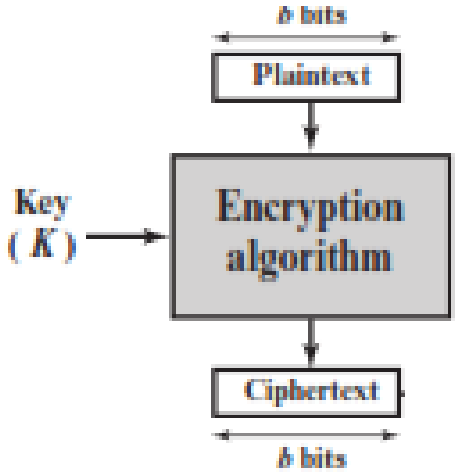
- **Transposition**
  - the plaintext characters of a message are systematically rearranged.
  - After transposing a message, the same characters are still present, but the order of the letters is changed.

- **Product**
  - involve multiple stages of substitutions and transpositions.

Types of Cryptography

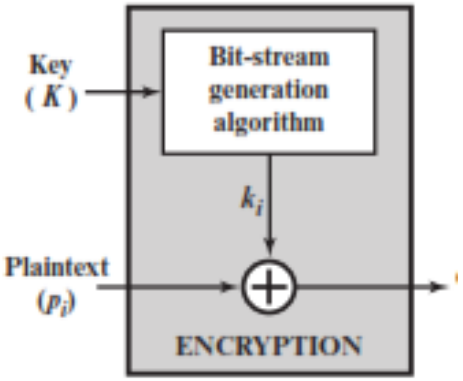
Block

- processes the input one block of elements at a time, producing an output block for each input block.



Stream

- processes the input elements continuously, producing output one element at a time, as it goes along.



Modular Arithmetic

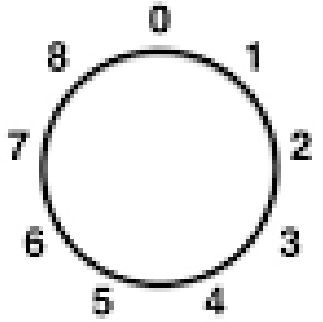
- If *a is an integer and n is a positive integer, we define a mod n to be the remainder* when *a is divided by n. The integer n is called the* ***modulus.***
- Note that, the (mod *n) operator maps all integers into* the set of integers {0, 1, … , (*n - 1)}.*

$$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$$

Example

Modulus 9

0 mod 9 = 0	9 mod 9 = 0
1 mod 9 = 1	10 mod 9 = 1
2 mod 9 = 2	11 mod 9 = 2
3 mod 9 = 3	12 mod 9 = 3
4 mod 9 = 4	13 mod 9 = 4
5 mod 9 = 5	14 mod 9 = 5
6 mod 9 = 6	15 mod 9 = 6
7 mod 9 = 7	16 mod 9 = 7
8 mod 9 = 8	17 mod 9 = 8



Example:

- Addition, multiplication and subtraction mod 5

$a+b$	$a=0$	1	2	3	4
$b=0$	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a-b$	$a=0$	1	2	3	4
$b=0$	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$a \times b$	$a=0$	1	2	3	4
$b=0$	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

For example, we have $3 \times 4 = 2$ because the remainder when we divide 3×4 by 5 is 2.

Congruent modulo

Two integers *a and b are said to be* ***congruent modulo n, if (a mod n) = (b mod n)****. This is written as* $a \equiv b \pmod{n}$

For instance, 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12. We write this as 1 = 13 = 25 = 37 mod 12.

Example

$12 \equiv 2 \pmod{10}$	12 mod 10 = 2
$107 \equiv 207 \pmod{10}$	207 mod 10 = 7
$7 \equiv 3 \pmod{2}$	7 mod 2 = 1
$7 \equiv -1 \pmod{2}$	-1 mod 2 = 1
$13 \equiv -1 \pmod{7}$	-1 mod 7 = 6
$-15 \equiv 10 \pmod{5}$	-15 mod 5 = 0

Classical Encryption: Substitution

- Monoalphabetic substitution cipher
- Homophonic substitution cipher
- Polyalphabetic substitution cipher
- Polygraphic substitution cipher

Monoalphabetic Substitution Ciphers

- A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext.

Additive Cipher

- The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher
- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.
- The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing **three places** further down the alphabet.

