Cryptography and Network Security Chapter 2

- Fifth Edition
  by William Stallings
- Lecture slides by
  Lawrie Brown

Classical Ciphers

Arabic Language Audio Comments by
Prof. Mohamed Ashraf Madkour

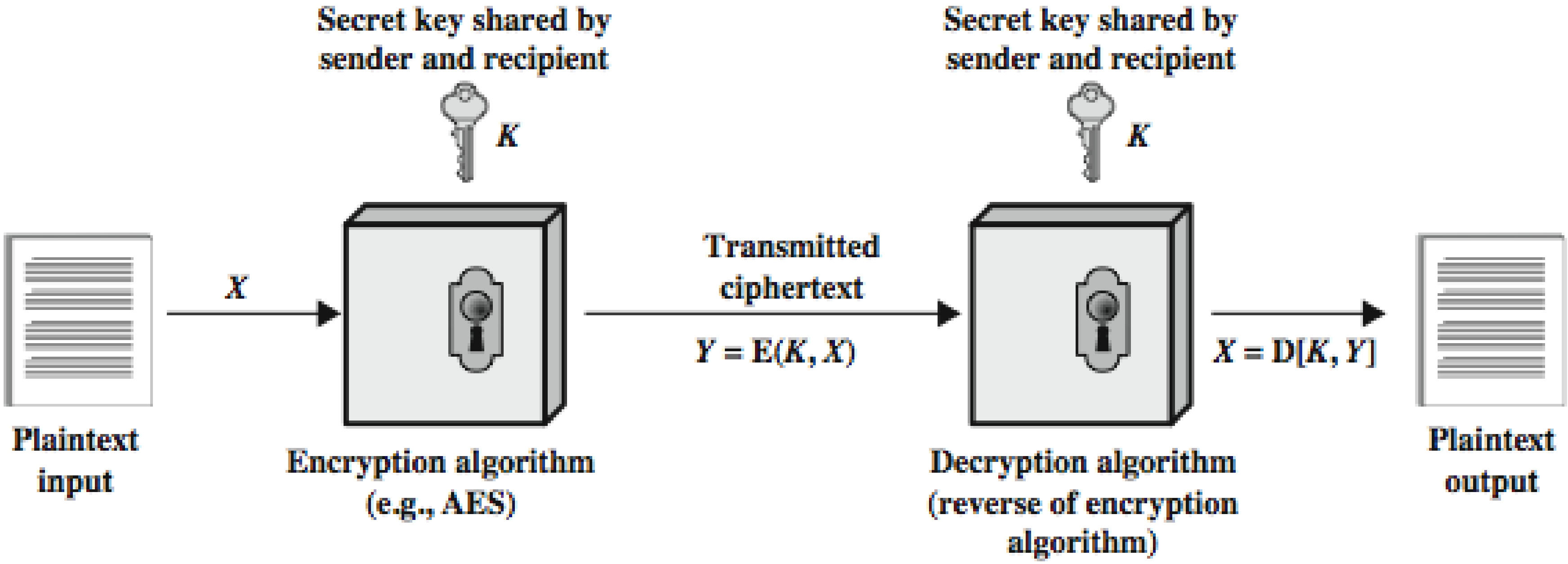
Symmetric Encryption

- Other names are conventional / private-key / single-key
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- Was only type prior to invention of public-key in 1970’s
- Symmetric encryption is by far most widely used

Some Basic Terminology

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

Symmetric Cipher Model



Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = \mathrm{E}(K, X)$

  $X = \mathrm{D}(K, Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- can characterize cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - Product = substitution + transposition
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Cryptanalysis

objective to recover key not just message

general approaches:

- cryptanalytic attack
- brute-force attack

if either succeed all future and past messages encrypted with the broken key are compromised

Cryptanalytic Attacks

- **ciphertext only** *{This is the **most difficult** problem}*
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext** *{Generally, an encryption algorithm is designed to withstand a known-plaintext attack}*
  - Know both plaintext & ciphertext of some random message
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text** *{This is the **least difficult** problem}*
  - select plaintext or ciphertext to encrypt/decrypt

