Cryptography

CSS 325

Cryptography

- Cryptography is the science of secret, or hidden writing
- It has two main Focus:

1. **Encryption**
   – Practice of hiding messages so that they can not be read by anyone other than the intended recipient
2. **Authentication & Integrity**
   – Ensuring that users of data/resources are the persons they claim to be and that a message has not been secretively altered

Key Terms

- Plaintext (original message)
- Ciphertext (Coded message)
- Enciphering or Encryption (Process of converting plaintext to ciphertext
- Deciphering or decryption (restoring plaintext from ciphertext)

Cryptology

- Cryptosystem (System doing encryption and decryption)
- Cryptanalysis (Deciphering of a message without a knowledge of the enciphering details - breaking the code)
- Cryptology (area of cryptography and cryptanalysis)
- Brute-force attack also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered

Why Cryptography

- The ubiquitous nature of computer networks has given rise to e-commerce, e-Business, e-Learning, e-health and other web-based application has enlarged the area in which cryptography is needed.
- Transactions over the web have changed the scale and environment in which the problems of secrecy and authentication exist.

Cryptographic systems

- **Symmetric Cipher**

  (Encryption and Decryption are performed using the same key)

- **Asymmetric Cipher**

  (Encryption and Decryption are performed using different keys)

Cryptographic System Characterization

Three independent dimensions

- **Type of operations used for transforming plaintext to ciphertext**

  All encryption algorithms are based on two general principles:

  ❖ Substitution in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element,

  ❖ Transposition in which elements in the plaintext are rearranged.

  The fundamental requirement is that no information be lost

  All operations are reversible

  Most systems are **PRODUCT SYSTEMS** (They involve multiple stages of substitutions and transpositions)

Cryptographic System Characterization Cont.

- **The number of keys used.**
  - ❖ If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
  - ❖ If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

Cryptographic System Characterization Cont.

- **The way in which the plaintext is processed.**
  - A block cipher processes the input one block of elements at a time, producing an output block for each input block.
  - A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

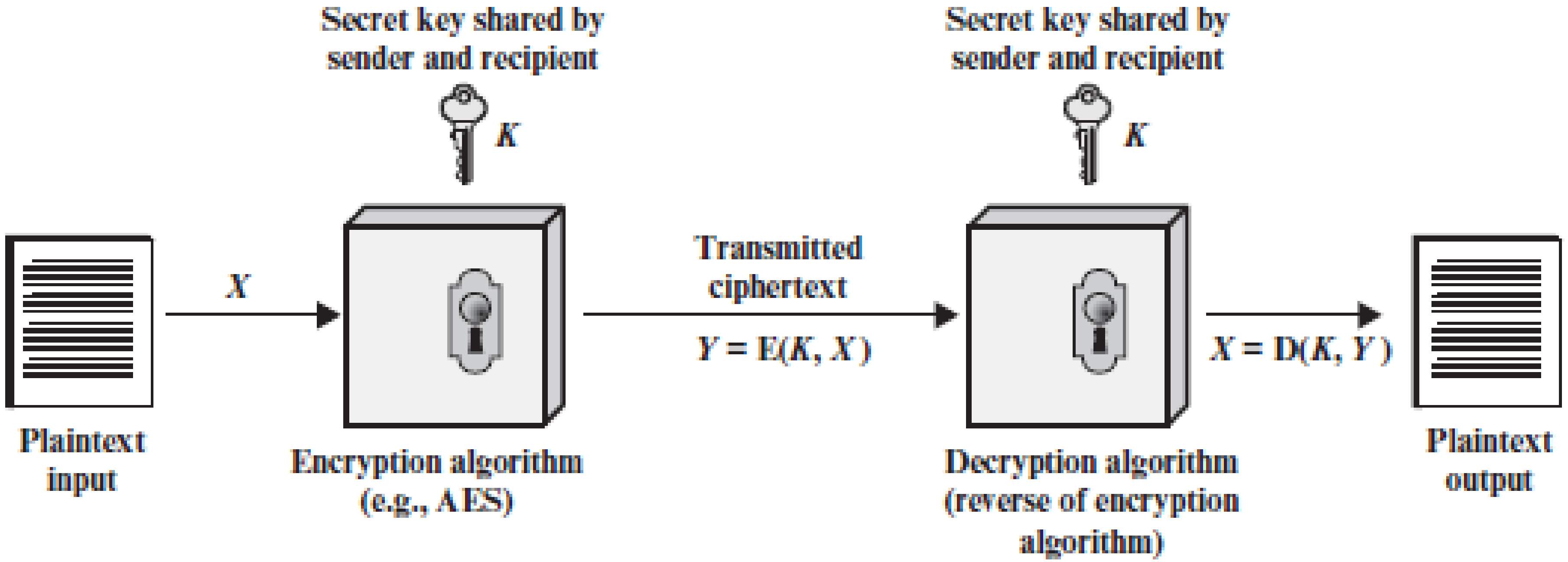
Symmetric cipher model

- A symmetric encryption scheme has five ingredients;
  - ❖Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
  - ❖Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
  - ❖Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Symmetric encryption scheme ingredients

