Classical Ciphers (CS-452)

Week 2

- This class
  - Chapter 2 Symmetric Encryption
    - Substitution ciphers
    - Transposition ciphers

Basic Terminology

Some Basic Terminology

- Plaintext: original message
- Ciphertext: coded message
- Enciphering (encryption): converting plaintext to ciphertext
- Deciphering (decryption): restoring the plaintext from ciphertext
- Cryptography: the area of study of encryption principles/methods
- Cipher: an algorithm for performing encryption
- Cryptanalysis: the area of study of principles/ methods of deciphering ciphertext without knowing key – breaking the cipher

Some Basic Terminology

- Cryptology: areas of cryptography and cryptanalysis together
- Secret key: the input of encryption algorithm. The key is independent of the plaintext and the algorithm

Cryptography

- Cryptographic system is characterized by:
  - The type of encryption operations used
    - Substitution: each element (a bit or a letter) in the plaintext is mapped into another element
    - Transposition: elements in the plaintext are rearranged.
    - Product: multiple stages of substitutions and transpositions
  - The number of keys used
    - Symmetric, Single-key encryption
    - Asymmetric, Two-key or Public-key encryption
  - The way in which plaintext is processed
    - Block: process one block of elements at a time, producing an output block for each input block
    - Stream: process the input elements continuously, producing one element at a time.

Cryptanalysis

- Objective of attacking an encryption system: recover key rather than simply to recover the plaintext of a single ciphertext.
- General approaches:
  - Cryptanalytic attack:
    - Rely on the nature of the algorithm + some knowledge of the plaintext (e.g. English or French) or some sample plaintext-ciphertext pairs.
  - Brute-force attack
    - Try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Cryptanalysis

- Objective of attacking an encryption system: recover key rather than simply to recover the plaintext of a single ciphertext.
- General approaches:
  - Cryptanalytic attack:
    - Rely on the nature of the algorithm + some knowledge of the plaintext (e.g., English or French) or some sample plaintext-ciphertext pairs.
  - Brute-force attack
    - Try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Cryptanalysis

- Types of cryptoanalytic attacks:
  - Ciphertext-only:
    - Attacker only has access to the ciphertext.
    - Attempts to use statistical techniques to discover the key and/or plaintext.
  - Known-plain text attack:
    - Attacker has access to the ciphertext and knows some properties of the plaintext
    - Example: the plaintext is known to contain a certain sentence.
  - Chosen-plaintext attack:
    - Attacker can encrypt any plaintext using the target encryption scheme
    - Uses analysis in order to figure out the function of the cryptographic system (and hopefully the secret key!).

A Brief History of Cryptography

Egypt 1900 BC: Beginnings of Cryptography

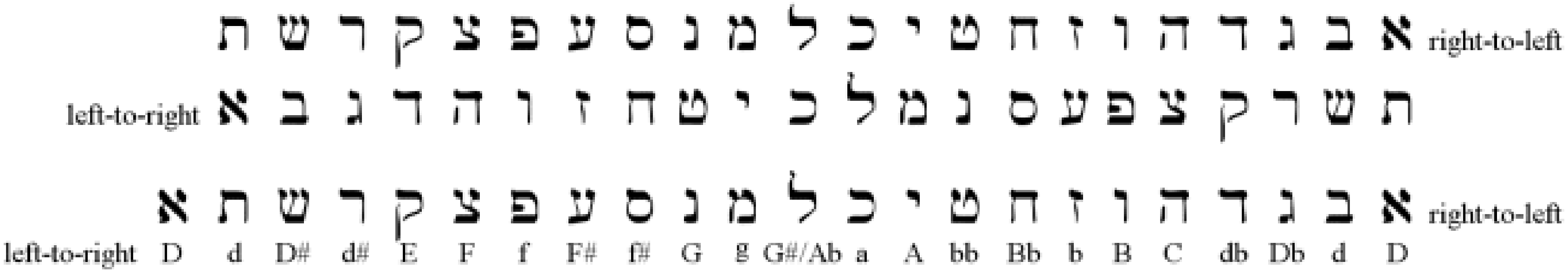
- Earliest known example of cryptography.
- Writing on the tomb wall of Egyptian nobleman Khnumhotep II.
- A story of the nobleman's life written using non-standard hieroglyphs.

Mesopotamia 1500 BC: Commercial use of Cryptography?

- Clay tablets discovered from Mesopotamia River contained an encrypted commercially valuable pottery glazing recipe.

Hebrews 500 - 600 B.C.: Atbash Cipher

- The last letter of the alphabet is replaced by the first, and vice versa, was used.
  - Example: A is replaced with Z, B with Y, etc.
- Example: Bible: Jeremiah 25:26 is believed to be written in Atbash:
  - "The king of Sheshach shall drink after them" - Sheshach meaning Babylon in Atbash (ששך=בבל).



