Classical Cryptography

Dr. Mana Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
Email: manaskhatua@iitg.ac.in

Classical Cryptography

Classical Cryptography:

"Classical Cryptography was confined to the art of designing and breaking encryption schemes (or secrecy codes)"

Modern Cryptography:

"Modern Cryptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it."

It emphasizes two aspects of the transition from classical to modern cryptography:

1) the widening of scope from one specific task to an utmost wide general class of tasks
2) the move from an engineering-art which strives on ad-hoc tricks to a scientific discipline based on rigorous approaches and techniques.

Ref: Oded Goldreich. Modern Cryptography, Probabilistic Proofs and Pseudorandomness. 1st Ed. 1999. Springer.

Definitions

Plaintext

- An original message

Ciphertext

- The coded message

Enciphering /encryption

- The process of converting from plaintext to ciphertext

Deciphering/decryption

- Restoring the plaintext from the ciphertext

Cryptography

- The area of study of the many schemes used for encryption

Cryptographic system /cipher

- A scheme

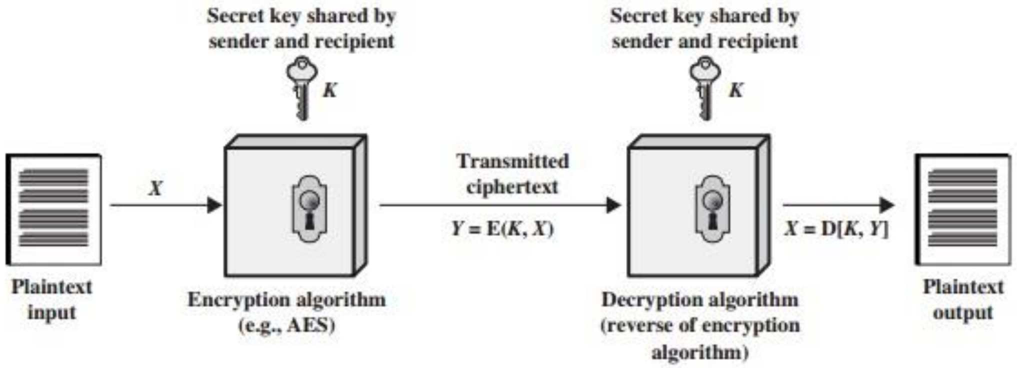
Cryptanalysis

- Techniques used for deciphering a message without any knowledge of the enciphering details

Cryptology

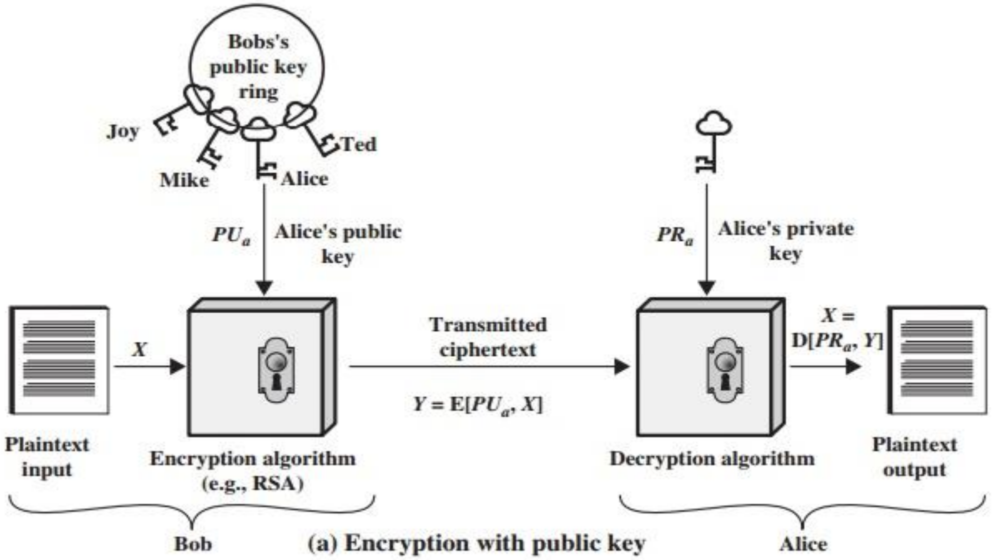
- The areas of cryptography and cryptanalysis

