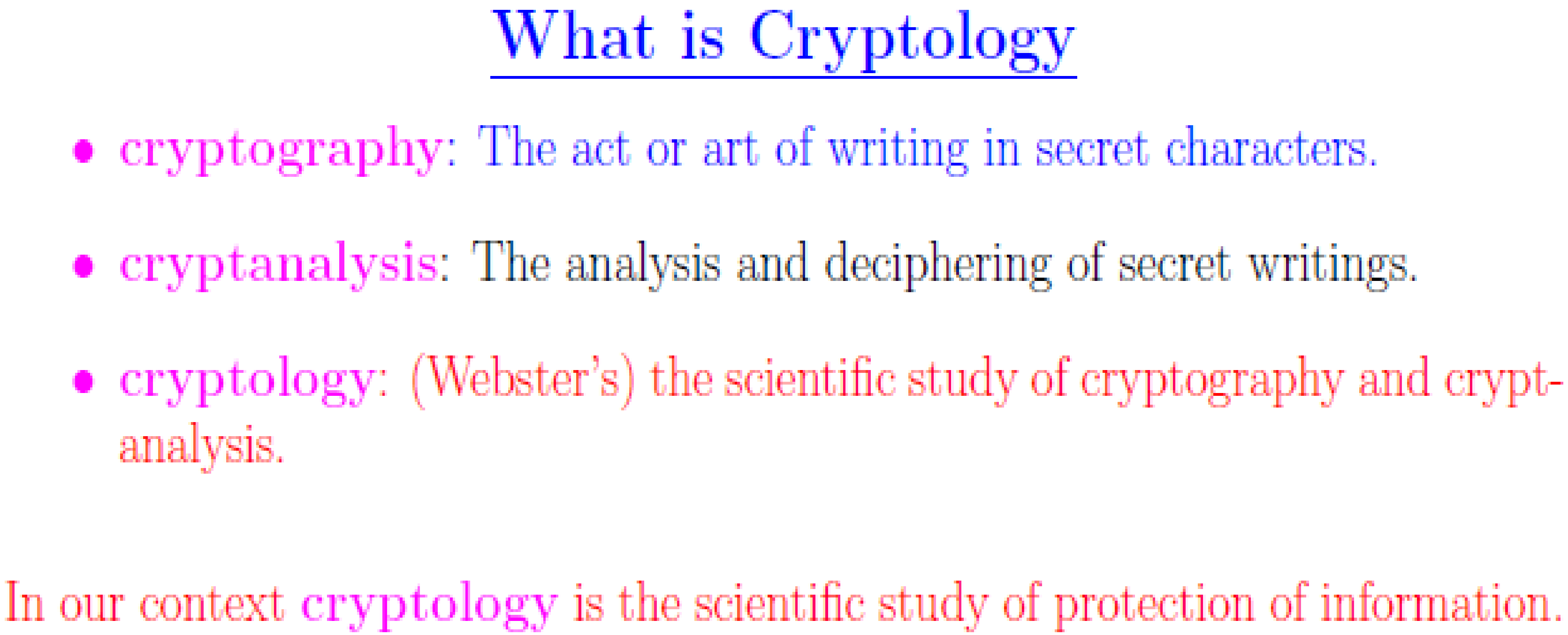
Introduction



What is Cryptology

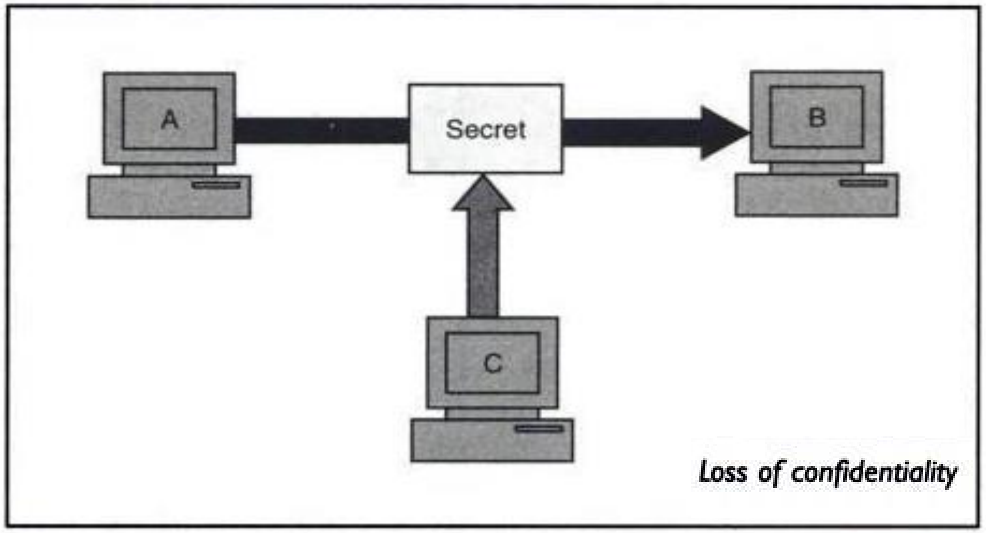
- cryptography: The act or art of writing in secret characters.
- cryptanalysis: The analysis and deciphering of secret writings.
- cryptology: (Webster's) the scientific study of cryptography and cryptanalysis.

In our context cryptology is the scientific study of protection of information.

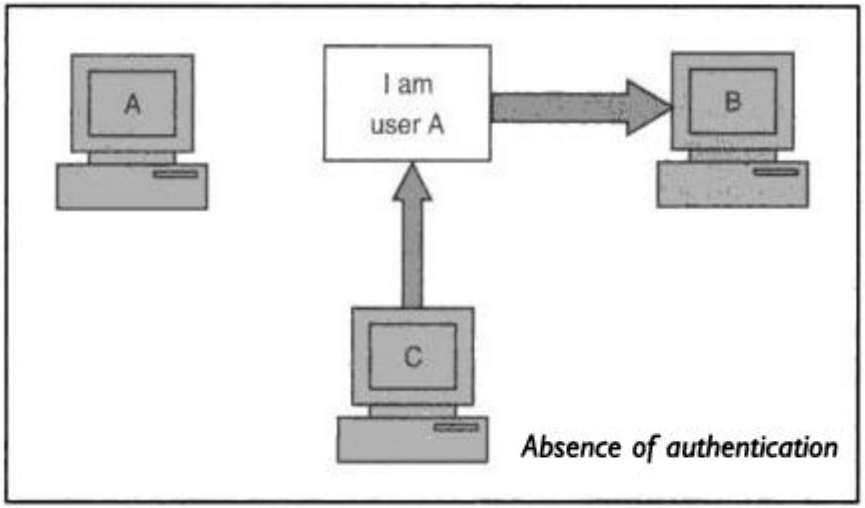
Applications

- Secure Communications (war-time)
- File and data base security
- Electronic funds transfer
- Electronic commerce
- Digital cash
- Contract signing
- Electronic mail
- Electronic voting
- Authentication: Passwords, PINs
- Secure identification, Access control
- Secure protocols