א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת right-to-left

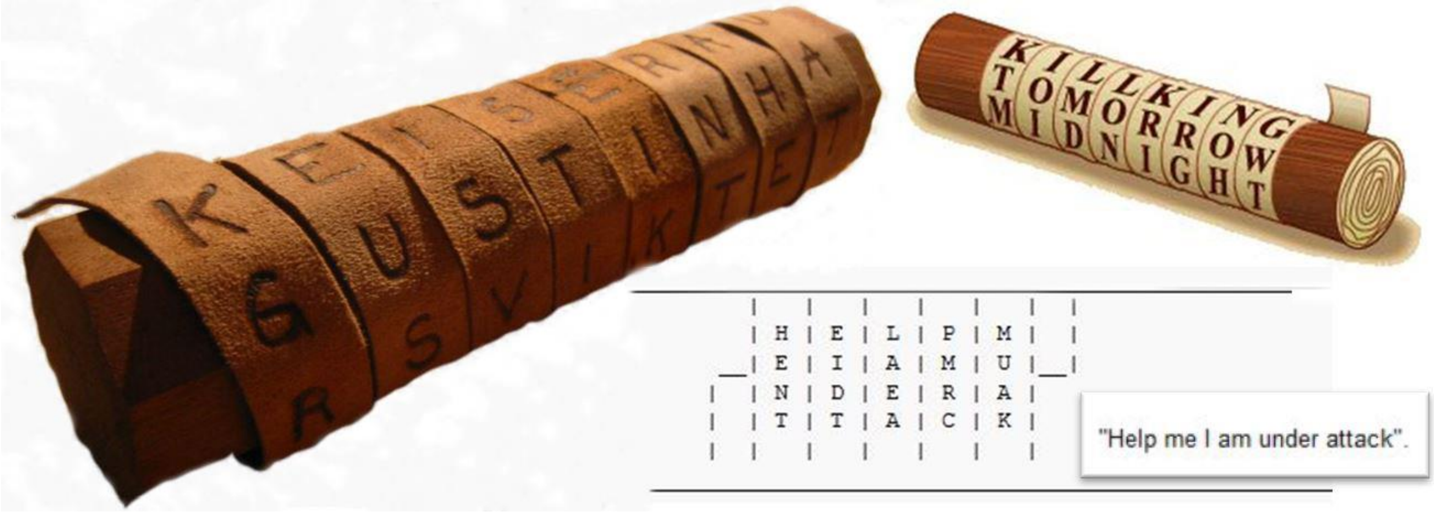
left-to-right א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת א right-to-left

left-to-right D d D# d# E F f F# f# G g G#/Ab a A bb Bb b B C db Db d D

Greece 500 BC: Scytale Cipher

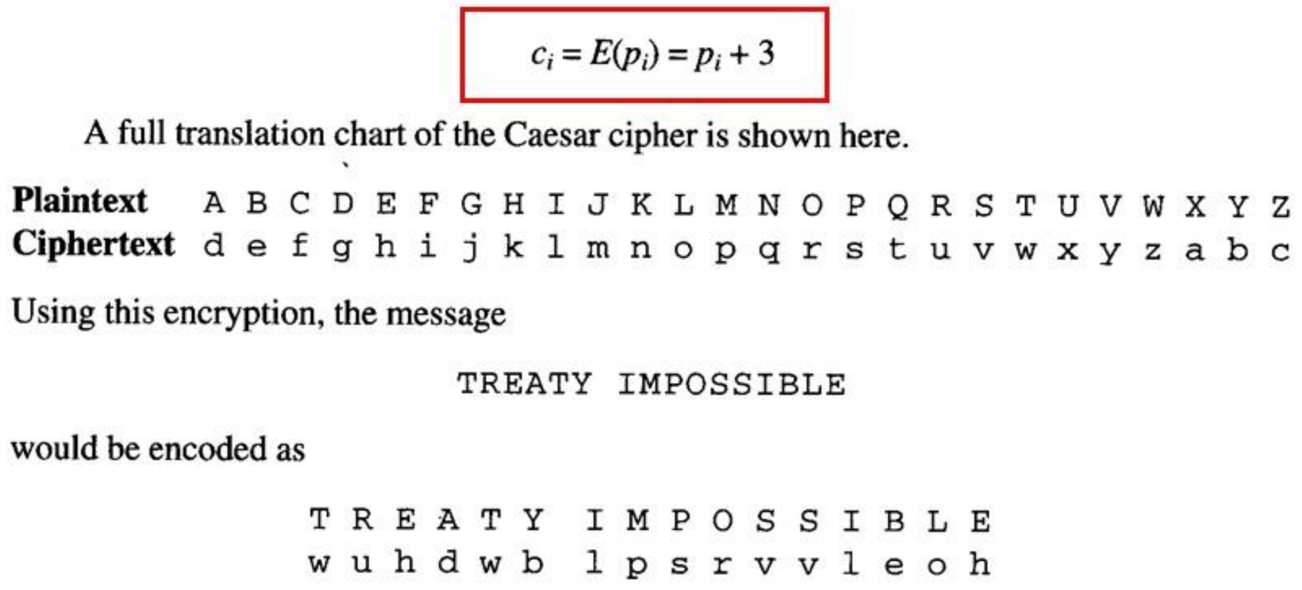
- Used by ancient Greek warriors.
- Messages written down along the length of the papyrus sheet wrapped around the staff.
    - Encryption: unwrap the sheet.
    - Decryption: wrapped the papyrus around a staff of equal diameter.
- Example of a transposition cipher: encipherment by rearranging the elements of the plaintext.



