11464: INFORMATION SYSTEMS SECURITY

Chapter 3: Classic Encryption Technique

2

Cryptography Tool

By

Mustafa Al-Fayoumi

Outline

- Substitution Cipher
  - Caeser cipher
  - Mono alphabetic cipher (Vernam cipher)
  - Poly alphabetic cipher
  - Playfair Cipher
  - Hill Cipher
  - Random number
  - One Time Pad
- Transposition Ciphers
  - Rail Fence
  - Complete Square (Double Transposition)
  - Row Transposition
  - Columnar Transposition
  - Fixed Period

Substitution Cipher

- **Substitution cipher:** The encryption process systematically manipulate a symbol (or a group of symbols) in the plaintext to produce a different symbol (or group of symbols), which becomes the ciphertext.
  - The substituted symbols in the ciphertext appear in exactly the same order as the original versions in the plaintext.

A simple substitution cipher: The Caesar cipher

- **Caesar cipher** is one of the earliest recorded and best known ciphers was used by Julius Caesar in the 1st century BC.
- **Caesar cipher** is one of the simplest of substitution ciphers.
- How did Caesar preserve the confidentiality of his message?
  - He substituted each letter in his message with the letter three places further forward in the alphabet.
  - Thus the letter 'a' would be substituted by the letter 'd', the letter 'b' by the letter 'e', and so on.
- The process used by Caesar is an example of a systematic manipulation!

A simple substitution cipher: The Caesar cipher

- **Example1:** using this method, the word '**acme**' becomes **DFPH.**

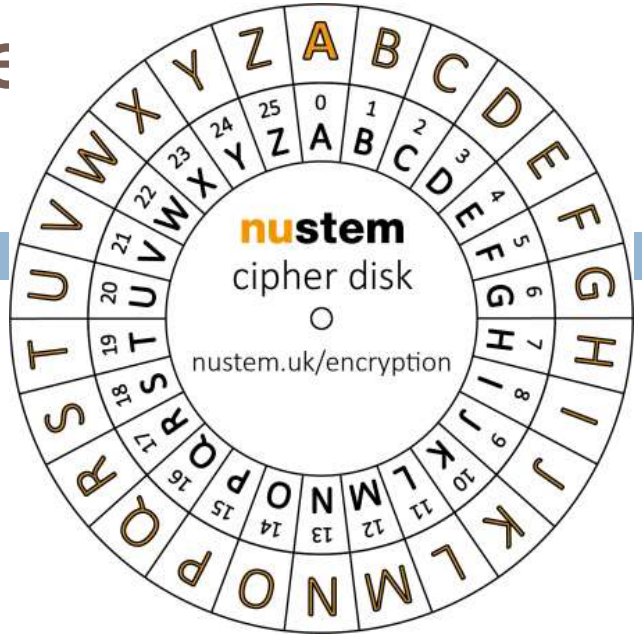
But what if we wanted to encrypt the word 'zenith' using the Caesar cipher? *How 'z' is encrypted?*

- The solution is to **jump back to the letter** 'a' and continue the count as if the letters of the alphabet were **arranged in a circle**
- **Example2:** the word '**zenith**' becomes **CHQLWK.**
- ***Study note:*** *Always represent the **plaintext in lower case** and **ciphertext in UPPER CASE**.*

A simple substitution ciphe
The Caesar cipher

- The circular nature of the Caesar cipher can be exploited to produce a simple encryption tool known as a **cipher wheel**.

  - The wheel is made up of two discs
  - The alphabet is written around the circumference of both discs
  - Discs are fitted together at their centers
  - The sender and recipient first agree on the number of shifts
  - One wheel is then rotated using the pre-agreed number of shifts.
    Each letter of the outer wheel is consequently aligned with any letter on the inner wheel



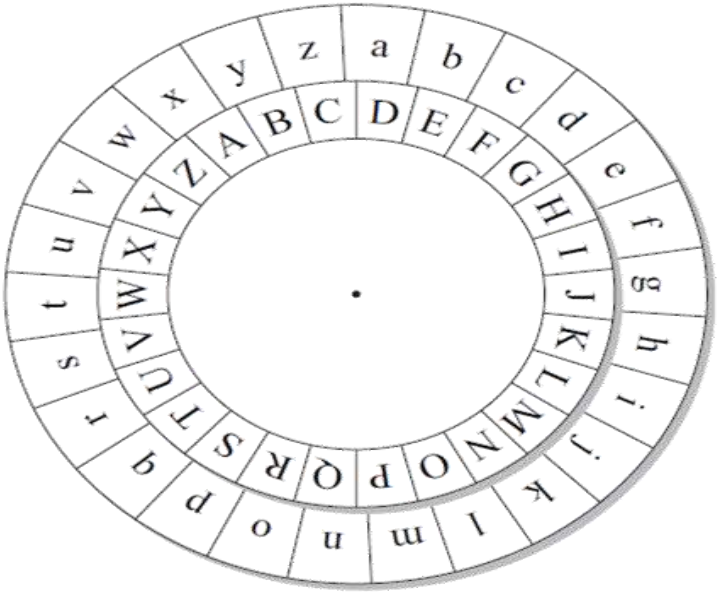
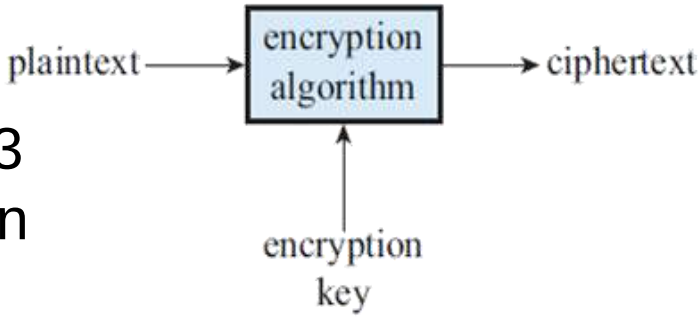


Figure 5.2 A cipher wheel

A simple substitution cipher: The Caesar cipher

- A key element in Caesar Cipher is "the number of shifts"
  - Changing the "number of shifts" produces different ciphertext from a given plaintext
    - Example: Caesar's successor, Augustus Caesar, changed the shift from 3 to 2.
  - Any shift of 1 to 25 would work equally and produces different ciphertext from a given plaintext.
- In any encryption process, when altering a "variable" produces different outcome (ciphertext) this "variable" is called a **Key**
  - So here we can say that Julius Caesar used an encryption key of 3 and Augustus Caesar an encryption key of 2.



Mathematical representation

- Modern communication systems use computers to process messages.
- Computers do not work with letters but with numbers!

How the Caesar cipher can be represented as a numerical algorithm that can be processed by a computer?

Mathematical representation

- Caesar Cipher can be mathematically represented by using "**Modular arithmetic**"
- **Modular arithmetic** operates with **a limited set of integers**
  - **Integer**: positive or negative whole number, including zero.
  - **Example** of a set of integers: S = {0, 1, 2, 3, 4, 5}.
- **In Modular arithmetic:**
  - **The modulus** is the number of integers in the set.
    - In the previous example, the modulus is 6.
  - Whatever mathematical operation we perform on the integers in the set, **the result must always be less than the modulus.**

Mathematical representation

- **Example3:** In a conventional clock, the hour changes in a modular fashion. With a conventional 12-hour clock, what is the modulus? What would be the modulus for a 24-hour clock?
  - With a conventional 12-hour clock
    - The set is: S={0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
    - The modulus is 12
  - For a 24-hour clock
    - The set is : S={0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23}
    - The modulus is 24.

What is modular arithmetic?

Mathematical representation

- **Modular Addition:**
- Let's assume we want to move forward eight hours from ten o'clock using the 12-hour clock, how can we implement this?
- **Mathematically** this can be represented as:

  10 + 8 modulus 12 is **congruent** to 6 modulus 12.
- **Firstly,** we add the two left-hand integers together in the conventional way:

$$10 + 8 = 18$$

- **Secondly,** if the result is equal to or greater than the modulus
  - subtract the modulus from the result
  - repeating the subtraction until the result is less than the modulus

$$18 - 12 = 6$$

- **Finally,** Now express the answer as **a congruence modulus 12**:

$$10 + 8 \equiv 6 \bmod 12$$

Using a calculator

- **Example:** the calculation to find 315 mod 26 can be performed by using a calculator:

  1- Dividing the number by the modulus

  $$315 \div 26 = 12.115385$$

  2- Take the whole number part and multiply by the modulus

  $$12 \times 26 = 312$$

  3- Subtract the result from the original number to find the remainder, which is the required result

  $$315 - 312 \equiv 3 \bmod 26$$

Mathematical representation

How to apply the same method to implement the Caesar Cipher encryption algorithm?

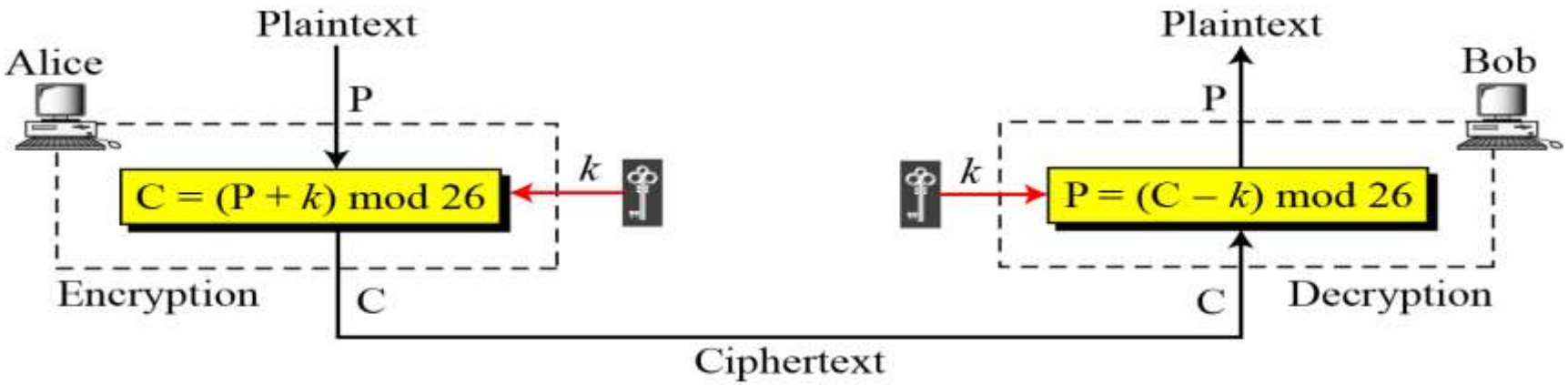
- **Modular arithmetic deals with integers, so:**
  - At first, alphabet is converted to numbers.
  - The following coding table can be used for this purpose:

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

Why we have chosen to set 'a' to 0 rather than to 1?