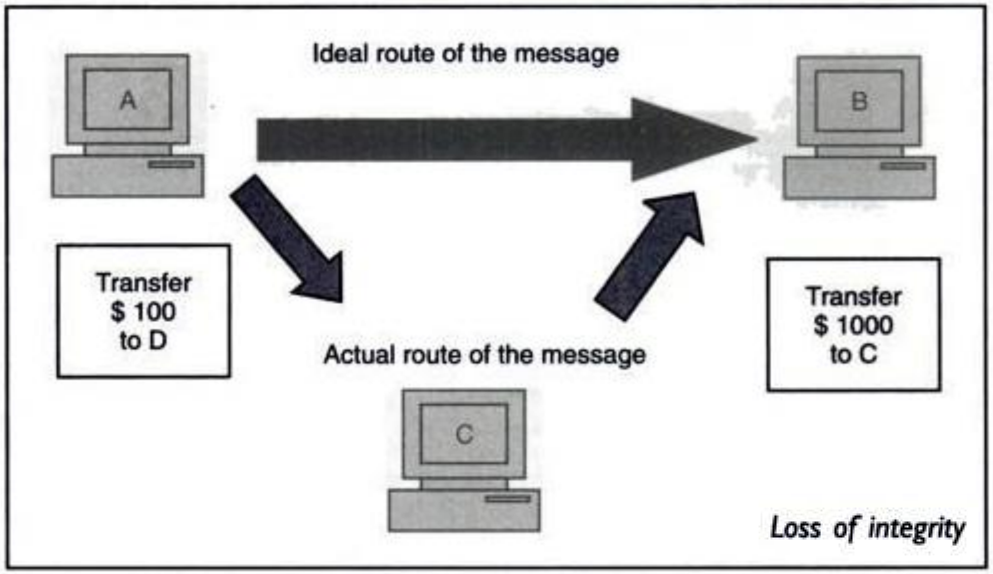
Principles of Security



Loss of confidentiality



Absence of authentication

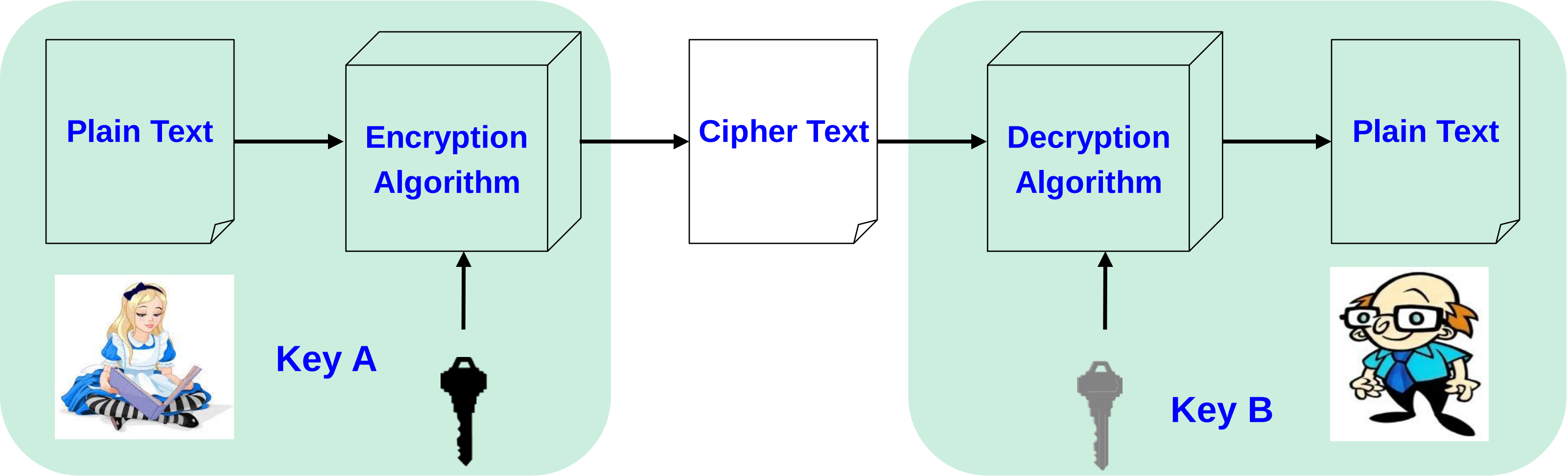


Loss of integrity

Principles of Security

- Secrecy/Confidentiality
  - Only intended receiver understands the message
- Authentication
  - Sender and receiver need to confirm each others identity
- Message Integrity
  - Ensure that their communication has not been altered, either maliciously or by accident during transmission
- Nonrepudiation
  - Sender should not be able to falsely deny that a message was sent
- Availability (System)
  - Ensure that the information concerned is readily accessible to the authorized viewer at all times

Cryptography components: Cipher

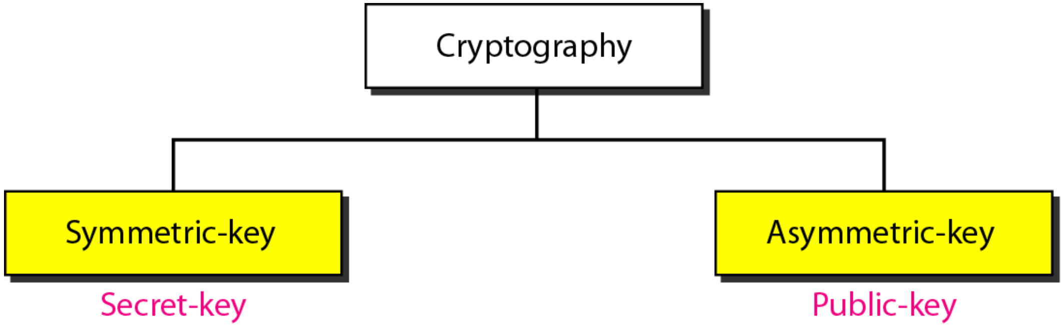


- Cipher is a method for encrypting messages
- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher -** algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Categories of cryptography