"Help me I am under attack".

Rome ~100 – 44 BC: Caesar Cipher

- Used by emperor Julius Caesar to convey secret messages to his army generals on the front-lines.
  - Was a major advantage for Romans during wars
  - Encryption: Each letter is shifted forward by an agreed upon amount.
  - Decryption: Each letter shifted backward by an agreed upon amount.



$$\boxed{c_i = E(p_i) = p_i + 3}$$

A full translation chart of the Caesar cipher is shown here.

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	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

Using this encryption, the message

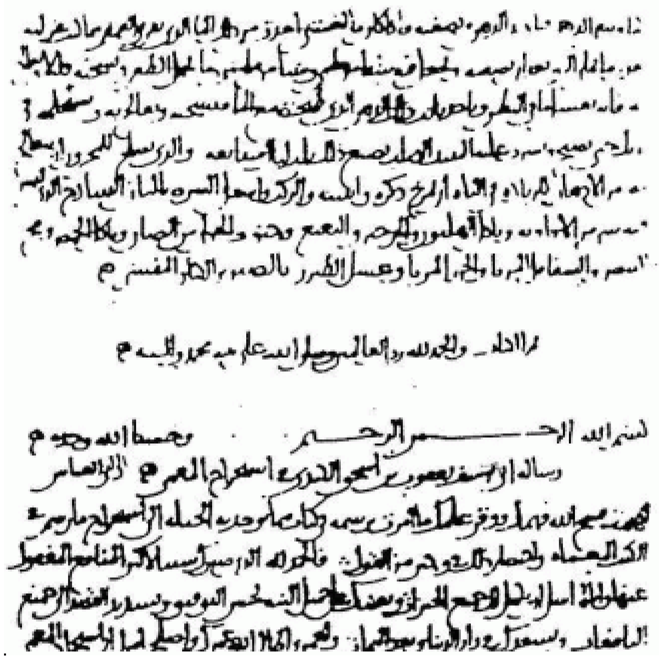
```
TREATY IMPOSSIBLE
```

would be encoded as

```
T R E A T Y   I M P O S S I B L E
w u h d w b   l p s r v v l e o h
```

Middle East 801-873 AD: First Cryptanalysis

- Al-Kindi (801-873 AD): Islamic scholar who developed a technique for breaking simple substitution ciphers using letter frequency analysis.
  - Important milestone in cryptoanalysis.
- Idea: Letters in messages written in natural human languages have certain letter frequencies.
  - Can crack the ciphertext by analyzing letter frequencies in the ciphertext and comparing them to those in the plaintext.