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

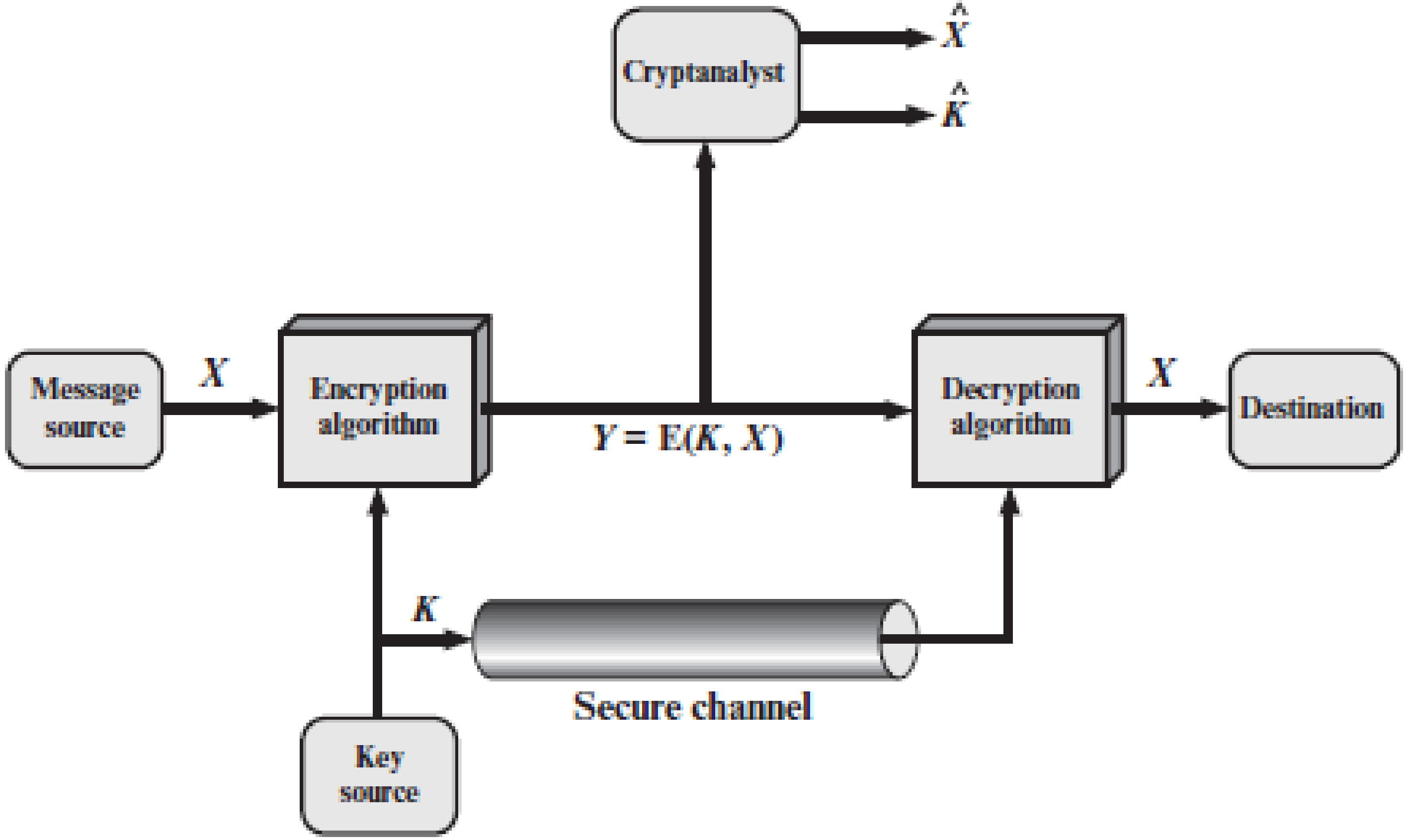
Simplified Model of Symmetric Encryption



Requirements for secure use of conventional encryption

- There are two requirements for secure use of conventional encryption
  - Strong encryption algorithm. We would like the algorithm to be strong such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key
  - Secure key sharing mechanism. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

Symmetric Cryptosystem Model



Approaches Against a conventional encryption scheme

- Cryptanalysis:

This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- Brute-force attack:

The attacker tries every possible key on a piece of ciphertext

until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success

Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key

Cryptanalytic attacks Cont.