- Because the result of any calculation in modular arithmetic must always be less than the modulus (i.e. 26).
  - if we had set 'a' to 1 and therefore 'z' to 26, 26 would be an invalid result.

Additive Cipher



Note

When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

Additive Cipher

- Caesar encryption technique can be mathematically modeled using "Modular addition"
- The general formula of a Caesar cipher would be expressed as:

$$p + K \equiv c \bmod n$$

$$C = p + K \bmod n$$

- **Where:**
  - *n is the modulus*
  - *p* is used to represent the plaintext
  - c is used to represent the ciphertext
  - *K* is used to represent the key.

- **For Caesar Cipher:**
  - We have 26 different letters so the modulus is n = 26
  - p, c and K can take any value between 0 and 25.

Additive Cipher

- **Example 4:** Encrypt the letter 'z' with a Caesar cipher using a key of K=3.

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

- The numerical form of z is: p=25.
- The ciphertext is obtained by: $c \equiv p + K \bmod 26$

  so, $c \equiv 25 + 3 \bmod 26 \equiv 28 \bmod 26 \equiv 2 \bmod 26$

  so, the numerical for of the ciphertext is $c = 2$
- The numerical value of 2 represents the letter 'C' (the ciphertext)
- So **'z' encrypts to C.**

Additive Cipher

- Use the additive cipher with key = 15 to encrypt the message "hello".
- Solution
  - We apply the encryption algorithm to the plaintext, character by character:

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

Additive Cipher

- **Exercise 1:** Write out the following using mathematical notation and evaluate the result. Use the previous table to translate between alphabetic symbols and numerical values.
  - (a) The ciphertext resulting from encryption letter 'f' using the Caesar cipher with a key of 6.
  - (b) The ciphertext resulting from encryption letter 's' using the Caesar cipher with a key of 12.
  - (c) The ciphertext resulting from encryption letter 'm' using the Caesar cipher with a key of 20.

Decrypting the Caesar cipher

- Using **the cipher wheel** the decryption process simply involves:
  - Displacing the outer wheel clockwise a number of places corresponding to the agreed key
  - Translating each ciphertext letter shown on the inner wheel to its equivalent plaintext letter on the outer wheel.
- Using Julius Caesar's version of the cipher this would require a clockwise displacement of three places.
  - This would be just the same as displacing the outer wheel 23 places in an anticlockwise direction.
  - An anticlockwise displacement of 23 (or 26 − 3) is the equivalent of a clockwise displacement of 3.
  - Thus 3 and 23 form a **complementary pair**
    - Two numbers X and Y are said to be complementary pair when X+Y = modulus (3+23 = 26 = modulus)

Decrypting the Caesar cipher

- Mathematically the decryption algorithm of a Caesar cipher would be expressed as:

$$p \equiv c - k \bmod 26$$

$$p \equiv c + \bar{K} \bmod 26$$

Where $\bar{K}$ (read as ***K* bar**) is **the decryption key**.

And K and $\bar{K}$ form a complementary pair ($K + \bar{K} = 26$)

- **Example 5:** What are the decryption keys for the Caesar cipher with encryption keys of: 10, 15 and 7?
  - $K=10 \rightarrow K+\bar{K}=26 \rightarrow \bar{K}=26-K=26-10 \rightarrow \bar{K}=16$
  - $K=15 \rightarrow K+\bar{K}=26 \rightarrow \bar{K}=26-K=26-15 \rightarrow \bar{K}=11$
  - $K=7 \rightarrow K+\bar{K}=26 \rightarrow \bar{K}=26-K=26-7 \rightarrow \bar{K}=19$

Decrypting the Caesar cipher

- Use the additive cipher with key = 15 to decrypt the message "WTAAD".
- Solution
  - We apply the decryption algorithm to the plaintext character by character:

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

Breaking a cipher

- **Breaking (or cracking) a cipher:** is to derive the plaintext from the ciphertext without knowledge of the key (and often without knowledge of the encryption algorithm).
- **The strength of a cipher is measured by how long it takes to break it.**
  - Notice that we said '*how long it takes to break it*' and **NOT** '*whether it can be broken*'.
    - Potentially all known ciphers except one are thought to be breakable !
  - The time and effort required to break a cipher is not justified by the value of the information retrieved.
    - The cipher may take so long to break that by the time the information is retrieved it has lost its value.

Breaking a cipher

- **Strong Ciphers** take **a long time to break,** but they also tend to be **more difficult to use.**
- **Weak ciphers** are **quicker to break** but are usually also **quite easy to use.**
- **The choice of cipher** will usually be determined by the value of the information it is designed to protect
  - The use of any cipher induces an **overhead in terms of time and processing demands**

How to break a cipher?

Cryptanalysis of Caesar Cipher

- Brute-Force Cryptanalysis of Caesar Cipher
- 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. (Linguistic Analysis)
- **Linguistic Analysis:** to attempt to exploit any linguistic patterns inherited from the plaintext (for only textual contexts).

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.
- Figure 2.3 shows the results of applying this strategy to the example ciphertext. In this case, the plaintext leaps out as occupying the third line

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

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Brute-Force Cryptanalysis of Caesar Cipher

- **Example:** Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use a brute-force attack to break the cipher.
- Solution
  - Eve tries keys from 1 to 7. With a key of 7, the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Linguistic analysis

- **All written languages exhibit characteristic patterns.**
  - For example, in written English
    - the letter ‘q’ is almost always followed by a ‘u’
    - certain pairs of letters (known as digraphs) are more likely to appear together than others: ‘th’ is common as are ‘ea’, ‘of’, and ‘st’.
    - Some identical letters can often appear together, for example ‘ee’, ‘oo’, ‘tt’, but seldom ‘uu’ or ‘hh’.
  - There is a higher probability of certain letters appearing than other letters
    - For example , in written English
      - The most common letter is ‘e’, followed by ‘t’, ‘a’ and ‘o’.
      - ‘etaoin’ are the six most frequent letters.

Linguistic analysis

Table 5.1 Typical letter frequencies of written English (Beker and Piper, 1982)

Letter	Frequency (%)	Letter	Frequency (%)
e	12.7	m	2.4
t	9.1	w	2.4
a	8.2	f	2.2
o	7.5	g	2.0
i	7.0	y	2.0
n	6.7	p	1.9
s	6.3	b	1.5
h	6.1	v	1.0
r	6.0	k	0.8
d	4.3	j	0.2
l	4.0	x	0.2
c	2.8	q	0.1
u	2.8	z	0.1

Table 5.1 ***Frequency of characters in English***

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Table 5.2 ***Frequency of diagrams and trigrams***