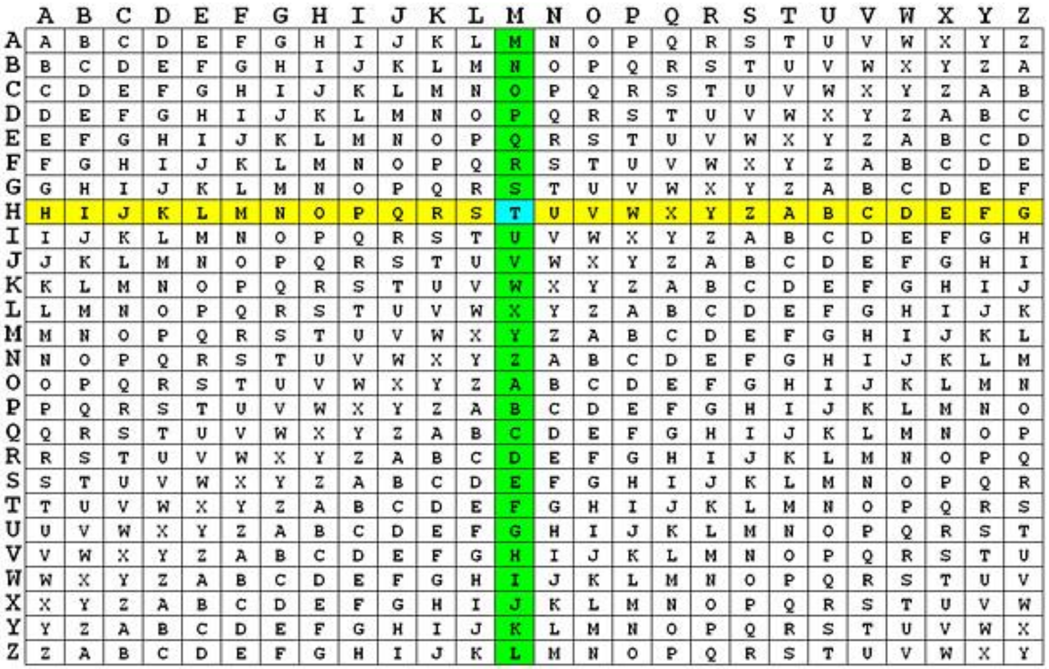
Al-Kindi's manuscript on letter frequency analysis.

1400 A.D. Europe: First Polyalphabetic Cipher

- Developed by Leon Battista Alberti (1404 – 1472): known as the “Father of Western Cryptology”
- Polyalphabetic cipher: the same plaintext letter is not always substituted with the same ciphertext letter.
- Based on two rotating concentric circles.
- Effective at defeating frequency analysis.

1500 A.D. France: Vigenere Cipher

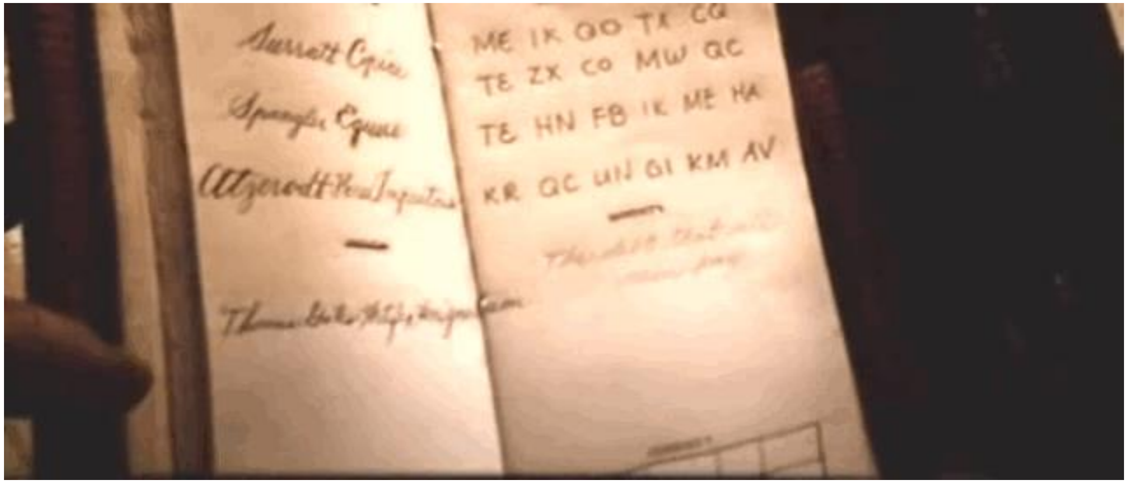
- Developed by Blaise de Vigenère (1523 – 1596).
- A polyalphabetic cipher inspired by the Alberti Cipher.
- Based on the Vigenère square (more later) which allows easy encryption using a piece of paper.
    - No need to carry a pair of disks as in case of Alberti Cipher!



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

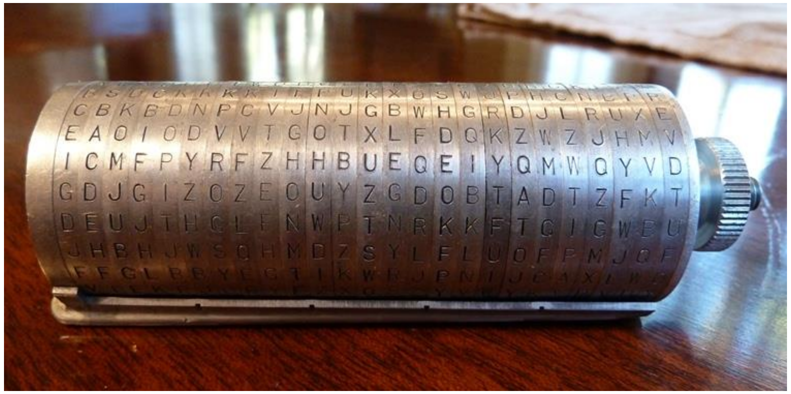
Britain 1845: First block cipher

- Invented by Charles Wheatstone (1802–1875) and Lyon Playfair (1818 – 1898).
- The first system to use pairs of symbols (i.e., block cipher) for encryption.
    - Encrypts plaintext two letters at a time.
- Lays the English alphabet in a 5 x 5 square matrix (more later).