Type of Attack	Known to Cryptanalyst
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding • ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalytic attacks Cont.

Type of Attack	Known to Cryptanalyst
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Unconditionally secure

- An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available
- However, there is no encryption algorithm that is unconditionally secure.
- Encryption Algorithm is all about;
  - ❖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.

Computationally secure Algorithm

- An encryption scheme is said to be computationally secure if either of the foregoing two criteria are met
- Unfortunately, it is very difficult to estimate the amount of effort required to cryptanalyze ciphertext successfully

Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Substitution techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- **Substitution Cipher** Techniques
  - Caesar Cipher
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Ciphers
    - ❖VIGENÈRE CIPHER
    - ❖One time pad

Caesar Cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.
- The Caesar cipher involves 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`

Caesar Cipher Cont.

- In Caesar Cipher alphabet is wrapped around, so that the letter following Z is A

plain: 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

cipher: 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

Numerical equivalent of letters:

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

Caesar Cipher Math Representation

- For each plaintext letter p, substitute the ciphertext letter C

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

- A shift may be of any amount, so that the general Caesar algorithm is written as;

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

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

- The decryption algorithm;

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

Caesar Cipher problem

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

Brute-Force Cryptanalysis of Caesar Cipher

With only 25 possible keys Caesar Cipher is far from secure

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

Solution on Caesar Cipher Problem

- In most networking situations, we assume that the algorithms are known. What generally makes brute-force cryptanalysis impractical is the use of an algorithm that employs a large number of keys E.g, triple DES algorithm
- Input may be abbreviated or compressed in some fashion, again making recognition difficult

Compressing using ZIP algorithm

```
˜+Wµ"— Ω–O)≤4{∞‡¸ ĕ~Ω%ràu·¯ƒ ◊¯Z-
Ú≠2∂#Åæ∂ œ«q7¸Ωn·®3N◊Ú Œz'Y–ƒ∞ƒ[±0_ èΩ,<NO¬±«ˇxã  Åäfèü3Å
x}ö§kºÂ
_yÍ ^ΔÉ] ¸¤ J/˚iTê&ı 'c<uΩ-
 ÄD(G WÄC~y_ïöÄW PÔı«ÎÜ†ç],¤¡ˇÌ^üÑπˇ≈ˇLˇ9OgflOˇ&Œ≤ ¬≤ ØÔ§˝:
 ˇŒ!SGqèvo^ ú\¸S>h<–*6ø‡%x´˝|fiÓ#≈˜my‰ˇ≥ñP‹,ƒi Áj  Å◊¿˝Zù-
Ω¨õ¯6Œÿ(% „ΩÊó ¸ÿ π+Áî˚úO2çSy´O-
2ÄflßI /@^"∏Kºª PŒπ¸úé^´3∑˘ö˘ÔZÌ"Y¬ŸΩœY› Ω+eô/˙‹K£¿*÷˜"≤û˜
B ZøK˜QßÿüÍ¸!ÒflÎzsS/]›ÈQ ü
```

