Lecture 2: Classical Cryptography

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Introduction

Monoalphabetic Cipher - Frequency analysis

Classical Ciphers

Other Substitution Ciphers

Transposition ciphers

Stream vs Block Enciphering

1. Homework

hqfubswlrq lv d phdqv ri dwwdlqlqj vhfxuh frpsxwdwlrq ryhu lqvhfxuh fkdqqhov eb xvlqj hqfubswlrq zh glvjxlvh wkh phvvdjh vr wkdw hyhq li wkh wudqvplvvlrq lv glyhuwhg wkh phvvdjh zloo qrw eh uhyhdohg

1. Monoalphabetic Cipher - Frequency analysis

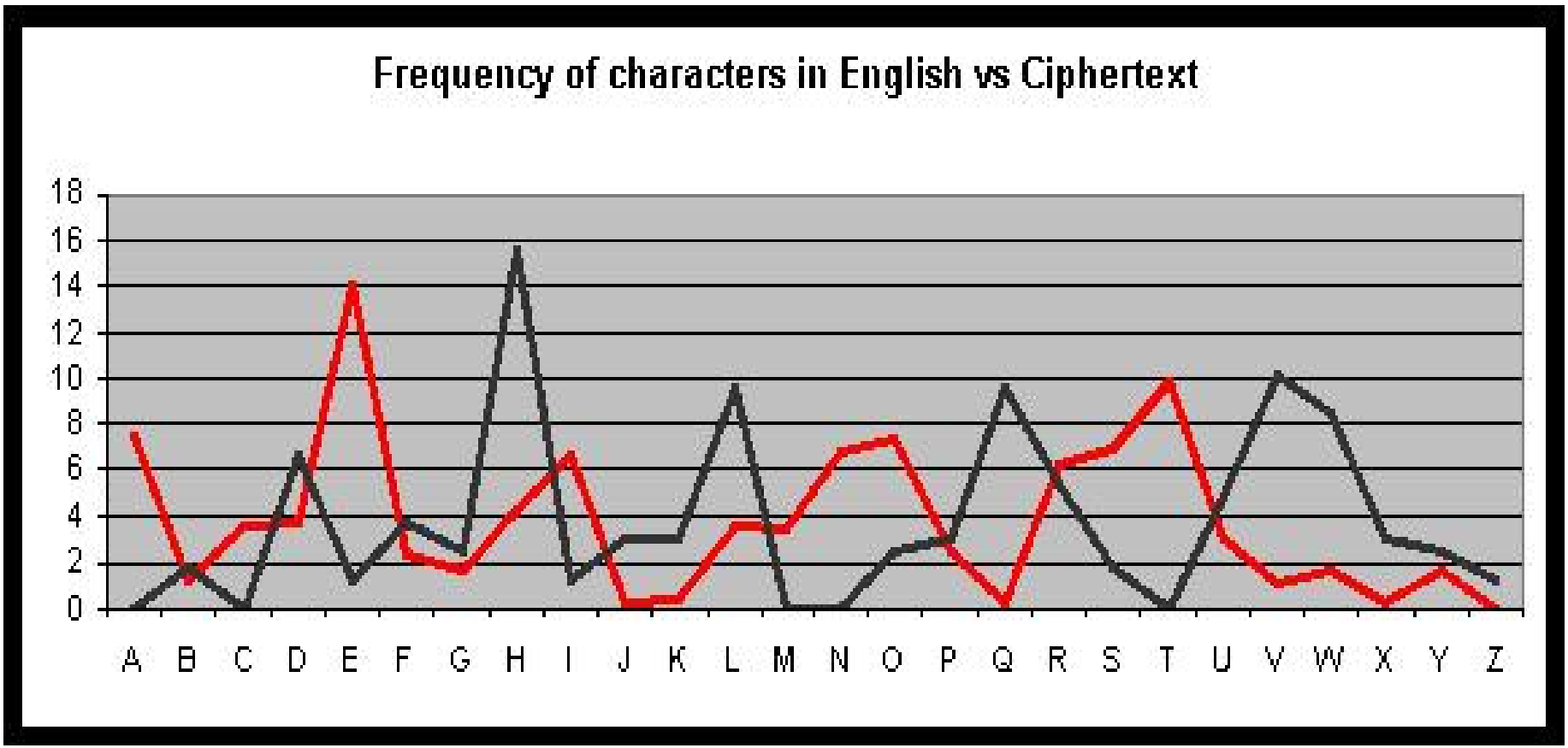
Do a frequency analysis

Letter distribution of English language is fixed (for a large body of text)

Tables of letter distribution

For instance, most commonly used letter is “e”

1. Monoalphabetic Cipher - Frequency analysis



1. Monoalphabetic Cipher - Answer

ENCRYPTION IS A MEANS OF ATTAINING SECURE COMMUNICATION OVER INSECURE CHANNELS BY USING ENCRYPTION WE DISGUISE THE MESSAGE SO THAT EVEN IF THE TRANSMISSION IS DIVERTED THE MESSAGE WILL NOT BE REVEALED

How do we increase security of the monoalphabetic cipher?