Cryptography

Symmetric-key

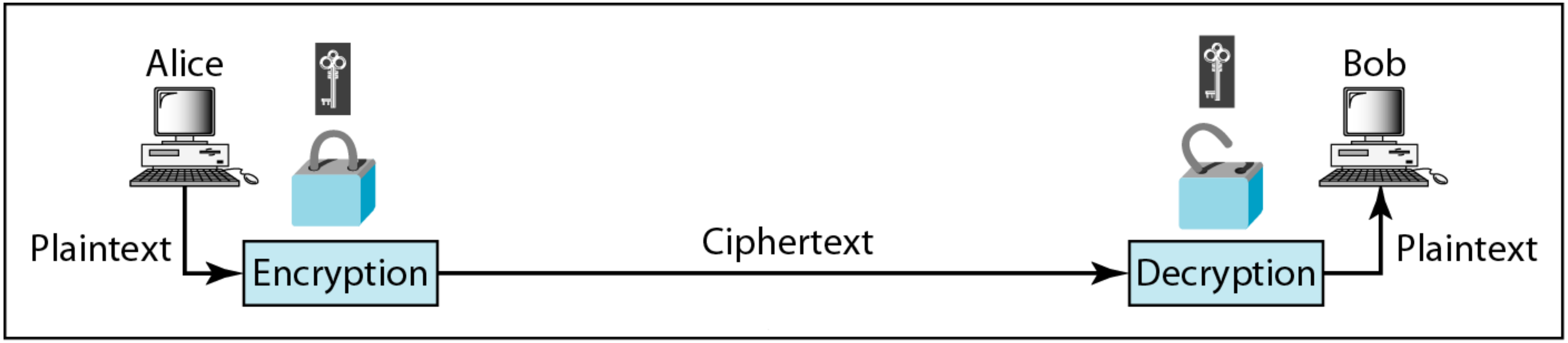
Secret-key

Asymmetric-key

Public-key

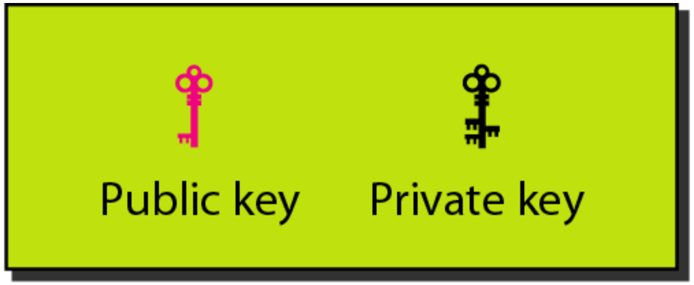
Symmetric-key cryptography

Symmetric-key cryptography

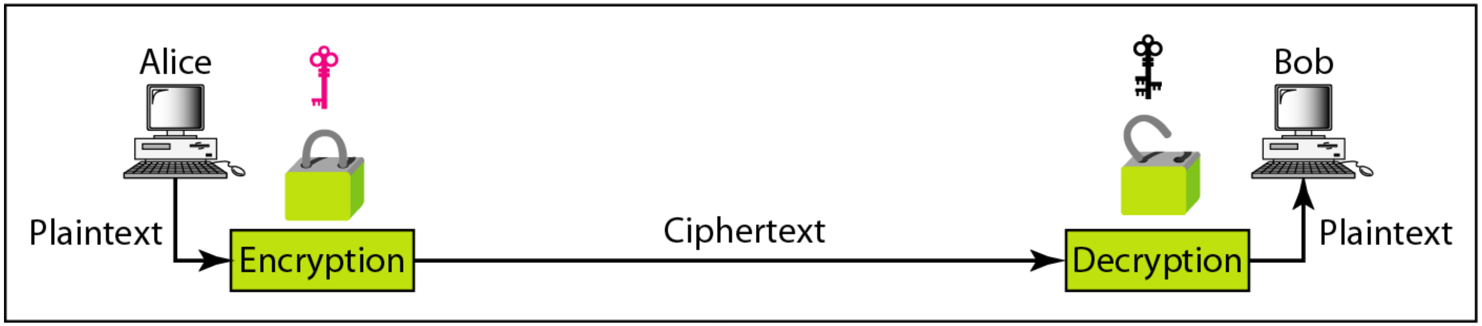


a. Symmetric-key cryptography

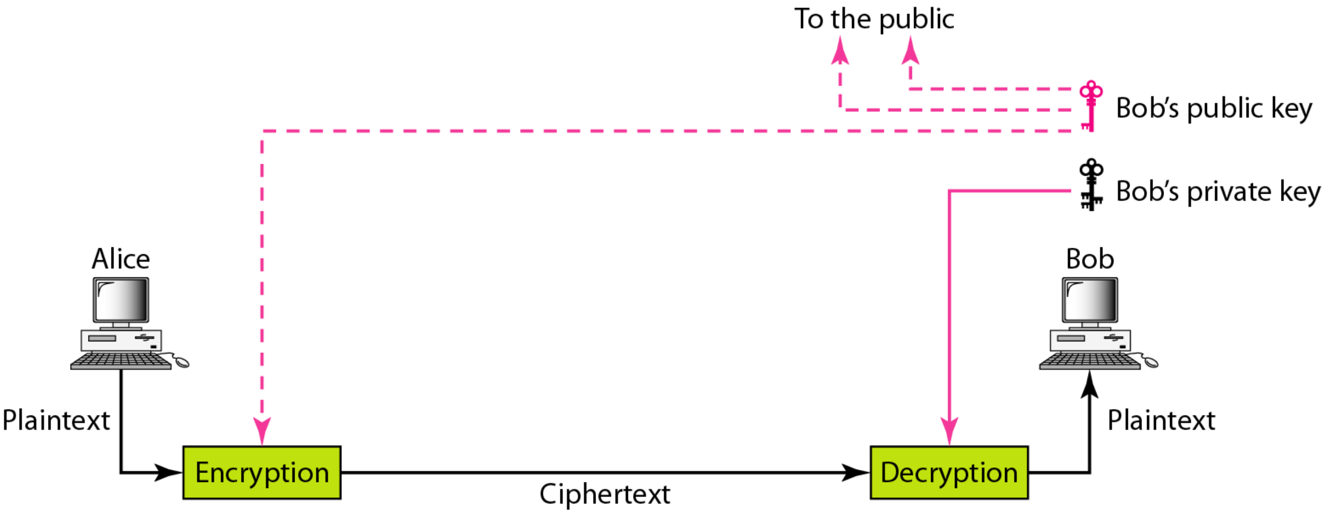
Asymmetric-key cryptography



Asymmetric-key cryptography

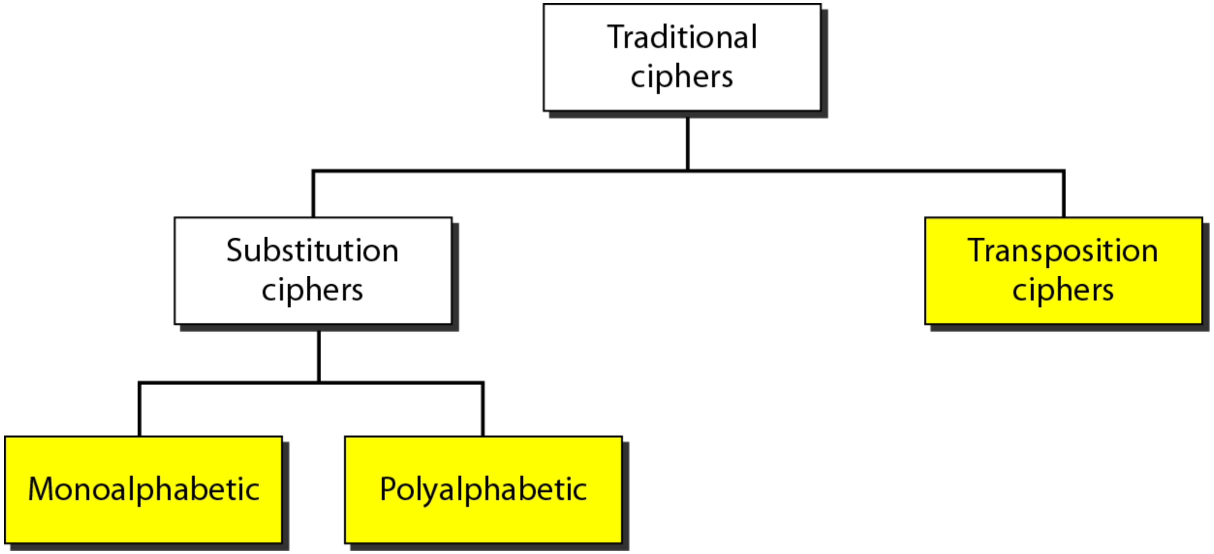


b. Asymmetric-key cryptography



Symmetric Key Cryptography: Traditional Ciphers

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war).