Linguistic analysis

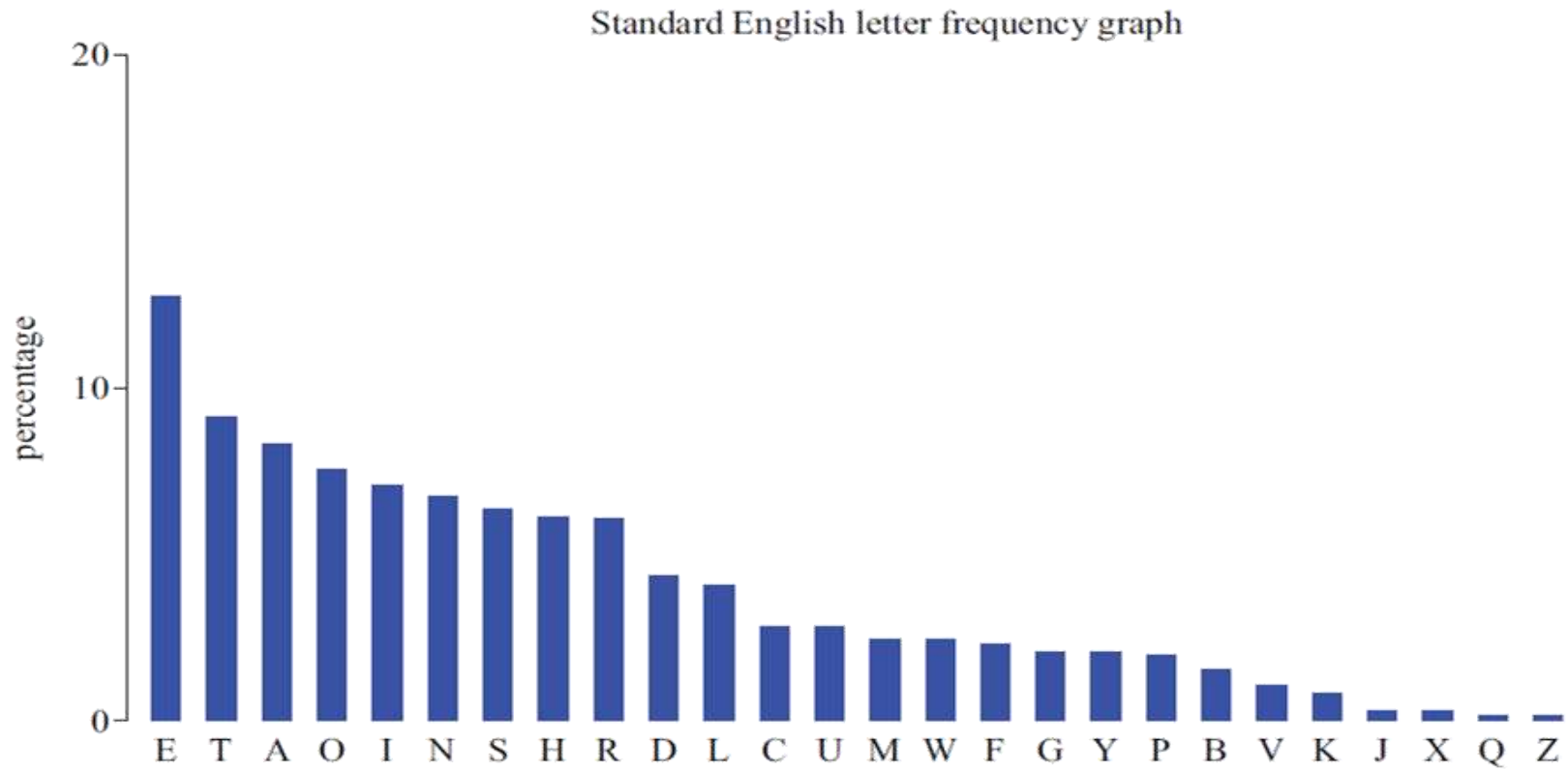


Figure 5.8 Graph of typical written English letter frequencies arranged in order of frequency

Linguistic analysis

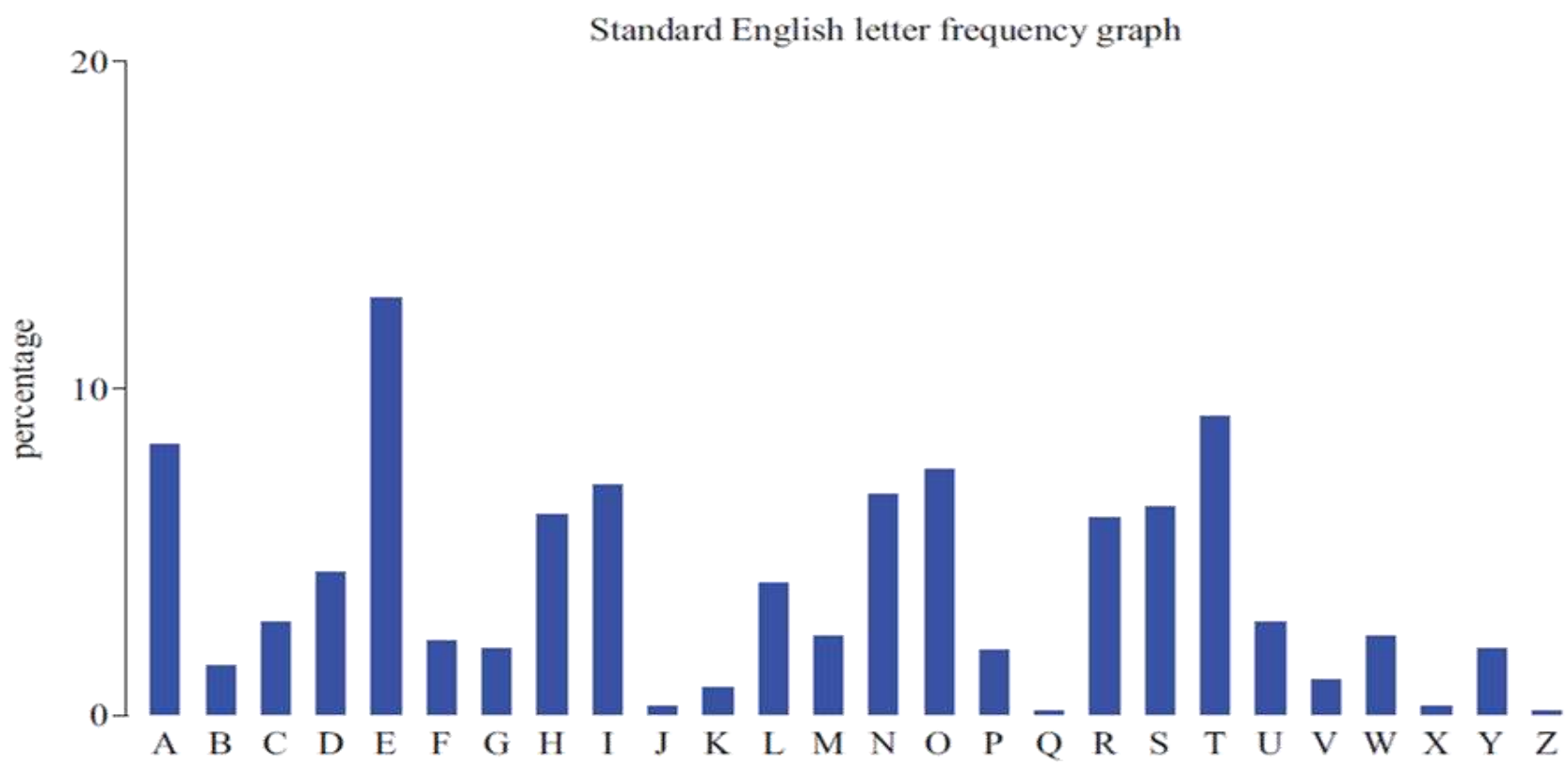


Figure 5.9 Graph of typical written English letter frequencies arranged in alphabetic order

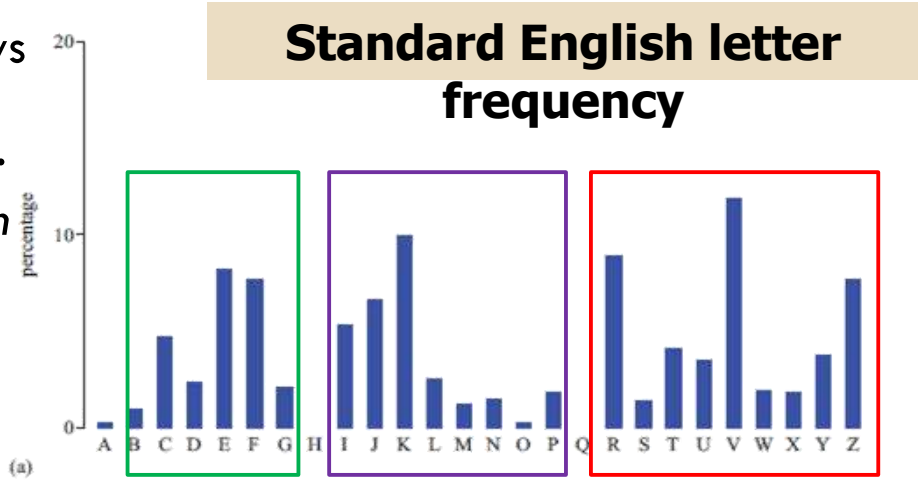
Linguistic analysis

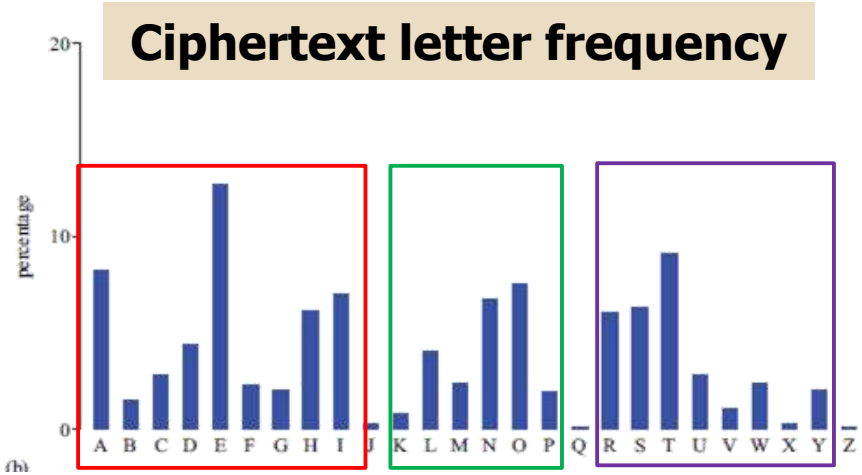
- A ciphertext sequence can also be analysed for **letter frequency**.
- If the analysis shows a curve similar to Figure 5.8 or Figure 5.9 then:
  - There is a strong possibility that the most frequently occurring ciphertext letters will correspond to their equivalents in standard English text!

How linguistic analysis can help to break ciphers?

Linguistic analysis

- **Example 6:** The figure below shows the results of letter frequency analysis of a sample of ciphertext.
  - *Does the ciphertext exhibit a pattern similar to standard English letter frequencies?*
  - *If so, what assumptions could you make about the cipher?*





- **Example 6 – Comments:**
- The following similarities can be noted:
  - R – Z → A – I
  - B – G → K – P
  - I – P → R – Y.

Linguistic analysis

Example 6 – Comments:

- **The similarities mean that the cipher was created using a simple substitution cipher!**
  - The ordering of the letters was preserved in the ciphertext but their identity was changed.
- **In fact, if the ciphertext letter frequency plot was shifted to the left by 17 places the result would look very similar to the standard English plot.**
  - The guess would be that the cipher used was **a simple Caesar cipher with a key of 17.**

A Cryptanalysis Example

The frequencies of occurrence of letters in English text:

Letter	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
Frequency	7	1	3	4	13	3	2	3	8	<1	<1	4	3	8	7	3	<1	8	6	9	3	1	1	<1	2	<1

(Suppose, we know that shift transformation cipher was used)

Ciphertext: YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDLR PD

Analysis of the frequencies of occurrence of letters in the ciphertext:

Letter	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
Frequency	1	0	4	5	1	3	0	0	0	1	0	1	1	1	0	7	2	2	2	3	0	0	1	2	3	2

Guess: P(7) = E(13) => $15 = 4 + k \pmod{26}$ => $k = 11$.