More Definitions

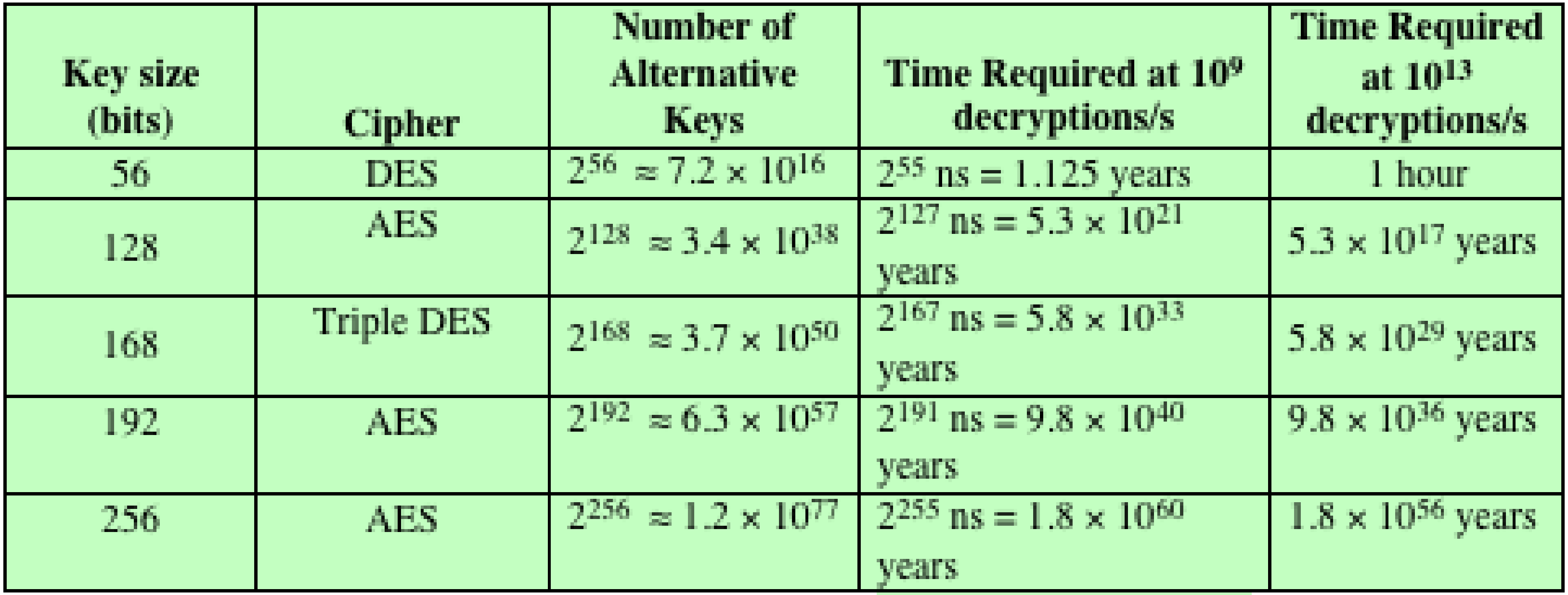
- **unconditional security**
  - no matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **computational security**
  - given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

Brute Force Search

T = Average Time Required for Exhaustive Key Search

{“T” depends on the speed of the computer used for decrypting; i.e. how many decryptions/second can be done on a given ciphertext using all possible keys}

- ➢ always possible to simply try every key
- ➢ most basic attack, proportional to key size
- ➢ assume either know / recognise plaintext



Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Classical Substitution Ciphers

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example: *{for convenience we use lower-case letters for plaintext , and upper-case letters for ciphertext}*

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

{This is the simplest monoalphabetic cipher}

- 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

- then have Caesar cipher as:

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

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

c: number representing ciphertext letter.
p: number representing plaintext letter.
k: numeric key from 0 to 25.

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers A maps to A,B,..Z {i.e. k from 0 to 25}
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters {all values of k}
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Polyalphabetic Ciphers

One way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is **polyalphabetic substitution cipher.** A simple example for polyalphabetic ciphers is the ***VIGEN`ERE cipher.***

VIGEN`ERE CIPHER

This is the best-known, and one of the simplest polyalphabetic ciphers. This scheme depends on using a set of Caesar ciphers each with a different shift value from 0 to 25.

The algorithm of the Vigenère cipher is explained by the next example in which Caesar cipher is used 4 times, each time with a different shift value; namely: 2, 14,12,4.