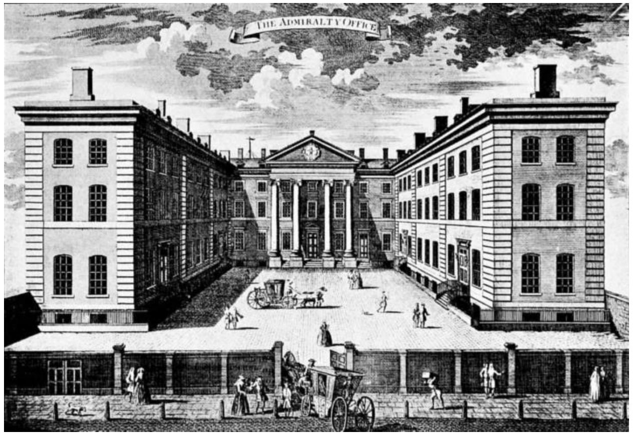
~1875 U.S.: Jefferson Wheel

- Invented by Thomas Jefferson (1801-1809).
- Used in the U.S. Army 1923 – 1942.
- A set of wheels around a horizontal axel. Each wheel consists of a random ordering of English letters.
- Encryption: The message is enciphered by aligning wheels such that one of the rows spells out a message. Read any other row.
- Decryption: align the wheels to form a ciphertext in a row. Look for a row spelling out the plaintext message.

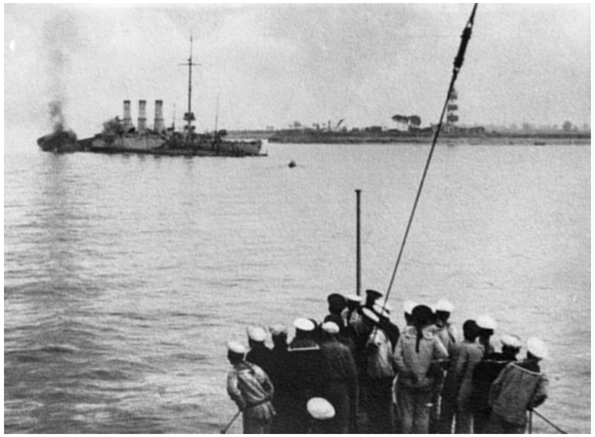

C B K B D N P C V J N J G B W H G R D J L R U X E
E A O I O D V V T G O T X L F D Q K Z W Z J H M V
I C M F P Y R F Z H H B U E Q E I Y Q M W Q Y V D
G D J G I Z O Z E O U Y Z G D O B T A D T Z F K T
D E U J T H C L F N W P T N R K K F T C I C W B U
J H B H J W S Q H M D Z S Y L F L U O F P M J Q F

World War I (1914 – 1918)

- Room 40 (est. 1914): British admiralty cryptanalysis office responsible for breaking many German ciphers during the war.



- SMS Magdeburg (1914): Russian navy captures German ship SMS Magdeburg and captures the naval codebooks.
  - Codebooks were handed over to Britain, giving it an edge over the Germans until the end of the war.