Plaintext: NUMBE RTHEO RYISU SEFUL FOREN CIPHE RINGM ESSAG ES
(NUMBER THEORY IS USEFUL FOR ENCIPHERING MESSAGES)

A Cryptanalysis Example

- Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

- Solution
  - When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Self Assessment

On a Caesar cipher text captured by an intruder, cryptanalysis showed that the highest frequency of the ciphertext letter is the letter "**Q**". If the captured message contains the word "**EQZPYQYAZQK**" then decrypt it.

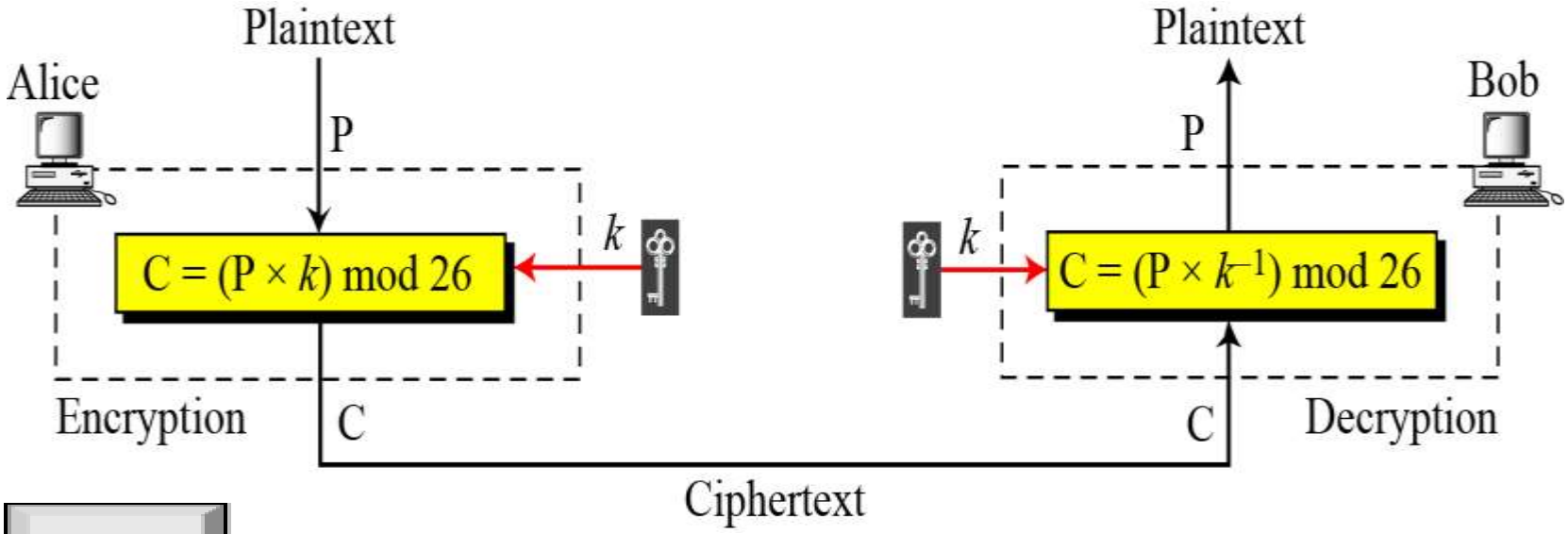
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Answer:
- Guess: **Q** is the highest occurrence in the ciphertext = **E** is the highest occurrence in the ciphertext in the language => *16 = 4 + k (mod 26) => (16 -4) => k = 12.*
- Decryption key = 26 – 12 = 14 *(1 mark)*
- *OR*
- *p ≡ C + 14 mod 26 (1 mark)*

Ciphertext	E	Q	Z	P	Y	Q	Y	A	Z	Q	K
code	4	16	25	15	24	16	24	0	25	16	10
C + 14 Mode 26	18	4	13	3	12	4	12	14	13	4	24
P	s	e	n	d	m	e	m	o	n	e	Y

- *(3 marks for each correct row)*
- The message is "send me money" *(1 mark)*

Multiplicative Ciphers



Note

In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}; the key is an integer in Z_{26}*.

Multiplicative Ciphers

Example

- What is the key domain for any multiplicative cipher?
- Solution
  - The key needs to be in Z_{26}^*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Coprime numbers

- There is a **theorem**, a mathematical finding, that says:
  - 'If you take a set of distinct numbers and multiply, using modular multiplication, each of them by a particular number then the collection of results will contain **no repeats provided** the particular number that was used in the multiplication was **either 1** or has **no factors in common with the modulus**.'

Coprime numbers

- **Two numbers that have no factors in common are said to be coprime**
  - The even numbers are not coprime with 26 because the even numbers and 26 can both be divided by 2. And 13 and 26 are not coprime because they both have the factor 13 and can therefore be divided exactly by 13. It should, therefore, be expected, from a knowledge of the theorem, that **even numbered keys or the key of 13 will create ambiguities** when encrypting using multiplication **modulo 26**
  - For any number it is **straightforward**, but often tedious, to work out how many smaller numbers have no factors in common with the original choice
- We stated that two integers *a* and *b* are relatively prime if and only if their only common positive integer factor is 1. This is equivalent to saying that *a* and *b* are relatively prime if gcd(*a*, *b*) = 1.
  - 8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

- If the number is 26 then only the odd numbers below 26 except 13 are coprime with it. This gives 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25 or a total of **12 smaller numbers** which are coprime with 26. This characteristic of a number has been given a special status by being associated with the oddly named Euler Totient Function
- The **Euler Totient Function** is usually denoted by the Greek letter ø (called 'phi'). For 26, we have discovered that **ø(26) = 12**. This means that there are twelve numbers smaller than 26 which are coprime with it and implies, in the encryption scheme using modulo 26 multiplication, there are twelve keys that will not generate ambiguous results

Example

k	13																									
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
Number equivlant	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
p * k	0	13	26	39	52	65	78	91	104	117	130	143	156	169	182	195	208	221	234	247	260	273	286	299	312	325
calculation results (P * k mod n)	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
Ciphertext	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N

k	8																									
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
Number equivlant	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
p * k	0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	136	144	152	160	168	176	184	192	200
calculation results (P * k mod n)	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
Ciphertext	A	I	Q	Y	G	O	W	E	M	U	C	K	S	A	I	Q	Y	G	O	W	E	M	U	C	K	S

k	9																									
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
Number equivlant	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
p x k	0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171	180	189	198	207	216	225
calculation results (px k mod n)	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
Ciphertext	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R

- **The Problems:**
  - Unfortunately, encryption using multiplication has some peculiarities
  - **The key 13 and even-numbered keys such as 8** (the alphabet Q appearing twice) generate encryption tables containing ambiguities when working with **modulo 26 multiplication**
- **The Solution:**
  - Such ambiguities during encryption restricts the choice of key and makes it necessary to **choose** the **modulus** and the **key carefully**
  - One way to ensure that multiplication can be used as an encryption operation for any key is to **choose the modulus** of the operation as a **prime number**

Multiplicative Ciphers

Example

- We use a multiplicative cipher to encrypt the message "hello" with a key of 7. The ciphertext is "XCZZU".

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

Question

- Give some problems related to modular multiplication when we use a modulus n=26, what are the conditions that the key K should satisfy in order to avoid such problems?
  - When we use n=26, some keys could generate encryption tables containing ambiguities (example K=13 or all even numbers like 8).
  - Solution: The key K should be co-prime with the modulus n.
- Finally, if we choose n=29, why K can take any value?
  - Because the modulus n=29 is prime. It is hence co-prime with all numbers that are less than 29.

Building Stronger Ciphers

Increasing the Key Space

Building stronger ciphers

- To combat **Brute force attack** we need:

  A very large key space

- To combat **Linguistic analysis benefits** we need:

  A weak association between the linguistic patterns in the plaintext and ciphertext

- So, two desirable **characteristics are required to build strong ciphers:**
  - **a very large key space**
  - **a weak association with the linguistic patterns in the plaintext.**

How ciphers can be designed to address these requirements?

Monoalphabetic Cipher

- **The Caesar cipher uses a monoalphabetic substitution.**
  - The key remains constant
  - For example, the plaintext letter ‘e’ will always be encrypted as the same ciphertext symbol.
  - This approach depend on shifting technique.
  - The ciphertext inherits the linguistic patterns of the plaintext
  - The ciphertext is susceptible to letter frequency and other linguistic analysis!

Monoalphabetic Cipher

- With only 25 possible keys, the Caesar cipher is far from secure.
- Because additive, and multiplicative ciphers have small key domains, they are very vulnerable to brute-force attack.
- A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.
- An example key for monoalphabetic substitution cipher

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

Monoalphabetic Cipher

- Monoalphabetic substitution cipher is similar to Caesar cipher but the replacement is random.
- a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.
- The key is changed for every message.
- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Before proceeding, we define the term permutation .
- A permutation of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once.
- For example, if S = {a, b, c}, there are six permutations of S : abc, acb, bac, bca, cab, cba
- In general, there are n ! permutations of a set of n elements, because the first element can be chosen in one of n ways, the second in n - 1 ways, the third in n - 2 ways, and so on.

```
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
```

- This will increase the possibilities to 26! (If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than $4 * 10^{26}$ possible keys).