Example to illustrate the algorithm of the VIGEN`ERE CIPHER

{This example uses Caesar Cipher repeatedly to encrypt the plaintext characters each time with a different shift value as follows: 2, 14,12, 4, 2, 14, 12, 4, 2,…}

Key word: “COME”

Simply, this key is equivalent to the sequence {2, 14, 12, 4}.

Plaintext: doyouunderstand

Ciphertext: FCKSWIZHGFEXCBP

Key	C	O	M	E	C	O	M	E	C	O	M	E	C	O	M
Numeric Value	2	14	12	4	2	14	12	4	2	14	12	4	2	14	12

index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Original Message	D	O	Y	O	U	U	N	D	E	R	S	T	A	N	D
Numeric Value	3	14	24	14	20	20	13	3	4	17	18	19	0	13	3

index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Numeric Value	5	2	10	18	22	8	25	7	6	5	4	23	2	1	15
Encrypted Message	F	C	K	S	W	I	Z	H	G	F	E	X	C	B	P

Another Example of Vigenère Cipher

- To encrypt a message, a key is needed that has the same number of characters as the message.
- Usually, the key is a repeating keyword.
- For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as:

key:	deceptivedeceptivedeceptive
plaintext:	wearediscoveredsaveyourself
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenère Autokey System

- A keyword is concatenated with the plaintext itself to provide a running key
- Example:

  key: deceptivewearediscoveredsav

  plaintext: wearediscoveredsaveyourself

  ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA
- Even this scheme is vulnerable to cryptanalysis
  - Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long; a key example is shown below

```
Plain:   abcdefghijklmnopqrstuvwxyz
Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN
```

- the following is a plaintext and the encrypted ciphertext using the given key

```
Plaintext:   ifwewishtoreplaceletters
Ciphertext:  WIRFRWAJUHYFTSDVFSFUUFYA
```

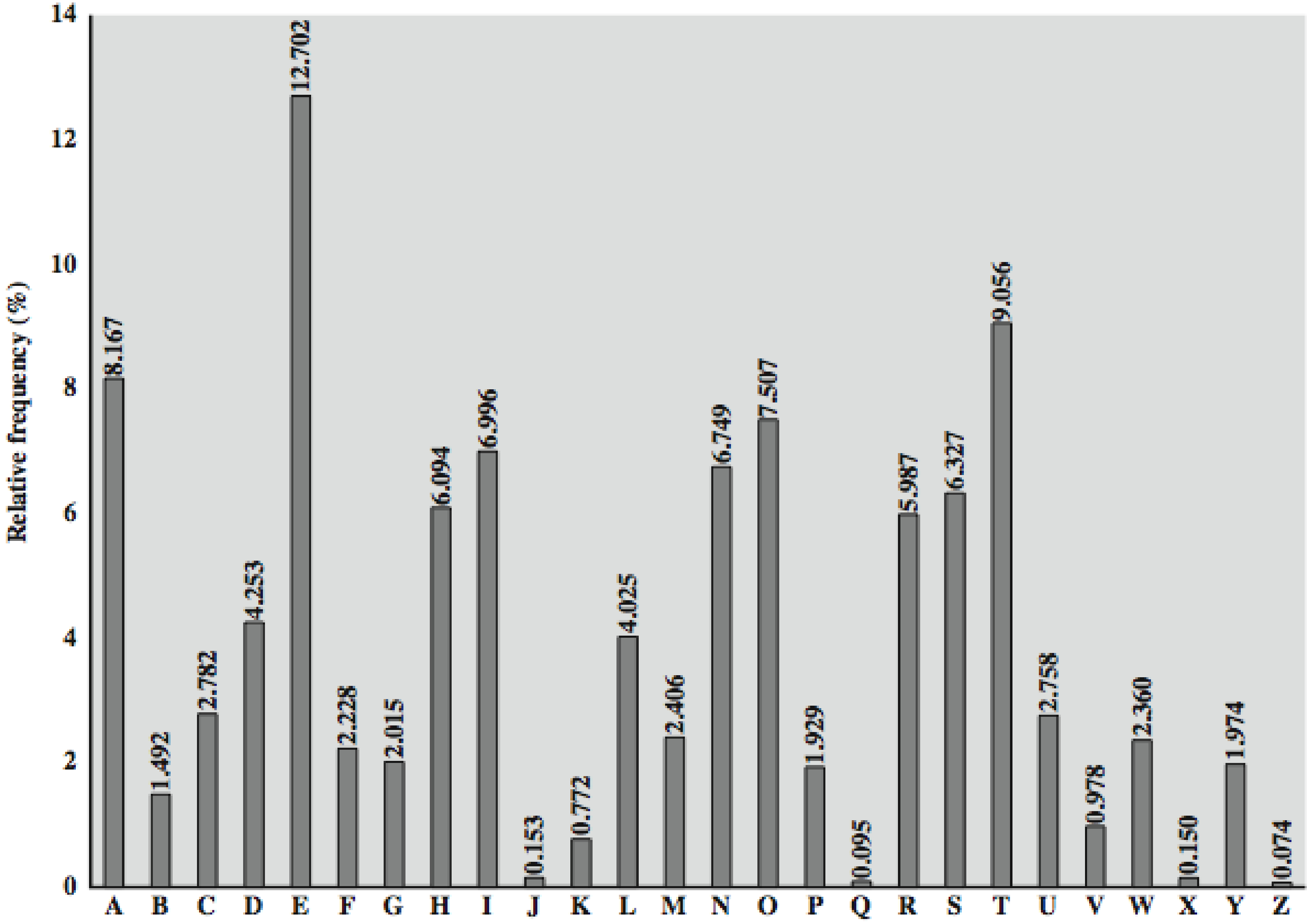
Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10^{26} keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Language Redundancy and Cryptanalysis