Encryption Models



Symmetric Encryption Model

Asymmetric Encryption Model



Cryptographic Systems

✓Cryptographic Systems are characterized along three independent dimensions:

Type of operations used for transforming plaintext to ciphertext	Number of keys used	The way in which the plaintext is processed
Substitution	Symmetric, single-key, secret-key, conventional encryption	Block cipher
Transposition	Asymmetric, two-key, or public-key encryption	Stream cipher

Caesar Cipher Used by Julius Caesar

- replacing each letter of the alphabet with the letter standing three places further down the alphabet

plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Rail Fence Cipher

- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows

plain: meet me after the toga party
write: m e m a t r h t g p r y
e t e f e t e o a a t
cipher: MEMATRHTGPRYETEFETEOAAT

Cryptanalysis and Brute-Force Attack

Two general approaches to attacking a conventional encryption scheme:

Cryptanalysis

- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

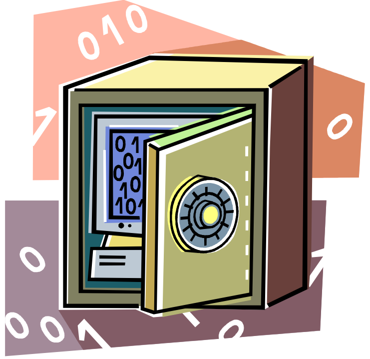
Brute-force attack

- Attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Encryption Scheme Security

Unconditionally secure

No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there



Computationally secure

The cost of breaking the cipher exceeds the value of the encrypted information

The time required to break the cipher exceeds the useful lifetime of the information

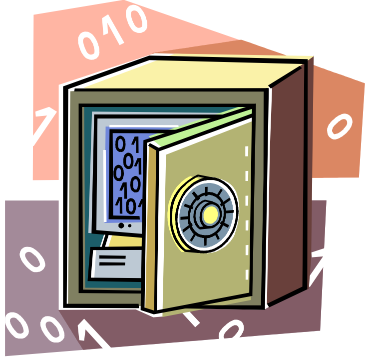
Caesar Cipher Algorithm

Can define transformation as:

```
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
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
```

Mathematically give each letter a number

```
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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
```



Algorithm can be expressed as:

$c = \mathrm{E}(3, p) = (p + 3) \bmod (26)$

A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k, p) = (p + k) \bmod 26$$

where k takes on a value in the range 1 to 25;

The decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

Brute-Force Cryptanalysis of Caesar Cipher

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

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

Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

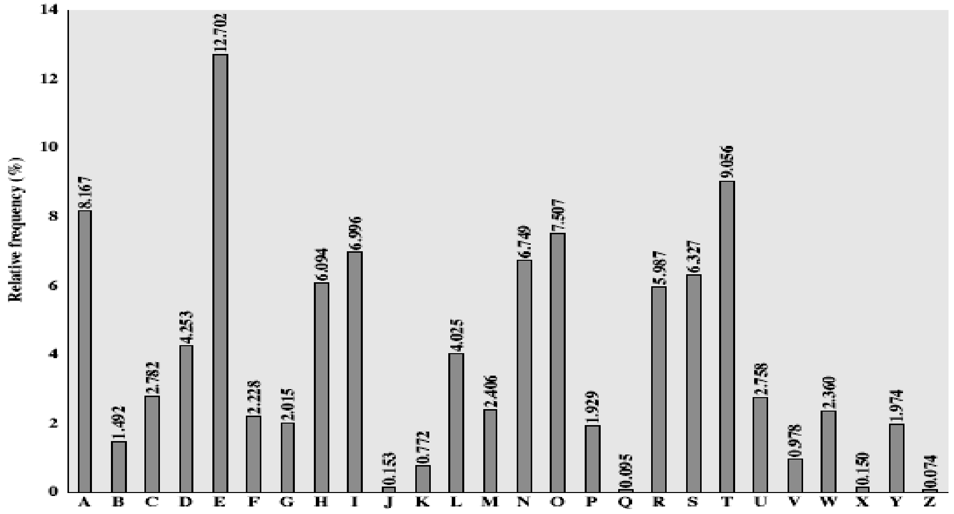
1) The encryption and decryption algorithms are known.
2) There are only 25 keys to try.
3) The language of the plaintext is known and easily recognizable.