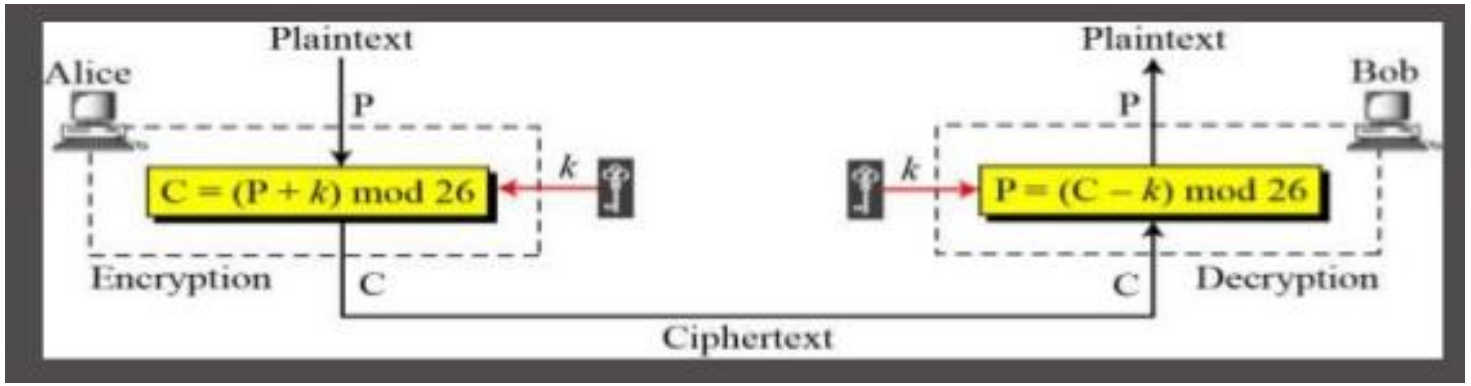
Example

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

Example: Encryption with k=3
Plaintext: hello
Ciphertext: KHOOR

Decryption with k=3
ciphertext: KHOOR
plaintext: hello

Additive cipher



Additive Cipher: How to encrypt

- Thus to cipher a given text we need an integer value, known as shift **(key)** which indicates the number of position each letter of the text has been moved down.
- Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number P. (a=0, b=1, c=2, ..., y=24, z=25)

- Calculate:

$$C = E(P, K) = (P + K) \; mod \; n$$, where n is the size of the alphabet.

- Convert the number **C** into a letter that matches its order in the alphabet.

Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Additive Cipher: How to decrypt

For every letter in the ciphertext:

- Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number C

  $P = D\ (C, K)\ =\ (C - K)\ mod\ n$, where n is the size of the alphabet

- Convert the number **P** into a letter that matches its order in the alphabet starting from 0. (a=0, b=1, c=2, ..., y=24, z=25)

Example

ENCRYPTION

Encrypt the plaintext ” **hello**” using additive cipher with k=4

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

Ciphertext: LIPPS

Or

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

$C = E(h, 4) = (7 + 4) \bmod 26 = 11 = L$

$C = E(e, 4) = (4 + 4) \bmod 26 = 8 = I$

$C = E(l, 4) = (11 + 4) \bmod 26 = 15 = P$

$C = E(l, 4) = (11 + 4) \bmod 26 = 15 = P$

$C = E(o, 4) = (14 + 4) \bmod 26 = 18 = S$

Ciphertext: LIPPS

DECRYPTION

Decrypt the ciphertext” LIPPS” using additive cipher with k=4

plaintext: hello

Or

$P = D(C, K) = (C - K) \bmod 26$

$P = D(L, 4) = (11 - 4) \bmod 26 = 7 = h$

$P = D(I, 4) = (8 - 4) \bmod 26 = 4 = e$

$P = D(P, 4) = (15 - 4) \bmod 26 = 11 = l$

$P = D(P, 4) = (15 - 4) \bmod 26 = 11 = l$

$P = D(S, 4) = (18 - 4) \bmod 26 = 14 = o$

plaintext: hello

Example

ENCRYPTION

Use the additive cipher with key = 15 to encrypt the plaintext “hello”.

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

DECRYPTION

Use the additive cipher with key = 15 to decrypt the cihertext“WTAAD”.

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Is the shift (additive)cipher secure?

- If it is known that a given ciphertext is a Caesar cipher, then a **brute-force cryptanalysis** is easily performed: simply try all the 25 possible keys.
- A **brute-force attack** involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld 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 julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm 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 bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Brute-Force attack of Caesar Cipher