Cæsar cipher

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
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

Cæsar cipher

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
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

→ *shift alphabet by n (6)*

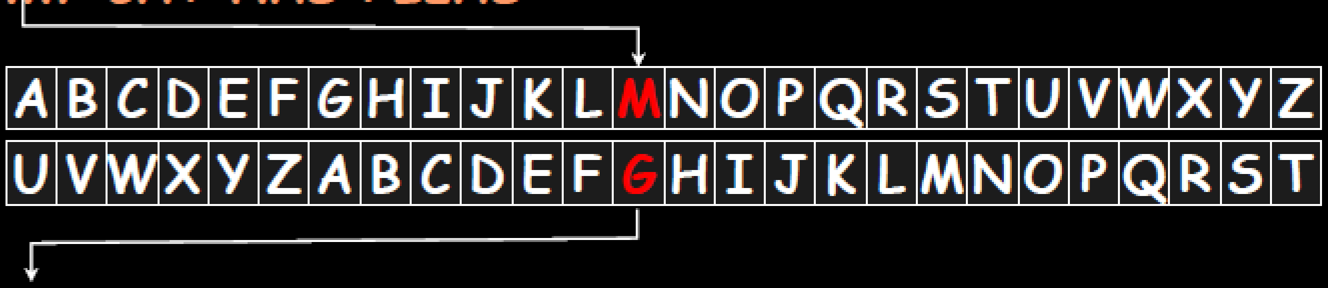
Cæsar cipher

MY CAT HAS FLEAS

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
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

Cæsar cipher

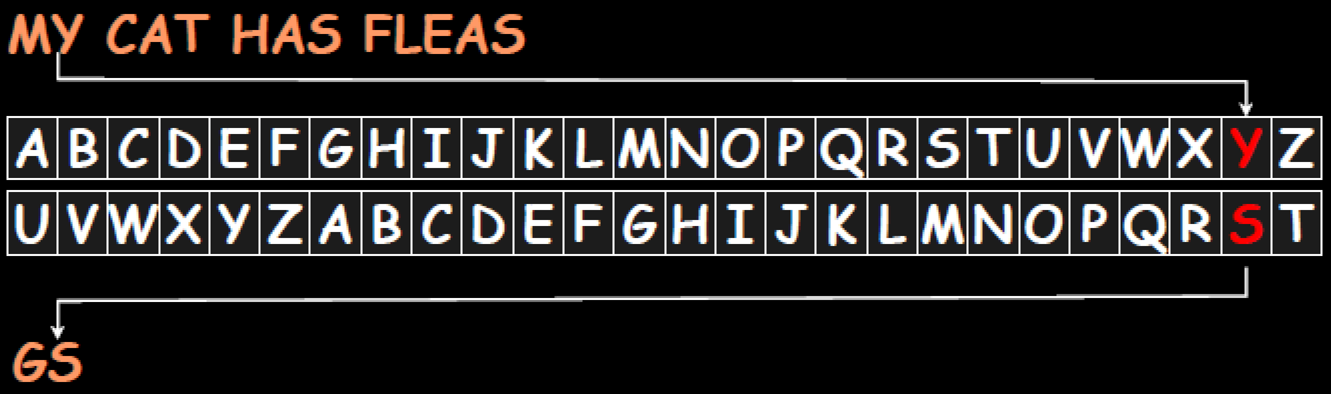
MY CAT HAS FLEAS



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
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

G

Cæsar cipher

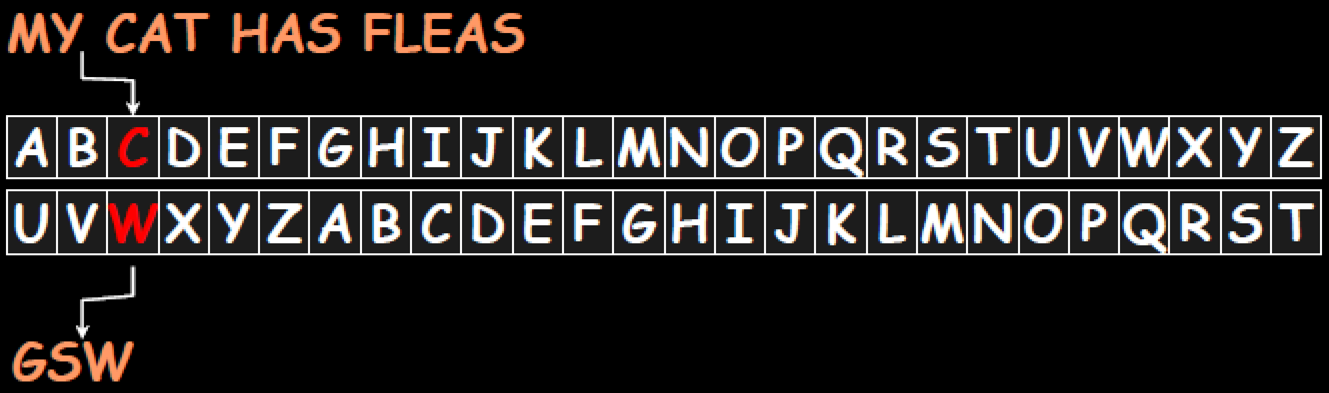


MY CAT HAS FLEAS

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
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

GS

Cæsar cipher

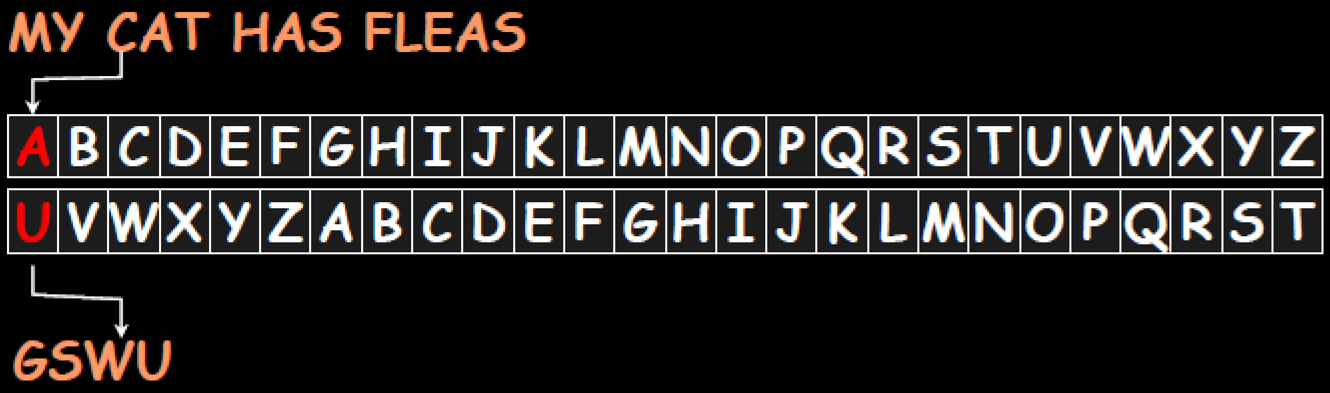


MY CAT HAS FLEAS

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
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