So, with only 25 possible keys, the Caesar cipher is far from secure!

Monoalphabetic Cipher

If the “cipher” line **can be any permutation** of the 26 alphabetic characters, then there are 26! or greater than 4 x 10^{26} possible keys

Let a ciphertext:
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ



How cryptanalysis might proceed?

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

We could make some tentative assignments and start to fill in the plaintext to see if it looks like a reasonable “skeleton” of a message.
Then, we could look for repeating sequences of cipher letters and try to deduce their plaintext Equivalents. Check two-letter combinations, three-letter combination, etc.

Continued analysis of frequencies plus trial and error should easily yield a solution.

So, Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet!

Few more substitution techniques

- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
  - Vigenère Cipher
  - Vernam Cipher
- One-Time Pad

Rail Fence Cipher

Rail Fence Cipher

- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows

plain: meet me after the toga party
write: m e m a t r h t g p r y
e t e f e t e o a a t
cipher: MEMATRHTGPRYETEFETEOAAT

It would be trivial to cryptanalyze !

A more complex scheme:

- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of the columns then becomes the key to the algorithm.

```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

The transposition cipher can be made significantly more secure by performing more than one stage of transposition.

Rotor Machines

Multiple stages of encryption can produce an algorithm that is significantly more difficult to cryptanalyze.

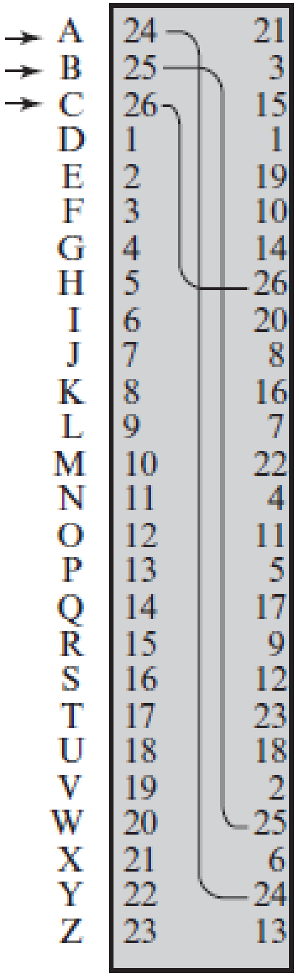