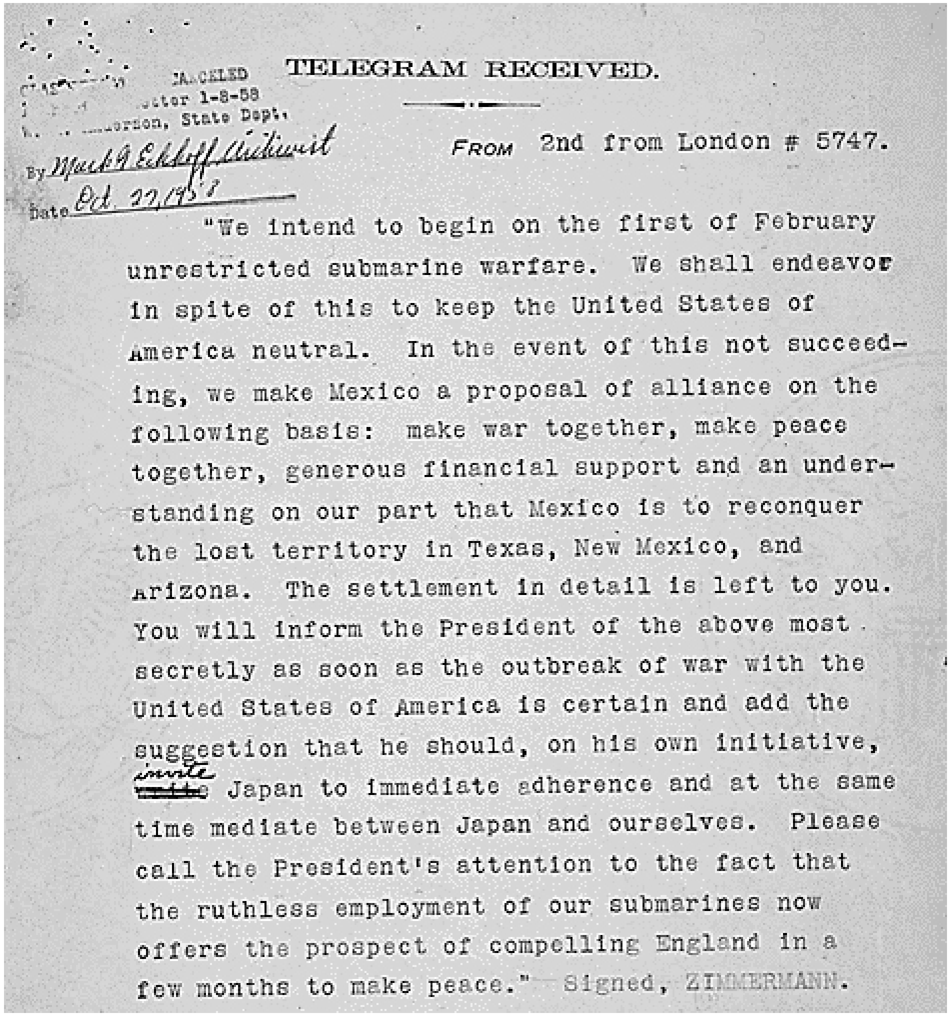


World War I (1914 - 1918) Cont.

- Russian defeat during invasion of east Prussia (1914): was a result of the Germans breaking Russia's disorganized and primitive cipher system.
  - Contributed to the spark of the Russian revolution

World War I (1914 - 1918) Cont.

- Zimmerman Telegram (January 1917):
  - Telegram sent by Foreign Secretary of the German Empire, Arthur Zimmerman, to the German ambassador in Mexico, Heinrich von Eckardt.
  - Offered Mexico to reclaim its territory of New Mexico, Texas, and Arizona if it supported Germany.



CANCELED
...ter 1-8-58
...orson, State Dept.
By Mark G Eckhoff Archivist
Date Oct. 22, 1958

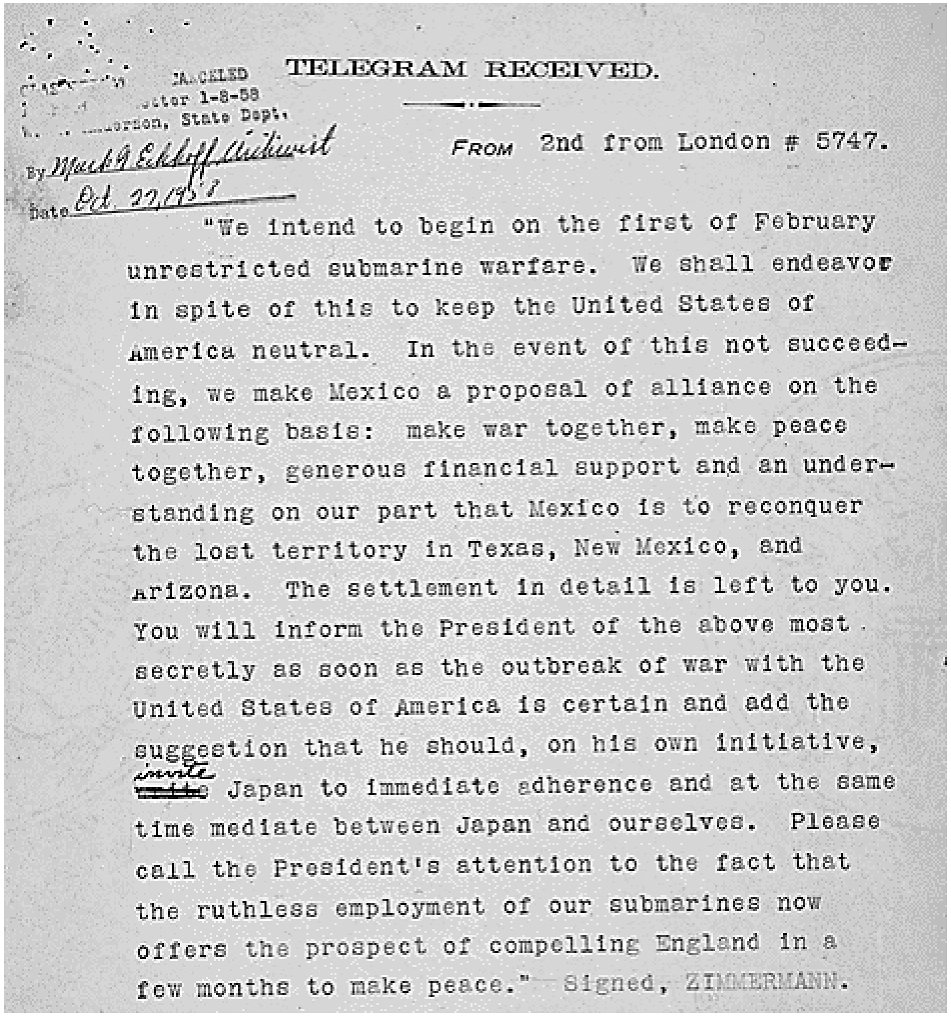
TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite ~~unite~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