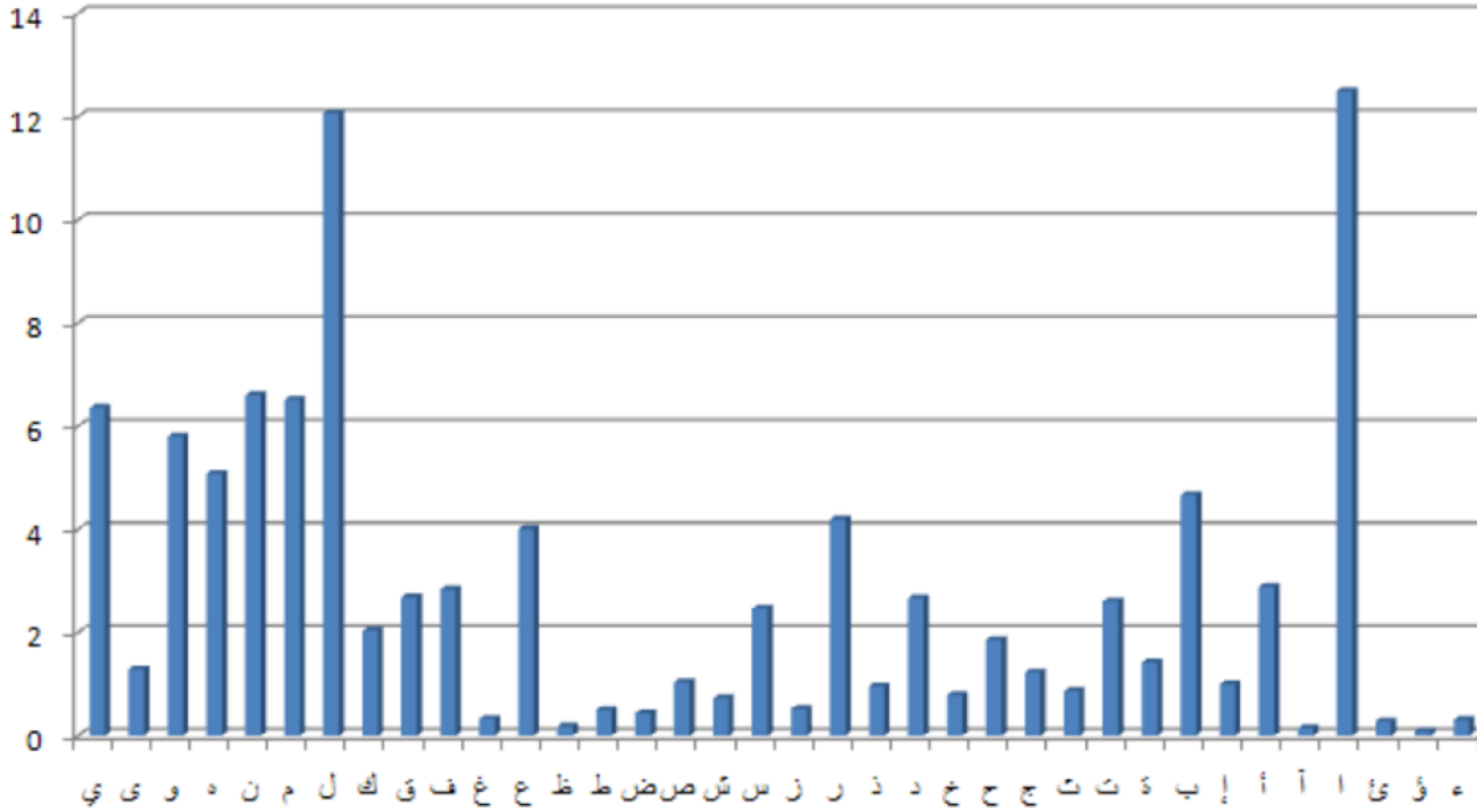
- human languages are **redundant** *{we don't actually need all the letters in order to understand written English text}*
- letters are not equally commonly used
- in English E is by far the most common letter, followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Arabic Letter Frequencies