Monoalphabetic Cipher

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

- Encrypt the message = "Root Sec" using monoalphabetic cipher given the key above

R	O	O	T	S	E	C
L	X	X	M	Z	W	F

Monoalphabetic Cipher

- Exercise: Decrypt the message = “LXXMZWF” using monoalphabetic cipher given the key above

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

Monoalphabetic Cipher

Example

- We can use the following key to encrypt the message "this message is easy to encrypt but hard to find the key"

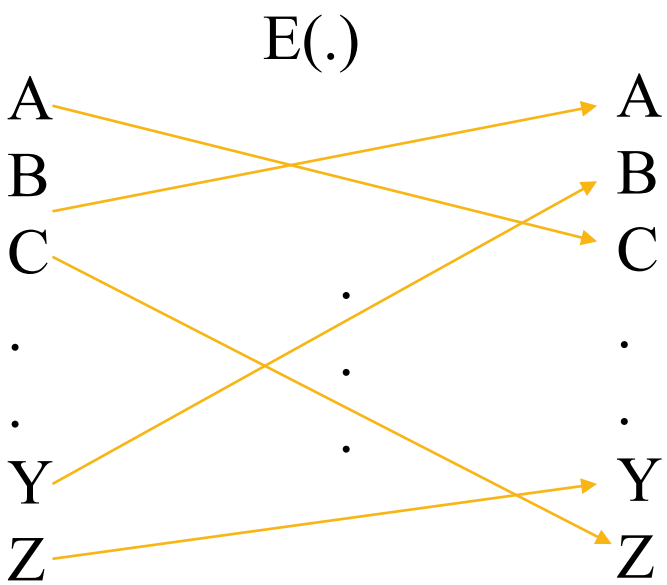
Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

- The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Each plaintext letter maps to a different random ciphertext letter



26! Possible transforms

Cryptanalysis of Monoalphabetic Cipher

- now have a total of $26! = 4 \times 10^{26}$ keys
- with so many keys, might think is secure
  - So, eliminate brute-force technique for cryptanalysis.
- Monoalphabetic is still vulnerable to Linguistic Analysis

Cryptanalysis of Monoalphabetic Cipher

- Given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- To analysis the cipher text you should follow the following steps:
- The relative frequency of the letters can be counted such as shown in the following table:
  - Calculate its relative frequencies: for letter Z occurrence = 14➔ frequency = 14/120 length of message *100% = 11.67

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								

Cryptanalysis of Monoalphabetic Cipher

- Compared to a standard frequency distribution for English

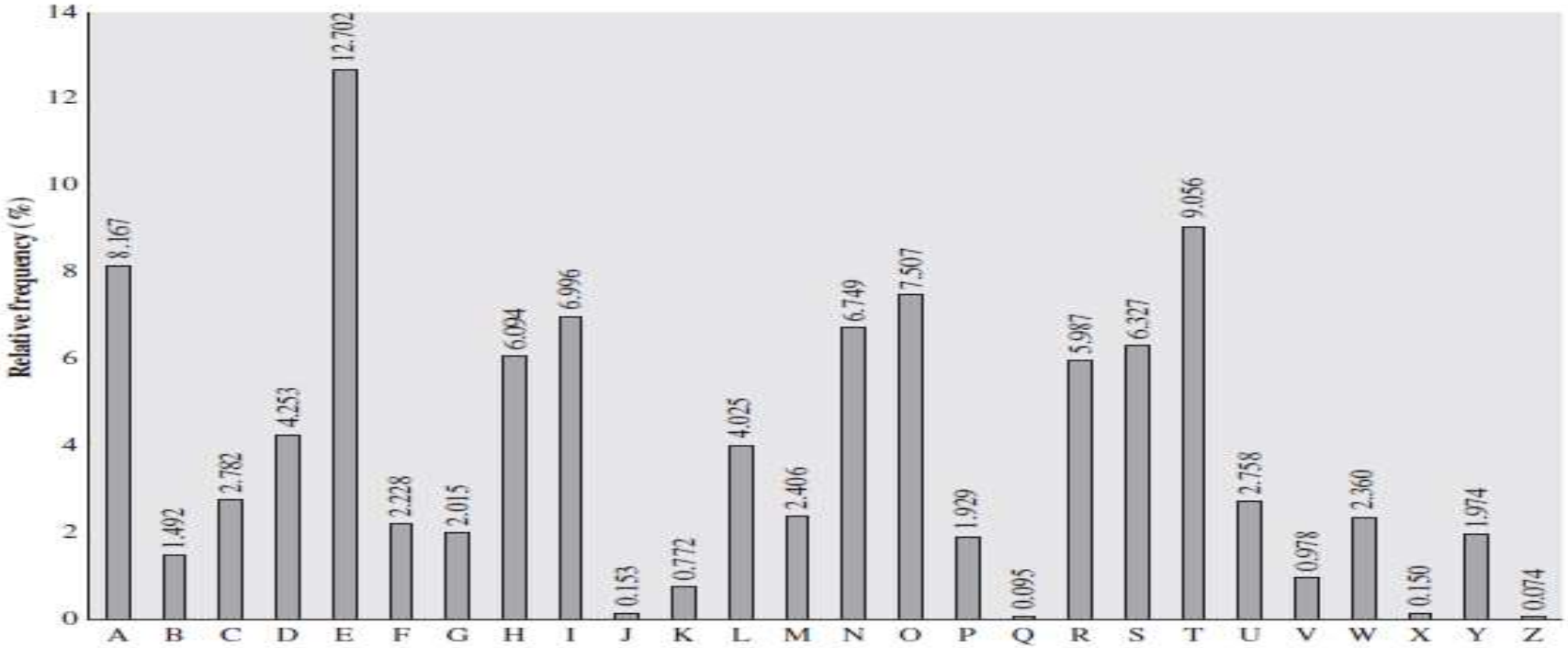


Figure 2.5 Relative Frequency of Letters in English Text

Cryptanalysis of Monoalphabetic Cipher

- Compared to a standard frequency distribution for English
  - One alphabet frequencies: Guess {P, Z} = {e, t}
  - The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}. The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.

U	Z	Q	S	O	V	U	O	H	X	M	O	P	V	G	P	O	Z	P	E	V	S	G	Z	W	S	Z	O	P	F	P	E	S	X	U	D	B	M	E	T	S	X	A	I	Z
	t											e			e		t	e					t			t		e		e														t
V	U	E	P	H	Z	H	M	D	Z	S	H	Z	O	W	S	F	P	A	P	P	D	T	S	V	P	Q	U	Z	W	Y	M	X	U	Z	U	H	S	X						
			e		t				t			t					e		e	e					e			t						t									
E	P	Y	E	P	O	P	D	Z	S	Z	U	F	P	O	M	B	Z	W	P	F	U	P	Z	H	M	D	J	U	D	T	M	O	H	M	Q									
	e			e		e		t		t			e				t		e			e	t																					

Cryptanalysis of Monoalphabetic Cipher

- look for other regularities. For example, certain words may be known to be in the text. Or we could look for repeating sequences of cipher letters and try to deduce their plaintext equivalents.
- A powerful tool is to look at the frequency of two-letter combinations, known as **digrams and trigrams**. In our ciphertext, the most
  - common digram is ZW, which appears three times. So we make the correspondence of Z with t and W with h. So, ZW is *th*
  - trigrams: frequencies of compound letters
  - The sequence ZWP ap[pears in the ciphertext, and we can translate that sequence as *the*
    - *So,* so guess ZW = th and hence ZWP = the
- Next, notice the sequence ZWSZ in the first line. We do not know that these four letters form a complete word, but if they do, it is of the form th_t. If so, S equates with a.

```
U Z Q S O V U O H X M O P V G P O Z P E V S G Z W S Z O P F P E S X U D B M E T S X A I Z
  t   a                 e     e   t e     a   t h a t   e   e   a               a       t

V U E P H Z H M D Z S H Z O W S F P A P P D T S V P Q U Z W Y M X U Z U H S X
      e   t       t a   t     a   e   e e     a   e     t h         t     a

E P Y E P O P D Z S Z U F P O M B Z W P F U P Z H M D J U D T M O H M Q
  e     e   e   t a t     e       t h e     e t
```

Cryptanalysis of Monoalphabetic Cipher

- Proceeding with trial and error

proceeding with trial and error finally get:

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

Weakening the linguistic association

How to decouple from the linguistic patterns of the plaintext?

Polyalphabetic Ciphers

- Polyalphabetic substitution cipher
  - Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:

- A set of related monoalphabetic substitution rules is used
- A key determines which particular rule is chosen for a given transformation

Polyalphabetic Ciphers

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

- **Example:** Use a polyalphabetic Cipher to encrypt the plaintext: 'Security' with a key rules as the following:
  - Shift first letter three positions to its right
  - Shift second letter five positions to its right
  - Shift third letter seven positions to its right
- Since we have three rules then the message is portioned into blocks 3 letters each.

Block 1:	s	e	c	→	V	J	J
Block 2:	u	r	i	→	X	W	P
Block 3:	t	y		→	W	D	

Plaintext	S	e	c	u	r	i	t	y
Key	K_1	K_2	K_3	K_1	K_2	K_3	K_1	K_2
	3	5	7	3	5	7	3	5
Ciphertext	**V**	**J**	**J**	**X**	**W**	**P**	**W**	**D**
VJJXWPWD								

Polyalphabetic Ciphers

- One way to do so is to encrypt with **a cipher that uses a succession of different keys.**
  - The **Vigenère cipher** provides an example of how this can be achieved.

Vigenère Cipher

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a

Vigenère Cipher

- **The Vigenère cipher** uses a key known as **a running key**, which is generated by a **keyword**.
- **Example:** Use the Vigenère cipher with the keyword 'jupiter' to encrypt the following sentence: "A stitch in time saves nine"
- **Solution:**
  - Using the convention of assigning a numerical value to each letter, 'jupiter' would produce a key sequence of 9, 20, 15, 8, 19, 4, 17.
  - This provides a succession of different keys that can be used over and over again in the same sequence.
  - Each symbol in the plaintext is encrypted using the next key in the sequence.