World War I (1914 – 1918) Cont.

- Zimmerman Telegram:
  - Telegram was intercepted and cracked by Room 40.
  - Caused U.S. to enter the war.



[illegible]CELED
[illegible]ter 1-8-58
[illegible]orson, State Dept.
By Mack A Eckhoff Archivist
Date Oct. 22, 1958

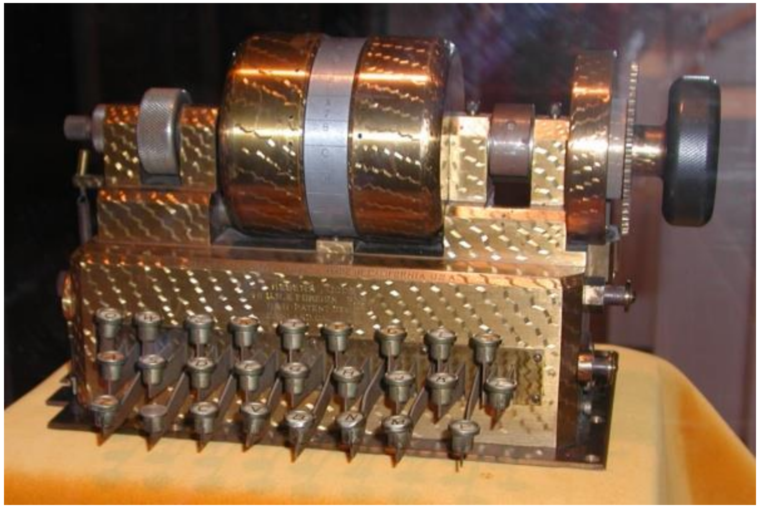
TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite ~~[illegible]~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

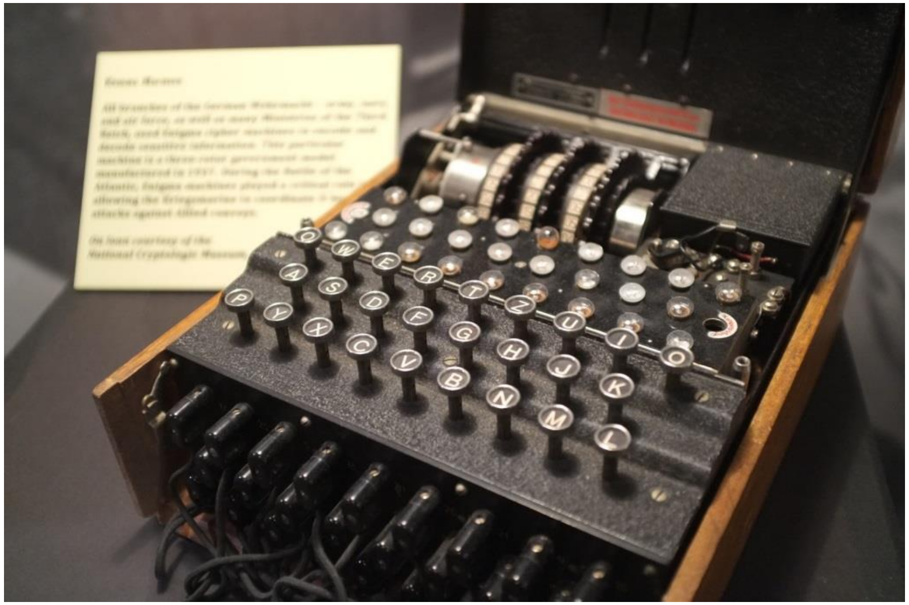
WWI - WWII: U.S: First Rotor Machine

- Hebern rotor machine
  - Invented by Edward Hebern (1869 – 1952)
  - Used a rotating disc in which the secret key is embedded.
  - The key encoded a substitution table.
  - Each key press from the keyboard resulted in the output of cipher text and rotated the disc by one letter.
  - Commercially unsuccessful.