GSW

Cæsar cipher



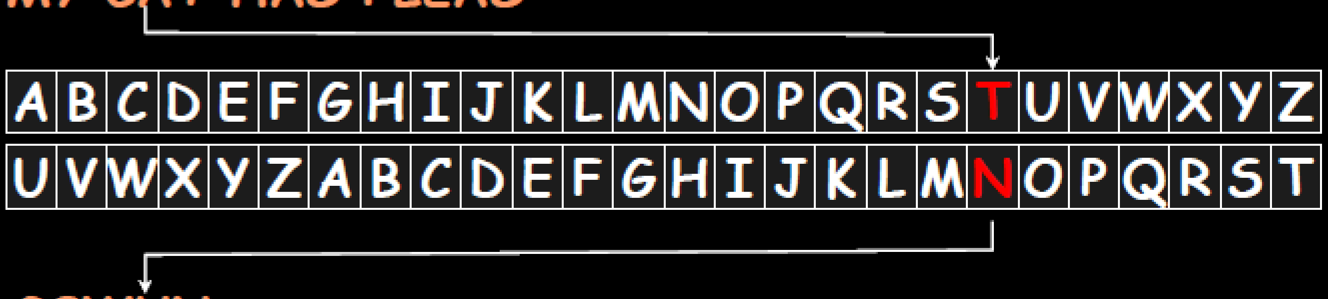
MY CAT HAS FLEAS

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
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

GSWU

Cæsar cipher

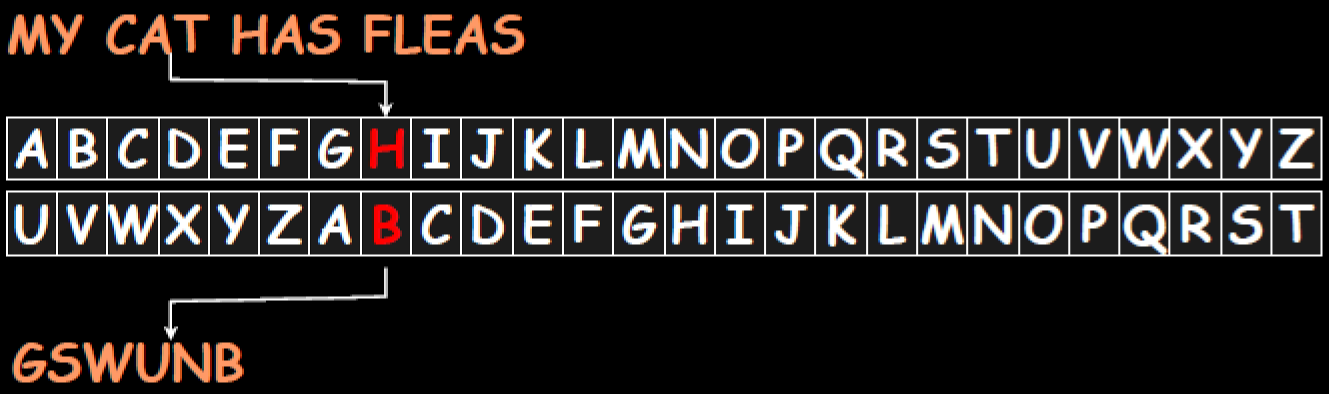
MY CAT HAS FLEAS



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
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

GSWUN

Cæsar cipher

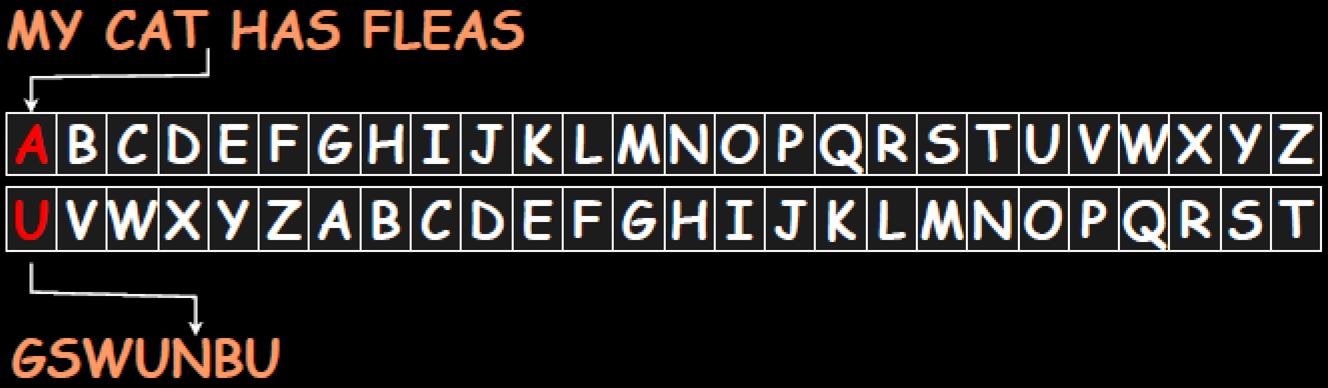


MY CAT HAS FLEAS

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
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

GSWUNB

Cæsar cipher



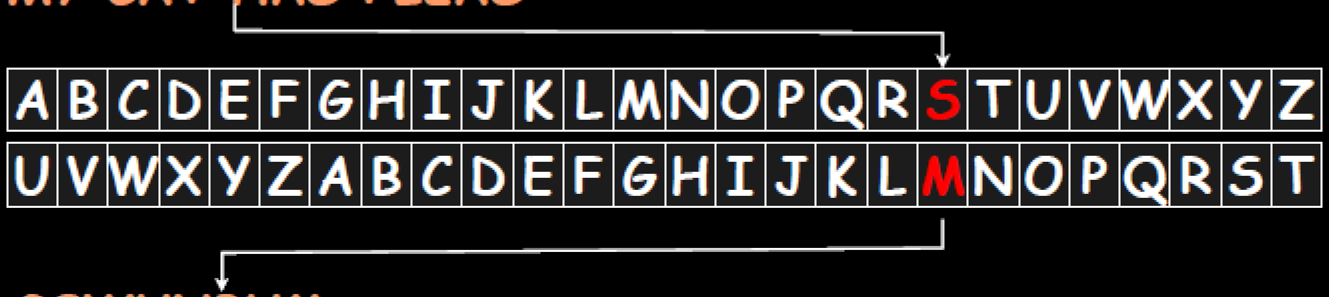
MY CAT HAS FLEAS

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
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