Vigenère Cipher

- **Example:** Use the Vigenère cipher with the keyword 'jupiter' to encrypt the following sentence: "A stitch in time saves nine
- **Solution:**
- The following Caesar Cipher's formula is used to determine the numerical code of the ciphertext of each letter:

$$c \equiv p + K \bmod 26$$

Where K takes sequentially the following values : {9, 20, 15, 8, 19, 4, 17}

plaintext	a	s	t	i	t	c	h	i	n	t	i	m	e	s	a	v	e	s	n	i	n	e
number equivalent	0	18	19	8	19	2	7	8	13	19	8	12	4	18	0	21	4	18	13	8	13	4
key	j	u	p	i	t	e	r	j	u	p	i	t	e	r	j	u	p	i	t	e	r	j
number equivalent	9	20	15	8	19	4	17	9	20	15	8	19	4	17	9	20	15	8	19	4	17	9
calculation result	9	12	8	16	12	6	24	17	7	8	16	5	8	9	9	15	19	0	6	12	4	13
ciphertext	J	M	I	Q	M	G	Y	R	H	I	Q	F	I	J	J	P	T	A	G	M	E	N

Vigenère Cipher- Encryption

Key	J	u	p	i	t	e	r																		
	k1	k2	k3	k4	k5	k6	k7																		
	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
K1	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
K2	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
K3	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
K4	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
K5	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
K6	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
K7	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
Plaintext	A	s	t	i	t	c	h	i	n	t	i	m	e	s	a	v	e	s	n	i	n	e				
Key	J	u	p	i	t	e	r	J	u	p	i	t	e	r	J	u	p	i	t	e	r	j				
Ciphertext	J	M	I	Q	M	G	Y	R	H	I	Q	F	I	J	J	P	T	A	G	M	E	N				

Vigenère Cipher- Decryption

	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
K1	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
K2	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
K3	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
K4	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
K5	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
K6	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
K7	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
Ciphertext	j	m	i	q	m	g	y	r	h	i	q	f	i	j	j	p	t	a	g	m	e	n				
Key	J	u	p	i	t	e	r	J	u	p	i	t	e	r	J	u	p	i	t	e	r	j				
Plaintext	a	s	t	i	t	c	h	i	n	t	i	m	e	s	a	v	e	s	n	i	n	e				

Vigenère Cipher

- Weakness of a Vigenère cipher:
  - Where similar letters appear at distances corresponding to the keyword length, their ciphertext letters will match each other!
    - For example, the letter pair 'ti' in the plaintext word 'stitch' and the letter pair 'ti' in 'time' are both encrypted as 'IQ'.

plaintext	a	s	t	i	t	c	h	i	n	t	i	m	e	s	a	v	e	s	n	i	n	e
number equivalent	0	18	19	8	19	2	7	8	13	19	8	12	4	18	0	21	4	18	13	8	13	4
key	j	u	p	i	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	p	i	t	e	r	j	u	p	i	t	e	r	j
number equivalent	9	20	15	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	15	8	19	4	17	9	20	15	8	19	4	17	9
calculation result	9	12	8	16	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	8	16	5	8	9	9	15	19	0	6	12	4	13
ciphertext	J	M	I	Q	M	G	Y	R	H	I	Q	F	I	J	J	P	T	A	G	M	E	N

7 steps= keyword length

Security of Vigenère Ciphers

- Weakness of a Vigenère cipher:
  - Given a large enough sample of ciphertext the probability of such an issue to appear increases
    - A cryptanalyst can hence determine the length of the running key '*n*'
    - Every *n*th symbol can then be treated and analyzed as one strand
    - The cipher can then be easily solved!
- To break Vigenere cipher:
  1. Try to guess the key length. How?
  2. If key length is N, the cipher consists of N Caesar ciphers. Plaintext letters at positions k, N+k, 2N+k, 3N+k, etc., are encoded by the same cipher.
  3. Attack each individual cipher as before.

Guessing the Key Length

- Main idea: Plaintext words separated by multiples of the key length are encoded in the same way.
- In our example, if plaintext = "…thexxxxxxthe…" then "the" will be encrypted to the same ciphertext words.
- So look at the ciphertext for repeated patterns.
- E.g. repeated "VTW" in the previous example suggests a key length of 3 or 9:

```
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- Of course, the repetition could be a random fluke.

Improve over Vigenère Cipher (1)

- Avoid repetition of key using Autokey cipher
- ideally want a key as long as the message
- Vigenère proposed the **autokey** cipher with keyword is prefixed to message as key knowing keyword can recover the first few letters use these in turn on the rest of the message
- but still have frequency characteristics to attack
- eg. given key *deceptive*

```
key:          deceptivewearediscoveredsav
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Playfair Cipher

Playfair Cipher

- one approach to improving security was to encrypt multiple letters the **Playfair Cipher** is an example invented by Charles Wheatstone, but named after his friend Baron Playfair
- The Playfair Cipher is the best-known multiple-letter encryption cipher
- The playfair algorithm is based on the use of a 5X5 matrix of letters constructed using a keyword
- The keyword MONARCHY will produce the following matrix:
  - fill in letters of keyword (remove duplicates)
  - fill rest of matrix with other letters

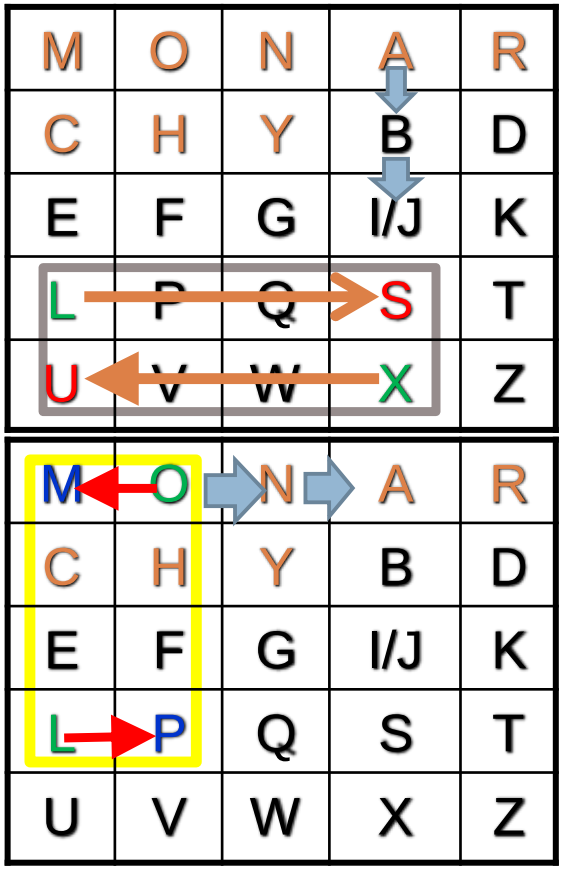
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Cipher

- To encrypt a message, one would break the message into digrams (groups of 2 letters), such that, for example, "**BALLOON**" becomes "**BA LL OO N**", and map them out on the key table.
- Then apply the following 4 rules, in order, to each pair of letters in the plaintext:
  1. If both letters are the same (or only one letter is left), add a filler like "X" after the first letter. Encrypt the new pair and continue. Example "BALLON" encrypts as "**BA LX LO ON**"
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), Example "**ar**" encrypts as "**RM**"
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), Example "**mu**" encrypts to "**CM**"
  4. otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg "hs" encrypts to "BP", and "ea" to "**IM**" or "**JM**" (as desired)
     - The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.
- To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s that do not make sense in the final message when finished).

Playfair Cipher-**Encryption**

- **Example:** Use the Playfair cipher with the keyword 'MONARCHY' to encrypt the plaintext: "BALLOON", The message will be " BA LX LO ON"
  - The pair **BA** is an column, replace it with **IB**. **Same column: shift-down**
  - The pair **LX** forms a rectangle, replace it with **SU**. **Intersection**
  - The pair **LO** forms a rectangle, replace it with **PM**. **Intersection**
  - The pair **ON** is in a row, replace it with **NA**. **Same row: shift-right**
- **The cipher text is: IBSUPMNA**



Playfair Cipher-**Decryption**

- **Example:** Use the Playfair cipher with the keyword 'MONARCHY' to decrypt the ciphertext: "IBSUPMNA", The message will be " IB SU PM NA"

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

- The pair **IB** is an column, replace it with **BA**. **Same column: shift-up**
- The pair **SU** forms a rectangle, replace it with **LX**. **Intersection**
- The pair **PM** forms a rectangle, replace it with **LO**. **Intersection**
- The pair **NA** is in a row, replace it with **ON**. **Same row: shift-lift**
- **The plain text is: balxloon**

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

Self Assessment

- Use the Playfair cipher with the keyword 'MONARCHY' to decrypt the ciphertext: "CFLXLO".

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

- The message will be " CF SU PM"

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 Cipher-**Decryption**

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

- The message will be " CF SU PM"

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

- The pair **CF** is an column, replace it with **he**. **Intersection** The pair **SU** forms a rectangle, replace it with **lx**. **Intersection**
- The pair **PM** forms a rectangle, replace it with **lo**. **Intersection**

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

- **The plain text is: helxlo = hello**

Security of the Playfair Cipher

- Equivalent to a monoalphabetic cipher with an alphabet of 26 x 26 = 676 characters (digrams).
- Security is much improved over the simple monoalphabetic cipher.
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- Was widely used for many decades
  - eg. by US & British military in WW1 and early WW2
- Actually, it **can** be broken, given a few hundred letters, because it still leaves some structure of plaintext intact.