Monoalphabetic Ciphers

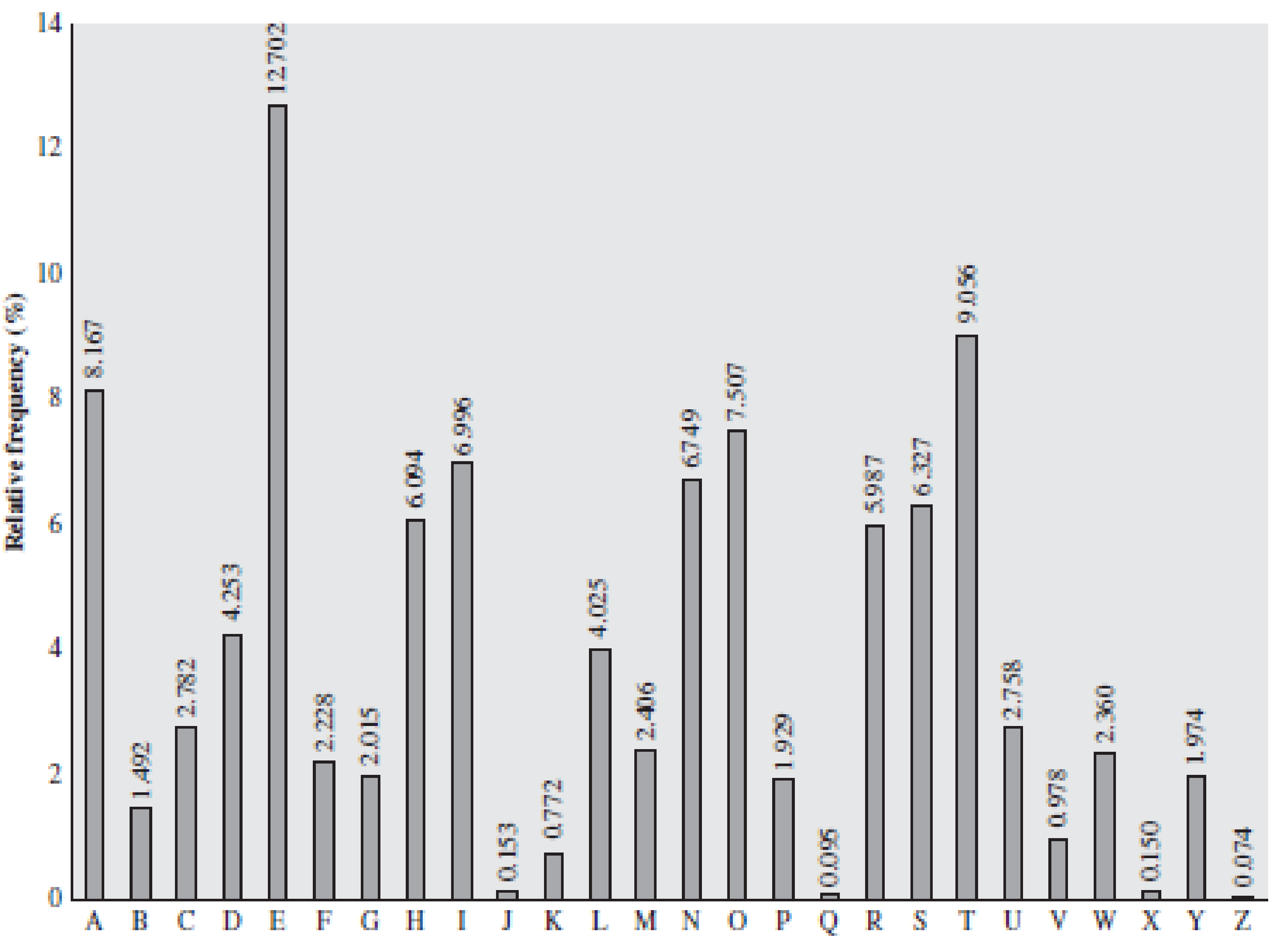
- A dramatic increase in key space can be achieved by allowing an **arbitrary substitution**

❖ If the cipher can be any permutation of the 26 alphabetic characters, then there are 26! Or greater than 4×10^{26} possible keys.

❖ This is greater key space and would seem to eliminate brute-force techniques for cryptanalysis

Relative frequency of Letters in English Text

Attack of
Monoalphabetic Cipher



Example

Cipher text

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Letters frequencies obtained for comparison

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								

Replacing in the obtained letters
(only four letters have been identified and replaced)