GSWUNBU

Cæsar cipher

MY CAT HAS FLEAS

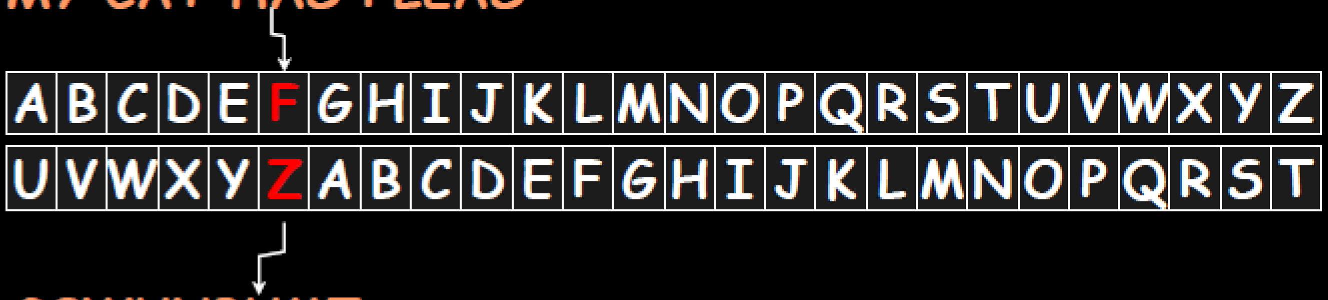


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

GSWUNBUM

Cæsar cipher

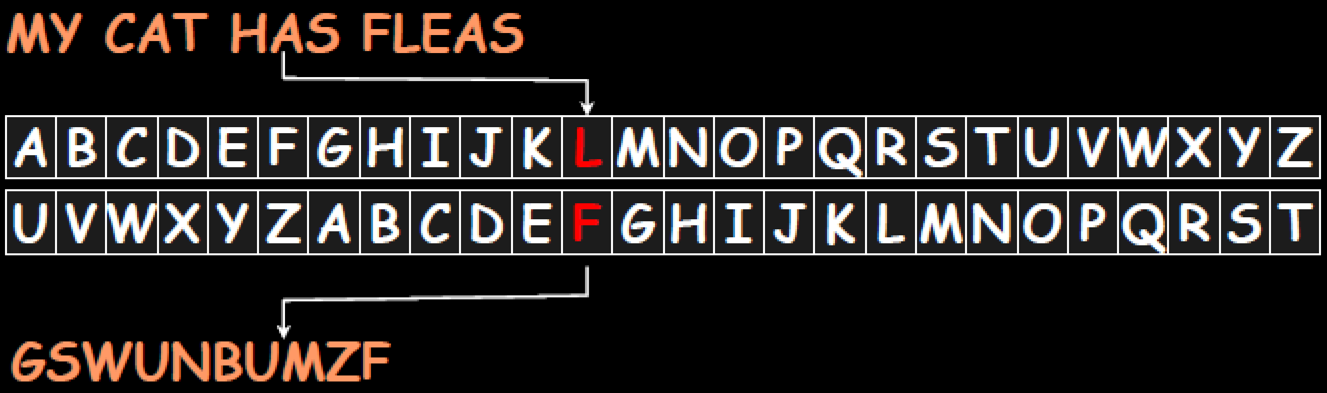
MY CAT HAS FLEAS



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
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

GSWUNBUMZ

Cæsar cipher

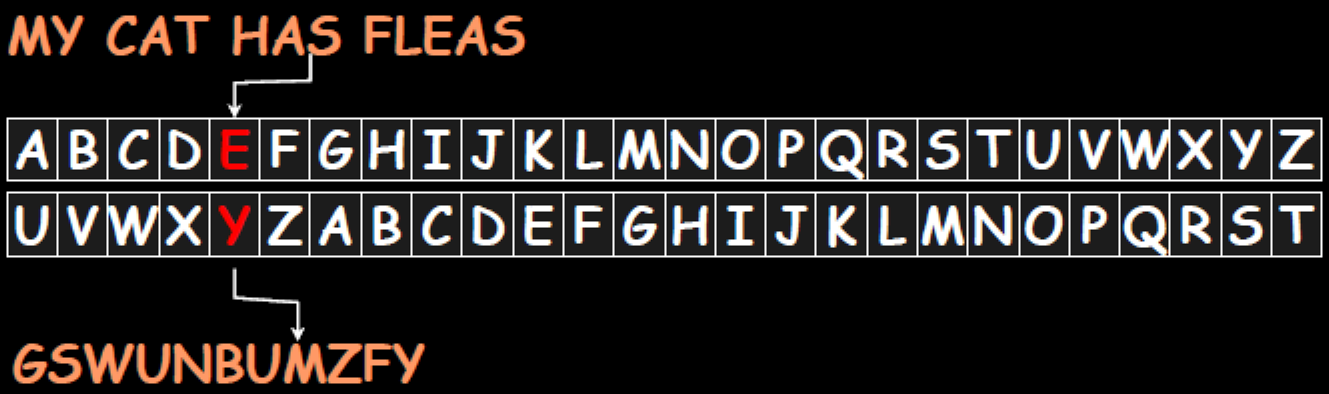


MY CAT HAS FLEAS

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
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

GSWUNBUMZF

Cæsar cipher

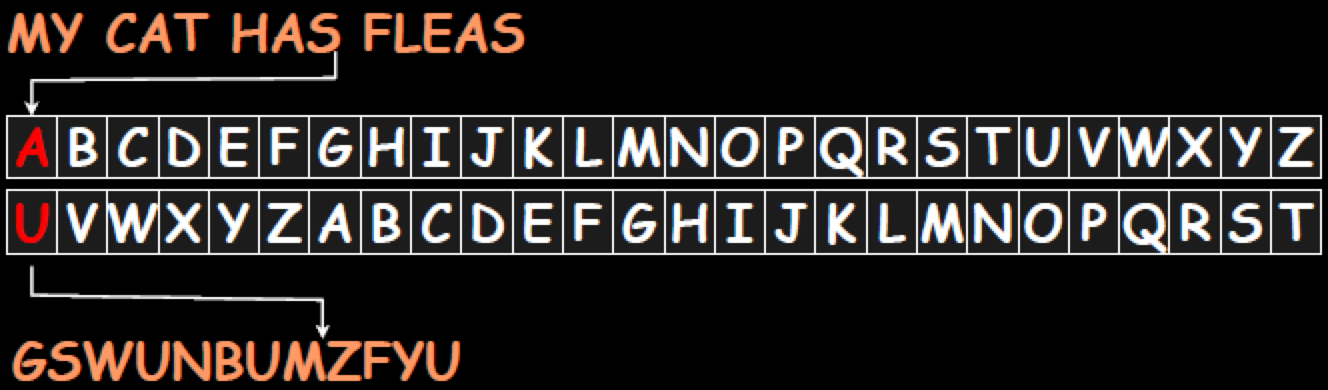


MY CAT HAS FLEAS

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
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