An unbreakable cipher

One-Time Pad

- **The idea is to use a key that is identical in length to the plaintext, and to use it only once.**
  - Use a random key that is as long as the message so that the key need not be repeated
  - Key is used to encrypt and decrypt a single message and then is discarded
  - Each new message requires a new key of the same length as the new message
- Encryption based on this method is known as **one-time pad encryption.**
- **A One Time Pad Encryption:**
  1. A **random key** – **the pad** – is generated that is at least as long as the plaintext message
     - Two copies of the pad are required
       - one is used by the sender to encrypt the message.
       - one is used by the recipient to decrypt the message.
  2. Once it has been used both copies must be destroyed.

One-Time Pad

- This Scheme is unbreakable
  - Produces random output that bears no statistical relationship to the plaintext
  - Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code
- The random nature of the pad (key) means that:
  - The ciphertext has no linguistic association with the original plaintext
  - The ciphertext cannot be broken by analysis or brute force.

One-Time Pad

- **When properly applied, the one-time pad is the only known truly unbreakable cipher.**
  - One-time pads have been successfully used in the past, mostly for high-level diplomatic exchanges.
  - But a one-time pad is not a practical cipher for use in modern communication technologies.
- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
  - There is the practical problem of making large quantities of random keys
    - Any heavily used system might require millions of random characters on a regular basis
  - Mammoth key distribution problem
    - For every message to be sent, a key of equal length is needed by both sender and receiver
- Because of these difficulties, the one-time pad is of limited utility
  - Useful primarily for low-bandwidth channels requiring very high security

Transposition Cipher

Outline

- Transposition Ciphers
  - Rail Fence
  - Complete Square (Double Transposition)
  - Row Transposition
  - Columnar Transposition
  - Fixed Period

Transposition Cipher

- Definition: A Transposition Cipher is a cipher in which the plaintext message is rearranged systematically by some means agreed upon by the sender and receiver so that it can be decrypted.
  - In transposition ciphers, no new alphabet is created. The letters of the plaintext are just rearranged in some fashion… (e.g. shuffle the plaintext, without altering the actual letters used- Letters stay the same and the order is different.
- Also called **permutation** ciphers.
- All symbols are reordered according to a permutation specified by the key

Rail Fence Cipher

- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- **Example:** consider the message "meet me after the toga party" with a rail fence of depth 2, encrypt using Rail fence.
- The depth =2, it means we have tow rows.
- The plaintext is written down as in a sequence of diagonals (the first letter is written in 1st line, the 2nd letter is written in 2nd line, the 3rd letter is written in 1st line, the fourth is written in 2nd line and so on. a zig-zag pattern in two rows and form the ciphertext.
- Example: the plaintext: "Meet me after the toga party"

Rail 1	M		E		M		A		T		R		H		T		G		P		R		Y
Rail 2		E		T		E		F		E		T		E		O		A		A		T	

- Form the ciphertext by reading off the letters from the first row followed by the second row. Encrypted message is:

MEMATRHTGPRYETEFETEOAAT

Rail Fence Cipher

- To decipher a rail fence cipher, we divide the ciphertext in half (or divide by the depth) and reverse the order of the steps of encipherment, that is, write the ciphertext in two rows and read off the plaintext in zig-zag fashion. (Note: if there are an odd number of letters, the first row has one more letter than the second)

Rail Fence Cipher

- **Example:** Decipher the message "MEMATRHTGPRYETEFETEOAAT"
- The number of letters for the ciphertext is 23
- 23/2 = 11 and remainder =1. So, every row will have 11 letters, and the remainder will be added to first row.
- Then the first row has 12 and second row has 11 letters
- write the ciphertext in two rows

M		E		M		A		T		R		H		T		G		P		R		Y	
	E		T		E		F		E		T		E		O		A		A		T		

- Read off the plaintext in zig-zag fashion.

  MEET ME AFTER THE TOGA PARTY

- Count the letters in ciphertext "MEMATRHTGPRYETEFETEOAAT" = 23.
- This mean going to need a grid with 2 rows and 23 columns
- The first letter of the ciphertext in the top left of the grid and draw dashes in a zig-zag fashion to indicate where the other letters will go replace each of the dashes in the top row with letters from the ciphertext until all dashes in the top row of being replaced as follows:

Rail 1	M		-		-		-		-		-		-		-		-		-		-	
Rail 2		-		-		-		-		-		-		-		-		-		-		-

- Now, go replace each of the dashes in the top row with letters from the ciphertext until all dashes in the top row of being replaced as follows:

Rail 1	M		E		M		A		T		R		H		T		G		P		R		Y
Rail 2		-		-		-		-		-		-		-		-		-		-		-	

- Now, replace the dashes in the second row with the rest of the ciphertext as follows:

Rail 1	M		E		M		A		T		R		H		T		G		P		R		Y
Rail 2		E		T		E		F		E		T		E		O		A		A		T	

- Now, you can read off the message in a zig-zag fashion "meet me after the toga party"

Rail Fence Cipher

- **Example:** to send the message "Meet me at the park" to Bob, Alice writes

m ↘ e ↗ e ↘ t ↗ m ↘ e ↗ a ↘ t ↗ t ↘ h ↗ e ↘ p ↗ a ↘ r ↗ k

- She then creates the ciphertext
  "MEMATEAKETETHPR"

Rail Fence Cipher

Example: consider the message "we are discovered flee at once" with a rail fence of depth 3, encrypt using Rail fence.

```
w - - - e - - - c - - - r - - - l - - - t - - - e
 - e - r - d - s - o - e - e - f - e - a - o - c -
 - - a - - - i - - - v - - - d - - - e - - - n - -
```

The message:

WECRL TEERD SOEEF EAOCA IVDEN

WECRL TEERD SOEEF EAOCA IVDEN

Rail 1	W				-				-				-				-				-			
		-		-		-		-		-		-		-		-		-		-		-		
			-				-				-				-				-				-	

Rail 1	W				E				C				R				L				T				E
		-		-		-		-		-		-		-		-		-		-		-		
			-				-				-				-				-				-	

Rail 1	W				E				C				R				L				T				E
Rail 2		E		R		D		S		O		E		E		F		E		A		O		C	
			-				-				-				-				-				-		

Rail 1	W				E				C				R				L				T				E
Rail 2		E		R		D		S		O		E		E		F		E		A		O		C	
Rail 3			A				I				V				D				E				N		

Rail Fence Cipher

Example: consider the message "we are discovered flee at once" with a rail fence of depth 3, encrypt using Rail fence.

w			r			i			o			r			f			e			o			e
	e			e			s			v			e			l			a			n		
		a			d			c			e			d			e			t			c	

The message:

WRIORFEOEEESVELANADCEDETC.

Rail Fence Cipher (Home Work)

Example: consider the ciphertext
"WRIORFEOEEESVELANADCEDETC".

with a rail fence of depth 3, decrypt using Rail fence.

WRIORFEOE EESVELAN ADCEDETC

Columnar Transposition Cipher

- Plain text: meet me after the toga party
- Key = “cipher”
- Create matrix the number of columns equal the length of key.
- Write the key in the 2nd row and in the first row write the alphabetic order for the key
- Write the plain text in the matrix from 3rd row, row by row and fill the empty cell with letter used frequently like “e”
- Write the cipher text column by column based on the order of the key

Columnar Transposition Cipher

- Matrix

Plain text: meet me after the toga party
Key = "cipher"

1	4	5	3	2	6
c	i	p	h	e	r
m	e	e	t	m	e
a	f	t	e	r	t
h	e	t	o	g	a
p	a	r	t	y	E

- Read col 1, 2, 3 , 4, 5 and 6
- Mahp mrgy teot efea ettr etae.

Columnar Transposition Cipher

- **Example:** Message: EVLNA CDTES EAROF ODEEEC WIR
- Key: STRIPE

5	6	4	2	3	1
s	t	r	i	p	e
e	v	l	n	a	c
d	t	e	s	e	a
r	o	f	o	d	e
e	e	c	w	i	r

Cipher text: caer nsow aedi lefc edre vtoe

Columnar Transposition Ciphers

- Is a more complex transposition
- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
- **Example:** Plaintext : "attack postponed until two am" and the key: 4312567
  - The order of the columns then becomes the key to the algorithm
  - Plaintext is written row by row in a rectangle.

Key:
Plaintext:

4	3	1	2	5	6	7
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

- To encrypt, write out the columns in an order specified by a key.
- Start with the column that is labelled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labelled 2, then col 2, then col 1 then col 5,6 and 7.

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Columnar Transposition Ciphers

- **Example:** Ciphertext: "**TTNAAPTMTSUOAODWCOIXKNLYPETZ**" and the key: 4312567
- The number of columns is the key information. The number of columns is 7
- The length of ciphertexet is 28
- Then the letters will fill nDIVk full rows = 28/7 = 4 rows, then distribute the ciphertext on 7 columns in an order specified by a key.

TTNA	APTM	TSUO	AODW	COIX	KNLY	PETZ
Col 1	**Col 2**	**Col 3**	**Col 4**	**Col 5**	Col 6	Col 7

4	3	1	2	5	6	7
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

- Transcribing row-by-row will then yield the plaintext.

Attakp ostpone duntilt woamxyz

Attak postponed until two am xyz

Columnar Transposition Ciphers

Key:
Plaintext:

4	3	1	2	5	6	7
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			

- To encrypt, write out the columns in an order specified by a key.
- Start with the column that is labelled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labelled 2, then col 2, then col 1 then col 5,6 and 7.

Ciphertext: **TTNAAPTMTSUOAODWCOIKNLPET**

Columnar Transposition Ciphers

- **Example:** Ciphertext: "**TTNAAPTMTSUOAODWCOIKNLPET**" and the key: 4312567
- The number of columns is the key information. The number of columns is 7
- The length of ciphertexet is 25
- Then the letters will fill nDIVk full rows = 25/7 = 3 rows, then distribute the ciphertext on 7 columns in an order specified by a key.