(Relative frequency percent)



Use in Cryptanalysis

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help

Example Cryptanalysis

- given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- 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

One-Time Pad

- if a truly random key having the same length as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though there areproblems in generation & safe distribution of key
- is useful primarily for low-bandwidth channels requiring very high security.

One-Time Pad: Encryption

For simplicity, we will consider a language containing only 8 letters. So, we need only 3 bits to represent each letter.

e=000 w=001 i=010 k=011 l=100 m=101 s=110 p=111

Encryption: Plaintext ⊕ Key = Ciphertext

	w	e	i	l	w	i	p	l	e	m
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	m	l	w	s	s	p	w	s	m

One-Time Pad: Decryption

e=000 w=001 i=010 k=011 l=100 m=101 s=110 p=111

Decryption: Ciphertext ⊕ Key = Plaintext

	s	m	l	w	s	s	p	h	s	m
Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	001	000	010	100	001	010	111	100	000	101
	w	e	i	l	w	i	p	l	e	m

One-Time Pad Summary

- **Provably** secure
  - Ciphertext provides **no** information about plaintext
  - All plaintexts are equally likely
- BUT only when be used correctly
  - Pad must be random, used only once
  - Pad is known only to sender and receiver
- Note: pad (key) is same size as message
- So, why not distribute message instead of pad?

  {Answer: key may be distributed before message becomes ready}

Transposition Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text

Row Transposition Ciphers

(Encryption example)

- This is a complex transposition algorithm
- Write letters of message out in rows over a specified number of columns
- Then reorder the columns according to some key before reading off the rows
- Example: consider a 7-digit key (digits from 1 to 7 are arranged in any required order) as follows

Key: 4312567

Column Out	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

Row Transposition Ciphers

(Decryption of the previous example)

- Step 1: count the number of letters in the ciphertext (this is 28 in the given example), and divide it by the number of digits in the key (this is 7) to get the number of letters in each column (that is: 28/7=4)
- Step 2: arrange the ciphertext into 7 groups each contains 4 letters as follows

  Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
- Step 3: write the key in a horizontal row and place the first 4 letters in the ciphertext vertically under the digit 1 of the key.
- Step 4: similarly place the second group under the digit 2 of the key, and so on until placing the last group under the digit 7
- Step 5: read the plaintext horizontally.

Key: 4312567

Decrypted 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**

Product Ciphers

A substitution followed by a transposition

- ciphers using substitutions or transpositions are not secure because of language characteristics
- hence consider using several ciphers in succession to make harder, but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- this is bridge from classical to modern ciphers

Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few information bits
- advantage:
  - it can obscure encryption use
  - messages can be exchanged without being noticed
- a message can be first encrypted and then hidden using steganography.

Summary

- have considered:
  - classical cipher techniques and terminology
  - monoalphabetic and polyalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - transposition ciphers
  - product ciphers
  - steganography