GSWUNBUMZFY

Cæsar cipher

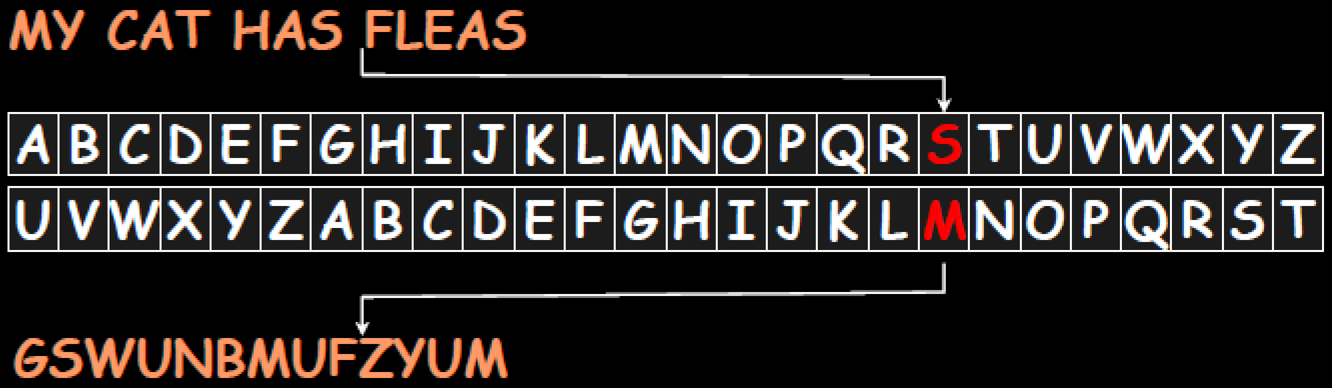


MY CAT HAS FLEAS

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
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

GSWUNBUMZFYU

Cæsar cipher

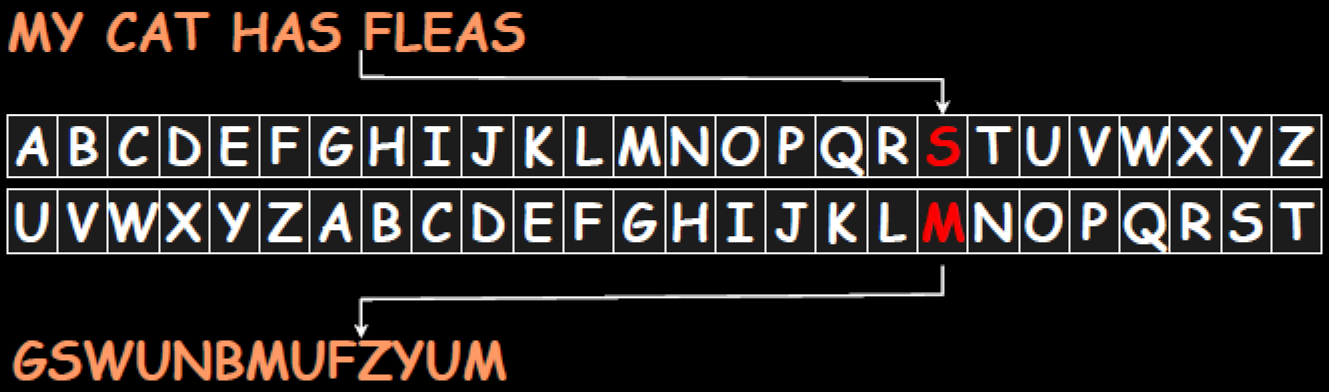


MY CAT HAS FLEAS

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
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

GSWUNBMUFZYUM

Cæsar cipher



MY CAT HAS FLEAS

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
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

GSWUNBMUFZYUM

- Convey one piece of information for decryption: *shift value*

- trivially easy to crack (26 possibilities for a 26 character alphabet)

Transposition Cipher: Columnar Transposition

- This involves rearrangement of characters on the plain text into columns
- If the letters are not exact multiples of the transposition size, padding with an infrequent letter such as x or z.

THIS IS A MESSAGE TO SHOW HOW A COLUMNER TRANSPOSITION WORKS

Plain Text

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

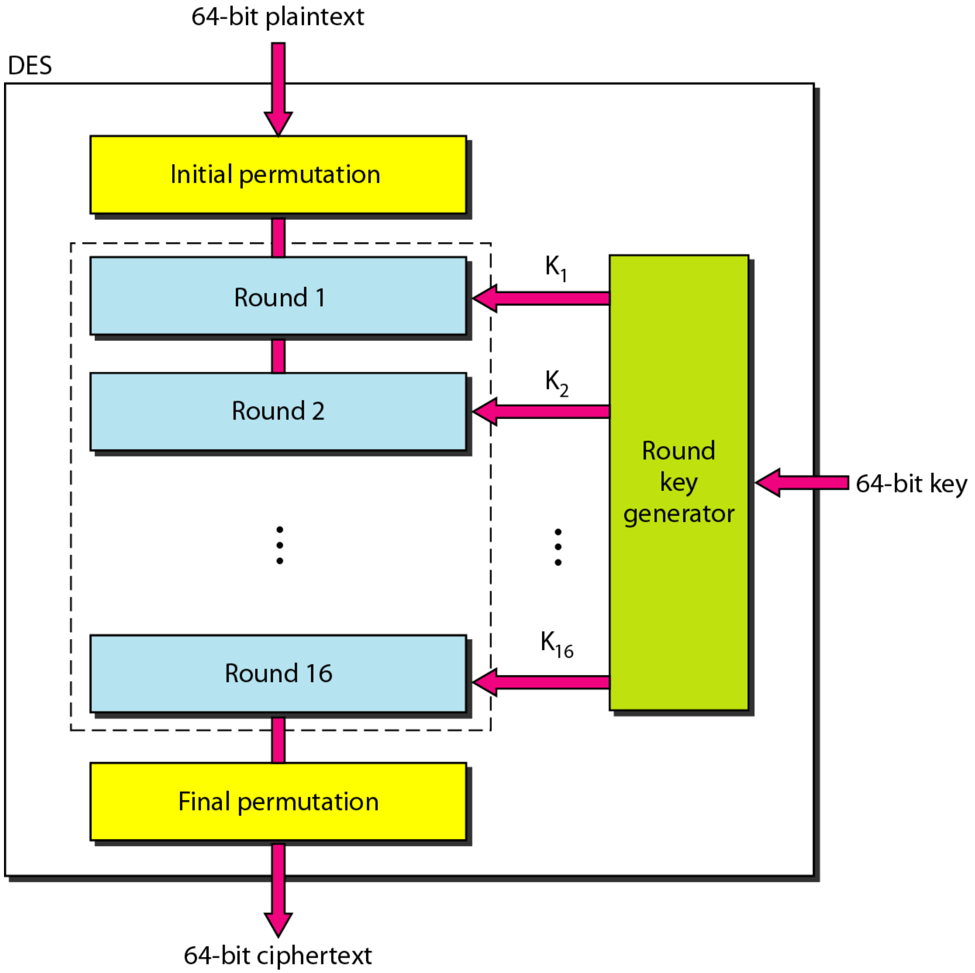
Cipher Text

T	S	S	O	H
O	A	N	I	W
H	A	A	S	O
L	R	S	T	O
I	M	G	H	W
U	T	P	I	R
S	E	E	O	A
M	R	O	O	K
I	S	T	W	C
N	A	S	N	S

Block vs Stream Ciphers

- Stream ciphers process messages a bit or byte at a time when en/decrypting.
- Block ciphers process messages in into blocks, each of which is then en/decrypted.
    - Like a substitution on very big characters: 64-bits or more
- Many current ciphers are block ciphers, one of the most widely used types of cryptographic algorithms