This is as true of substitution ciphers as it is of transposition ciphers.

This class of systems is known as **rotor machines.**

The machine consists of a set of independently rotating cylinders through which electrical pulses can flow.

Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.

Let a single cylinder defines a monoalphabetic substitution.



Fast rotor

Consider a machine with a single cylinder.

After each input key is depressed, the cylinder rotates one position, so that the internal connections are shifted accordingly.

Thus, a different monoalphabetic substitution cipher is defined.

Thus, we have a polyalphabetic substitution algorithm with a period of 26.

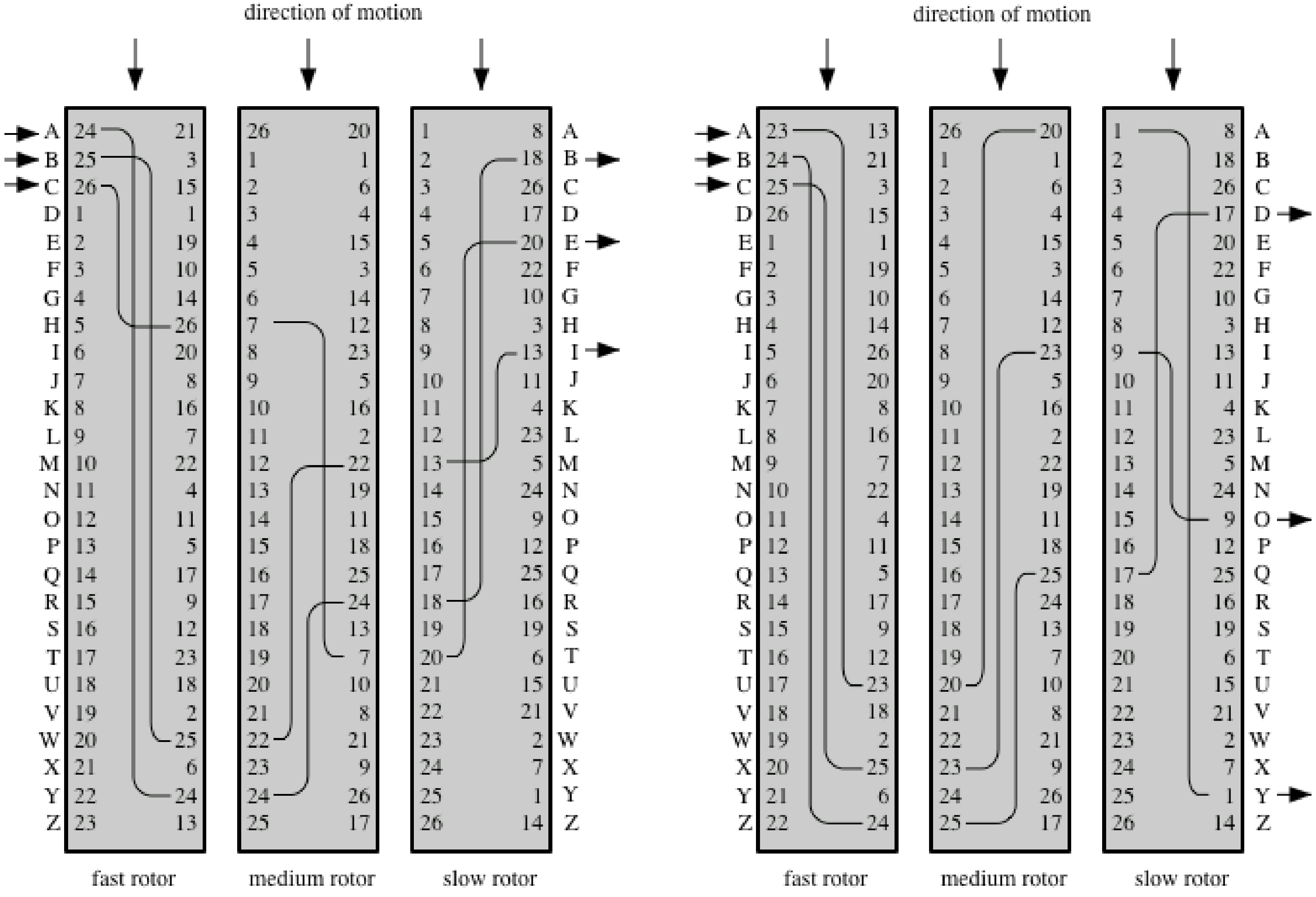
Rotor Machines

The power of the rotor machine is in the use of multiple cylinders, in which the output pins of one cylinder are connected to the input pins of the next.

As per this figure, 26 * 26 * 26 = 17,576 different substitution alphabets used before the system repeats.

Thus, a given setting of a 5-rotor machine is equivalent to a cipher with a key length of 11,881,376!

So, it presents a formidable cryptanalytic challenge.



(a) Initial setting

(b) Setting after one keystroke

Steganography

Steganography conceals the existence of the message.

Various techniques:

- Character marking
  - Selected letters of printed or typewritten text are over-written in pencil
  - The marks are ordinarily not visible unless the paper is held at an angle to bright light
- Invisible ink
  - A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper
- Pin punctures
  - Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light
- Typewriter correction ribbon
  - Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Thank You