TTNA	APTM	TSUO	AODW	COI	KNL	PET
Col 1	**Col 2**	**Col 3**	**Col 4**	**Col 5**	Col 6	Col 7

4	3	1	2	5	6	7
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			

- Transcribing row-by-row will then yield the plaintext.

Attackp ostpone duntilt woam

Attack postponed until two am

Columnar Transposition Ciphers

- **Note about decryption:**
- In general, given a simple columnar transposition with total letters (n) and columns (c), we use the division algorithm to divide by to compute to determine the number of letters in each column that make up the transposition.
  - There are n/c full rows if the remainder is 0,
  - Else, there are $n/c + 1$ rows, with the first r columns have (or contain) $c/n + 1$ entries (letters), each for a total of $r(n/c + 1$ letters.
  - The remaining $c - r$ columns have n/c letters in each column for a total of $(\mathrm{c} - \mathrm{r}) * (\frac{\mathrm{n}}{\mathrm{c}})$ total letters

Columnar Transposition Ciphers - Decryption

Example: Suppose a simple columnar transposition is made up of 25 total letter distributed over 7 columns. Determine the number of letters in each column that make up the transposition.

- 25/7= 3 and the remainder (r) = 4 ≠ 0
- Then there are 25 / 7 + 1 = 4 rows. The first 4 (r) columns contain (25/7+1)=4 letters in each column for a total of 16 letters.
- The remaining (c-r)= 7- 4 = 3 columns have (n/c)= 25/7=3 letters in each column for a total of 9 letters (i.e. the last row will have 3 letters in it- and the first 4 columns will each have 4 letters, and the last 3 columns will have 3 letters).

Self Assessment

Decrypt the "**MITYESUSARAVYUNI**" by using **Row Transposition Ciphers**, if the key is "**361524**". **(3 Points)**

Self Assessment

- Answer:
  - Cipher text: **MITYESUSARAVYUNI** = 16 letters
  - key= 361524 d= 6 (i.e., length)
  - The number of columns is the key information. The number of columns is 6
  - The length of cipher texet is 16
  - Then the letters will fill nDIVk full rows = 16/6 = 2 rows. This mean we have 2 rows are full (i.e. each row contains 6 letters) for a total of 12 letters
  - 16/6 = 2.66 → This mean we have 2 rows are full (i.e. each row contains 6 letters) for a total of 12 letters
  - The last row will contain 4 letters.
  - Then distribute the ciphertext on 6 columns in an order specified by a key, where the first 4 columns will be 3 letters and the last 2 columns will be 2 letters
  - Cipher text: write letter as the key 361524: column 3→3 letters, column 6 → 3 letters, column 1 → 3 letters, column 5 → 3 letters, column 2 → 2 letters and then column 4 → 2 letters

Self Assessment

"**MITYESUSARAVYUNI**
key= 361524

MIT	YE	SUS	RA	AVY	UNI
Col 1	Col 2	Col 3	Col 4	Col 5	Col 6

3	6	1	5	2	4
S	U	M	A	Y	A
U	N	I	V	E	R
S	I	T	Y		

- Read plain text row by row Cipher text: **sumaya university**

Home Work

Example: Suppose a simple columnar transposition is made up of 50 total letter distributed over 9 columns. Determine the number of letters in each column that make up the transposition.

Row Transposition Ciphers

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed

Row Transposition Ciphers

1. The sender and receiver **agree on a codeword** and **a way to reorder the letters** in the keyword into an anagram.
   - **For example**: Suppose the code word is **Tuesday** and the agreed transposition is:
     - to reverse the order of the letters (**YADSEUT**)
     - then swap pairs of letters, starting at the right-hand end to produce the anagram **YDAESTU**.
   - The number of letters in the keyword dictates the number of columns in the matrix
2. The plaintext is entered into each of the columns (with the keyword at the top) a letter at a time working across the rows.
3. Any empty places in a row can be padded with redundant letters (the 'x' in the chosen example).
4. The columns are then reordered according to the keyword anagram.
5. The ciphertext is given by reading back the letters from the reordered matrix.

Row Transposition Ciphers

Example: The sender and recipient agreed to use the keyword "tuesday" and its anagram "YDAESTU" to encrypt the following message using columnar transposition cipher: "Mary had a little lamb its fleece was white as snow".

What the ciphertext from this message?

(a) First stage

T	U	E	S	D	A	Y
m	a	r	y	h	a	d
a	l	i	t	t	l	e
l	a	m	b	i	t	s
f	l	e	e	c	e	w
a	s	w	h	i	t	e
a	s	s	n	o	w	x

(b) Second stage

Y	D	A	E	S	T	U
D	H	A	R	Y	M	A
E	T	L	I	T	A	L
S	I	T	M	B	L	A
W	C	E	E	E	F	L
E	I	T	W	H	A	S
X	O	W	S	N	A	S

The resulting ciphertext is:

"DHARYMAETLITALSITMBLAWCEEEFLEITWHASXOWSNAS"

Row Transposition Ciphers

Example: The sender and recipient agreed to use the keyword- Key (r) "25413" and its anagram - k(w) = 41532 to encrypt the following message using columnar transposition cipher: "Thesimplestpossibletranspositionsxx".

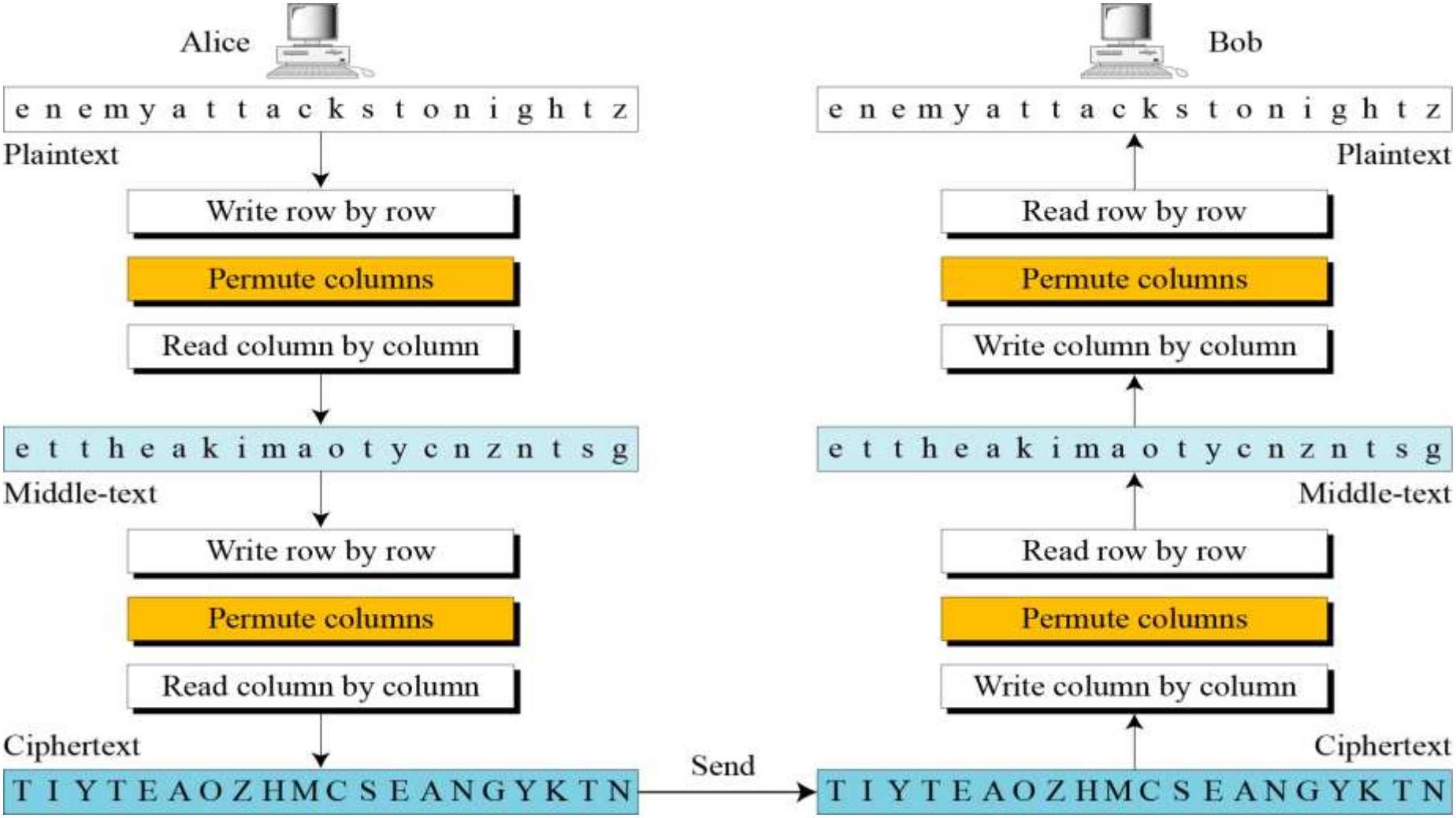
What the ciphertext from this message?

First Stage

Col #	1	2	3	4	5
Key (R)	2	5	4	1	3
	t	h	e	s	i
	m	p	l	e	s
	t	p	o	s	s
	i	b	l	e	t
	r	a	n	s	p
	o	s	i	t	i
	o	n	s	x	x

Second Stage

Key (W)	4	1	5	3	2
	S	T	I	E	H
	E	M	S	L	P
	S	T	S	O	P
	E	I	T	L	B
	S	R	P	N	A
	T	O	I	I	S
	X	O	X	S	N

The resulting ciphertext is: **"STIEH EMSLP STSOP EITLB SRPNA TOIIS XOXSN"**

Double Transposition Cipher