DES (Data Encryption Standard)



Strength of DES – Key Size

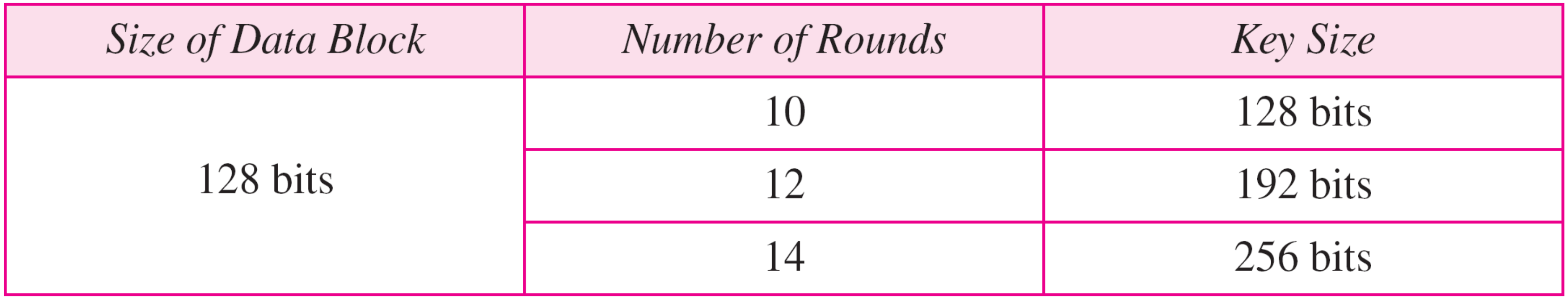
- 64-bit keys have 2^{64} values
- Brute force search looks hard
- Recent advances have shown is possible
  - in 1997 on a huge cluster of computers over the Internet in a few months
  - in 1998 on dedicated hardware called "DES cracker" by Electronic Frontier Foundation (EFF) in a few days ($220,000)
  - in 1999 above combined in 22hrs!

AES (Advanced Data Encryption Standard)

- Advanced Encryption Standards (AES)
  - – US NIST issued call for ciphers in 1997
  - – Rijndael was selected as the AES in Oct-2000
- Private key symmetric block cipher
- Stronger & faster than Triple-DES
- In AES, all operations are performed on 8-bit bytes. In particular, the arithmetic operations of addition, multiplication, and division are performed over the finite field GF(2^8).

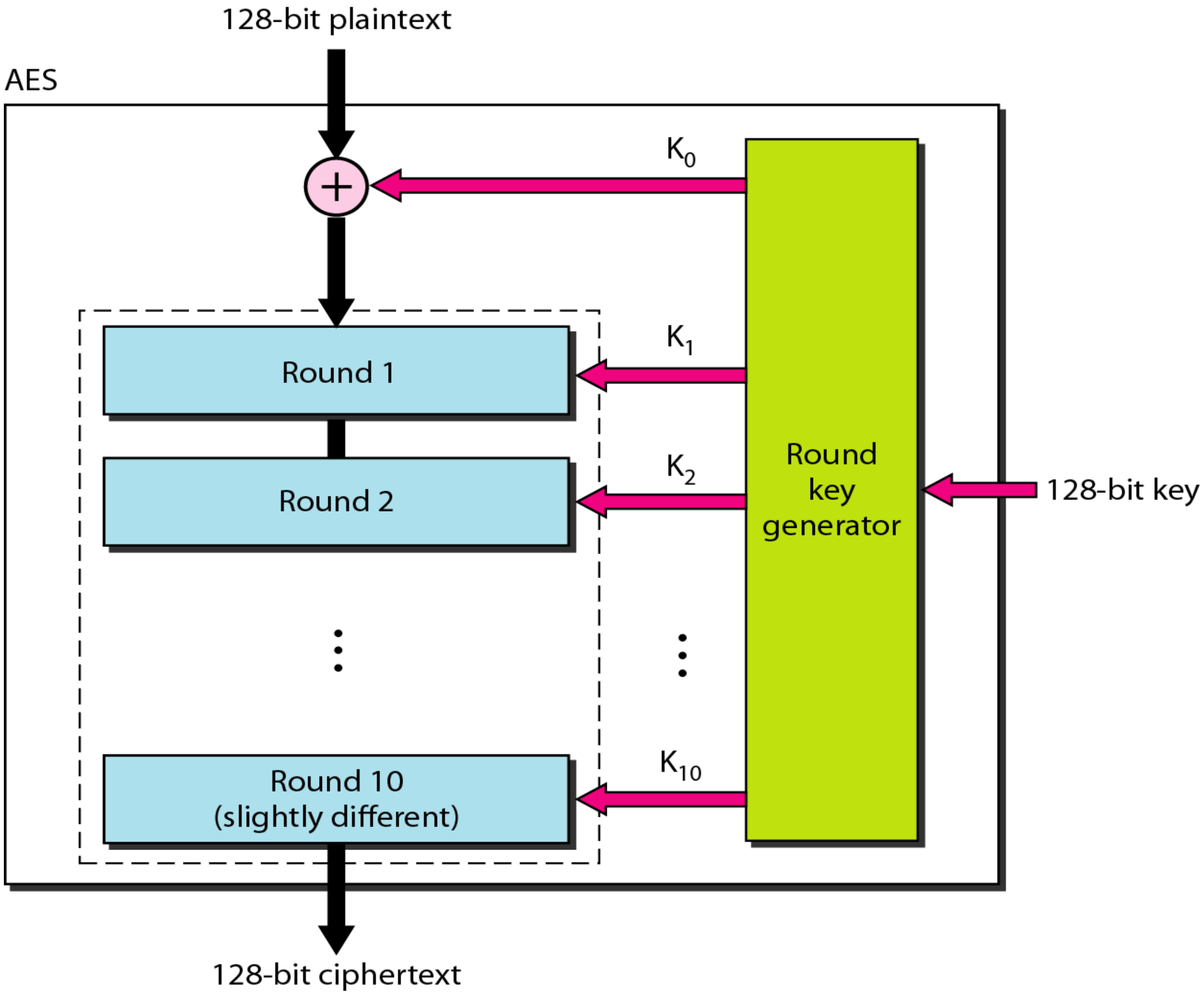
AES (Advanced Data Encryption Standard)

AES has three different configurations with respect to the number of rounds and key size.



Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

AES (Advanced Data Encryption Standard)



Substitution-Permutation Ciphers

- Substitution-permutation (S-P) networks [Shannon, 1949]
  - modern substitution-transposition product cipher
- S-P networks are based on the two primitive cryptographic operations
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message
- These form the basis of modern block ciphers

Confusion and Diffusion

- Cipher needs to completely obscure statistical properties of original message
- A one-time pad does this
- More practically Shannon suggested S-P networks to obtain:
- **Diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- **Confusion** – makes relationship between ciphertext and key as complex as possible