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a         e  e te  a that e e a         a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th     t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the    t
```

Plain text obtained

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Playfair Cipher

- The best known multiple letter cipher
- Based on 5x5 matrix of letters constructed using a keyword
- For example "MONARCHY" is a keyword

Fill in the letters in the matrix from left to right after the keyword without repeating the letter

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

Playfair Encryption rules

Plaintext is encrypted two letters at a time

1. Repeating plaintext letters that are in the same pair are separated with a **filler letter**, such as **x**, so that: { **balloon** is treated as **ba lx lo on**}

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, **ar** is encrypted as **RM**.

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, **mu** is encrypted as **CM**.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, **hs** becomes **BP** and **ea** becomes **IM** (or **JM**, as the encipherer wishes).

Hill Cipher

- Developed by the mathematician Lester Hill in 1929.
- It is based on modulo arithmetic and matrix

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

Example of Hill Cipher

Table A– Letters and Their Corresponding Positions																									
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
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	0

Given **P = DR**

The encryption Key K**=** $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

Polyalphabetic Ciphers

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message
- This approach is known as **polyalphabetic substitution cipher**
- Common features of polyalphabetic substitution cipher techniques
  - ❖A set of related monoalphabetic substitution rules is used.
  - ❖A key determines which particular rule is chosen for a given transformation.

VIGENÈRE CIPHER

- $P = p_0, p_1, p_2 \ldots\ldots p_{n-1}$
- $K = k_0, k_1, k_2 \ldots\ldots k_{m-1}$
- $C = C_0, C_1, C_2 \ldots\ldots\ldots\ldots Cn\text{-}1$
- $C = C_0, C_1, C_2 \ldots\ldots\ldots\ldots Cn\text{-}1 = E(K, P) = E[(k_0, k_1, k_2 \ldots\ldots k_{m-1)}),(p_0, p_1, p_2 \ldots\ldots p_{n-1})]$
- $C = (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26,$ c,$(p_{m-1} + k_{m-1}) \bmod 26, (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26,$ c, $(p_{2m-1} + k_{m-1}) \bmod 26,$

$$\boxed{C_i = (p_i + k_i \bmod m) \bmod 26}$$

Vigenère Example

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

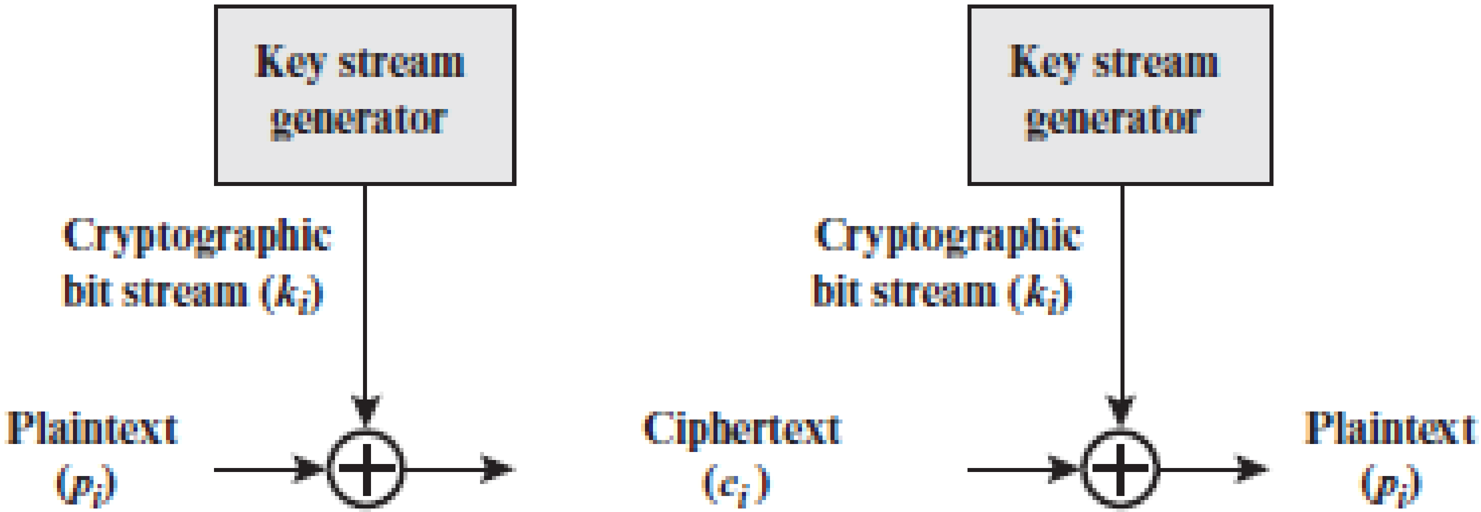
key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenère Weakness

- ZICVTWQNGRZGVTWAVZHCQYGLMGJ
- An analyst looking at only the ciphertext would detect the repeated sequences **VTW** at a displacement of 9 and make the assumption that the keyword is either three or nine letters in length
- By looking for common factors in the displacements of the various sequences, the analyst should be able to make a good guess of the keyword length

Vernam cipher



Vernam cipher Cont.

- The system can be expressed succinctly as follows

$$\boxed{c_i = p_i \oplus k_i}$$

- where

  pi = *i*th binary digit of plaintext

  ki = *i*th binary digit of key

  ci = *i*th binary digit of ciphertext

  $\oplus$ = exclusive or (XOR) operation

- Decryption $\boxed{p_i = c_i \oplus k_i}$

Transposition Cipher Techniques (Rail Fence Technique)

- Enciphering
  - ❖Write a plain text letters in a sequence of diagonals
  - ❖Read off as a sequence of rows

Example:

P="Meet me after the toga party"

Key = (depth) = (2)

M	e	m	a	t	r	h	t	g	p	r	y
	e	t	e	f	e	t	e	o	a	a	t

C= "MEMATRHTGPRYETEFETEOAAT"

Steganography

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Steganography techniques

- **Character marking:** Selected letters of printed or typewritten text are overwritten 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.