3. Polyalphabetic ciphers

Use more than one alphabetic substitution to flatten the frequency distribution

Combine substitutions that are high with those that are low

Eg use:

- P_1(a) = (a*3)mod26
- P_2(a) = ((5*a)+13)mod26

3. Polyalphabetic ciphers

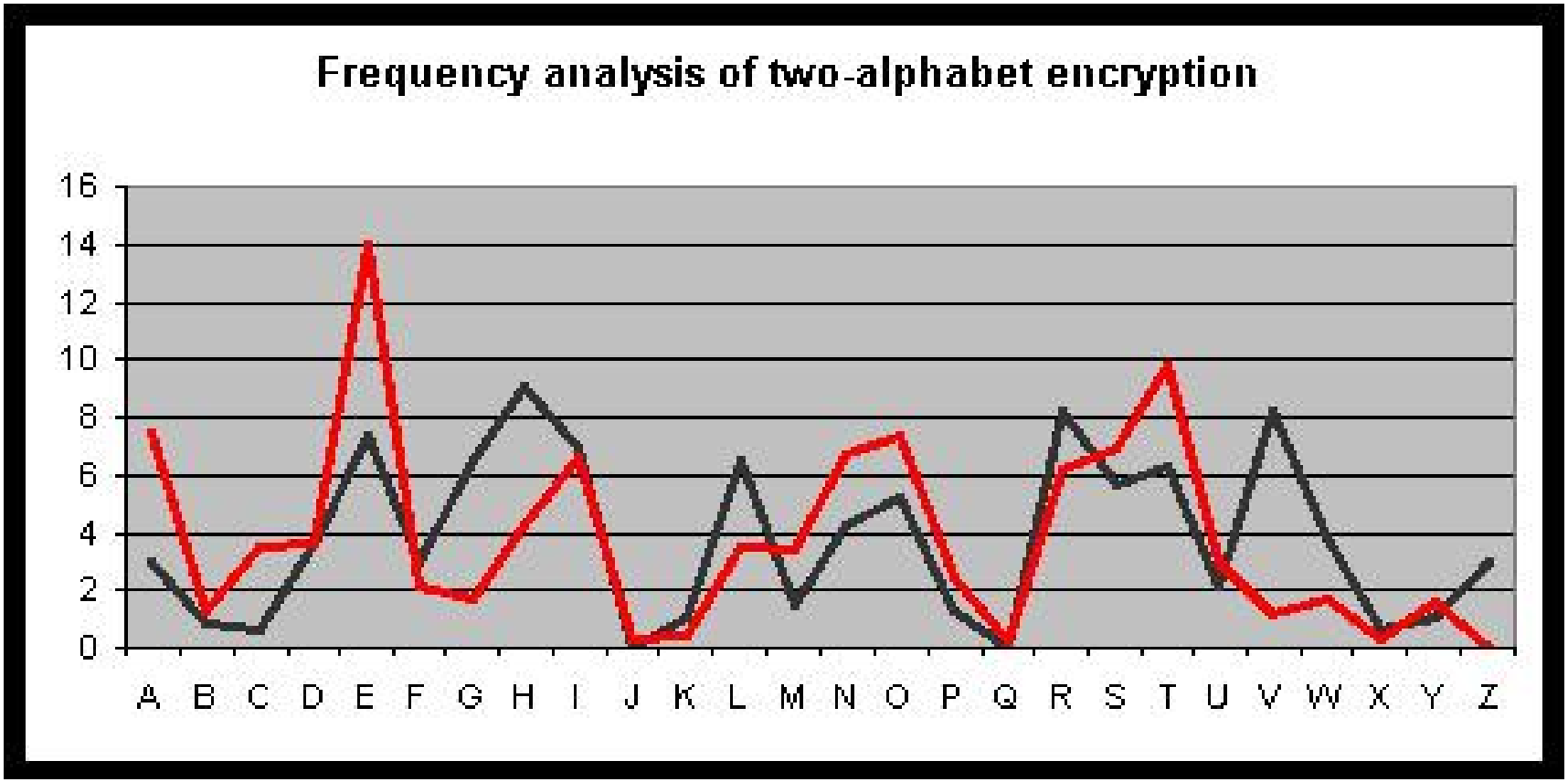
Cipher I:

A	B	C	D	E	F	G	...	S	T	U	V	W	X	Y	Z
a	d	g	j	m	p	s	...	c	f	i	l	o	r	u	x

Cipher II:

A	B	C	D	E	F	G	...	S	T	U	V	W	X	Y	Z
n	s	x	c	h	m	r	...	z	e	j	o	t	y	d	i

3. Polyalphabetic ciphers - Frequency distribution



3. Vigenere tables

	a	b	c	d	e	f	...	t	u	v	w	x	y	z	π
A	a	b	c	d	e	f	...	t	u	v	w	x	y	z	0
B	b	c	d	e	f	g	...	u	v	w	x	y	z	a	1
C	c	d	e	f	g	h	...	v	w	x	y	z	a	b	2
⋮			⋮				⋱				⋮				⋮
X	x	y	z	a	b	c	...	q	r	s	t	u	v	w	23
Y	y	z	a	b	c	d	...	r	s	t	u	v	w	x	24
Z	z	a	b	c	d	e	...	s	t	u	v	w	x	y	25

3. Polyalphabetic Keys

Some type of key needed for polyalphabetic ciphers

Can be a series of indices for monoalphabetic substitution using

- formula $\rightarrow P_n(a) = (a + n) \mod 26$
- key $\rightarrow$ 0123456789

0	1	2		3	4	5	6	7		8	9	0		1	2	3	4	5	6
S	H	E		S	E	L	L	S		S	E	A		S	H	E	L	L	S
s	i	g		v	i	q	r	z		a	n	k		d	t	r	z	a	i

3. Polyalphabetic Keys

More usually key is some codeword

Eg, use delta as keyword

d	e	l	t	a	d	e	l	t	a	d	e	l	t	a	d	e	
S	H	E	S	E	L	L	S	S	E	A	S	H	E	L	L	S	
v	l	p	l	e	o	p	d	l	e	d	w	s	x	l	o	w	

frequency distribution not totally flat

4. Other Substitution Ciphers

ROT(13)

XOR function (Bitwise)

Rotor Machines (WW II style)

5. Transposition ciphers

Effectively creates a permutation of the plaintext

Letters do not change - Only the order in which they are written

Eg $\rightarrow$ seapigeon

5. Transposition ciphers

What is the letter frequency of a transposition cipher?

5. Transposition ciphers

Diffusion - process of mixing up plaintext to form ciphertext (transposition)

Confusion - disguising each of the plaintext characters (substitution)

5.1 Columnar Transposition

Plaintext:

$$\begin{array}{ccccc} C_1 & C_2 & C_3 & C_4 & C_5 \\ C_6 & C_7 & C_8 & C_9 & C_{10} \\ C_{11} & C_{12} & C_{13} & C_{14} & C15 \end{array}$$

Ciphertext:

$$C_1\,C_6\,C_{11} \quad C_2\,C_7\,C_{12} \quad C_3\,C_8\,C_{13} \quad C_4\,C_9\,C_{14} \quad C_5\,C_{10}\,C_{15}$$

5.1 Columnar Transposition

Well Known Columnar Transposition:

tcrnu oramg oypao mphkn utyeu cocyt hgaos

5.1 Columnar Transposition

Answer:

5.1 Columnar Transposition

Answer:

T	O	O	M	U	C	H
C	R	Y	P	T	O	G
R	A	P	H	Y	C	A
N	M	A	K	E	Y	O
U	G	O	N	U	T	S

5.2 Transposition ciphers - characteristics

Delay in encoding and decoding

Can use a lot of memory

Not appropriate for large amounts of data

6. Stream vs Block Enciphering

Substitution cipher a stream cipher

Columnar Transposition a block cipher

6.1 Stream Cipher

Advantages:

- Speed of transformation
- Low error propagation

Disadvantages

- Low diffusion
- Susceptible to integrity attacks

6.2 Block Cipher

Advantages:

- Diffusion
- Immunity to insertions

Disadvantages:

- Slow translation
- Error propogation

Summary

Monoalphabetic Cipher - Frequency analysis

Classical Ciphers

Other Substitution Ciphers

Transposition ciphers

Stream vs Block Enciphering