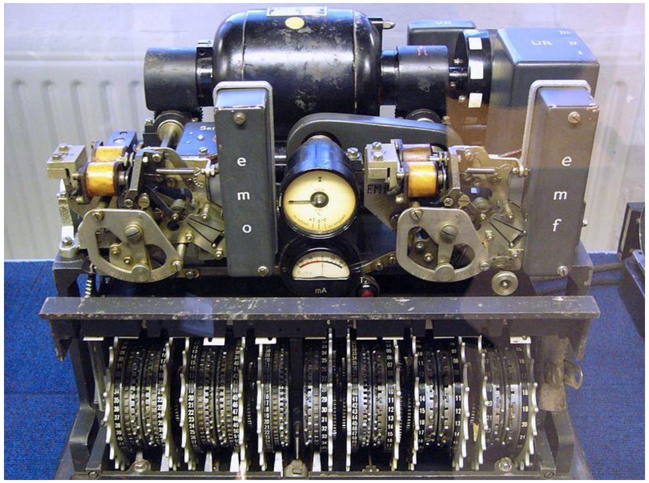
WWI – WWII Germany: Enigma Machine

- Invented by Dr. Arthur Scherbius (1878-1929)
- Used multiple rotating discs
- Was adopted by German military in 1937
- Played key role during WWII (more later)

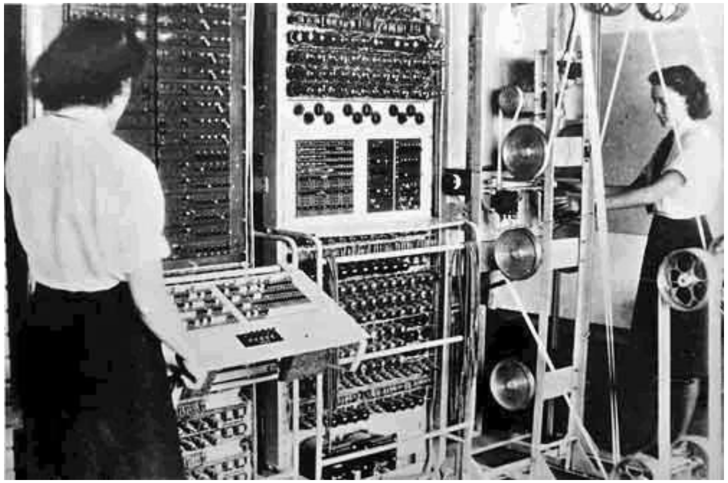


WWII (1939 to 1945): Germany

- Extensively used Enigma machines.
  - Broken using the "Bomb" machine designed by Polish cryptologist Marian Rejewski and refined by Alan Turing.
- Top German commanders used Lorentz machines produced by German C. Lorenz AG (1880-1958) firm.
  - Codes broken using the Colossus digital computer at Bletchley park.



Lorentz machine



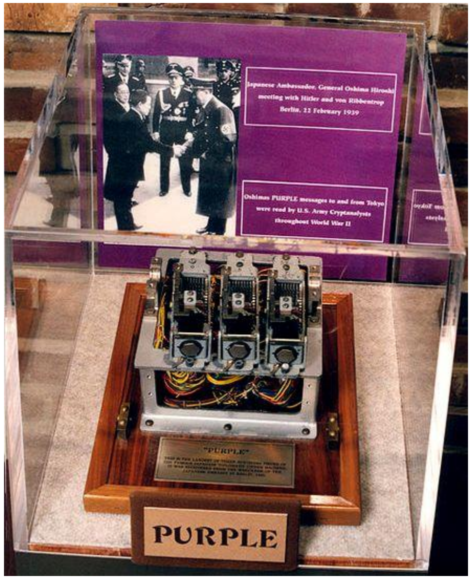
Colossus

WWII (1939 to 1945): Japan

- RED machine:
  - Based on a single rotor
  - Encrypted vowels and consonants separately (a weakness)
  - Eventually cracked by U.S.

WWII (1939 to 1945): Japan

- PURPLE machine:
  - Replaced RED and was more secure.
  - Based on several rotors and telephone switches.
- Broken by U.S. using the Known Plaintext Attack:
  - Attacker has access to the plaintext and the corresponding ciphertext and uses them to deduce keys, codebooks, etc.
  - Made possible by Japanese encrypting the same texts using both (the already broken) RED and PURPLE systems.

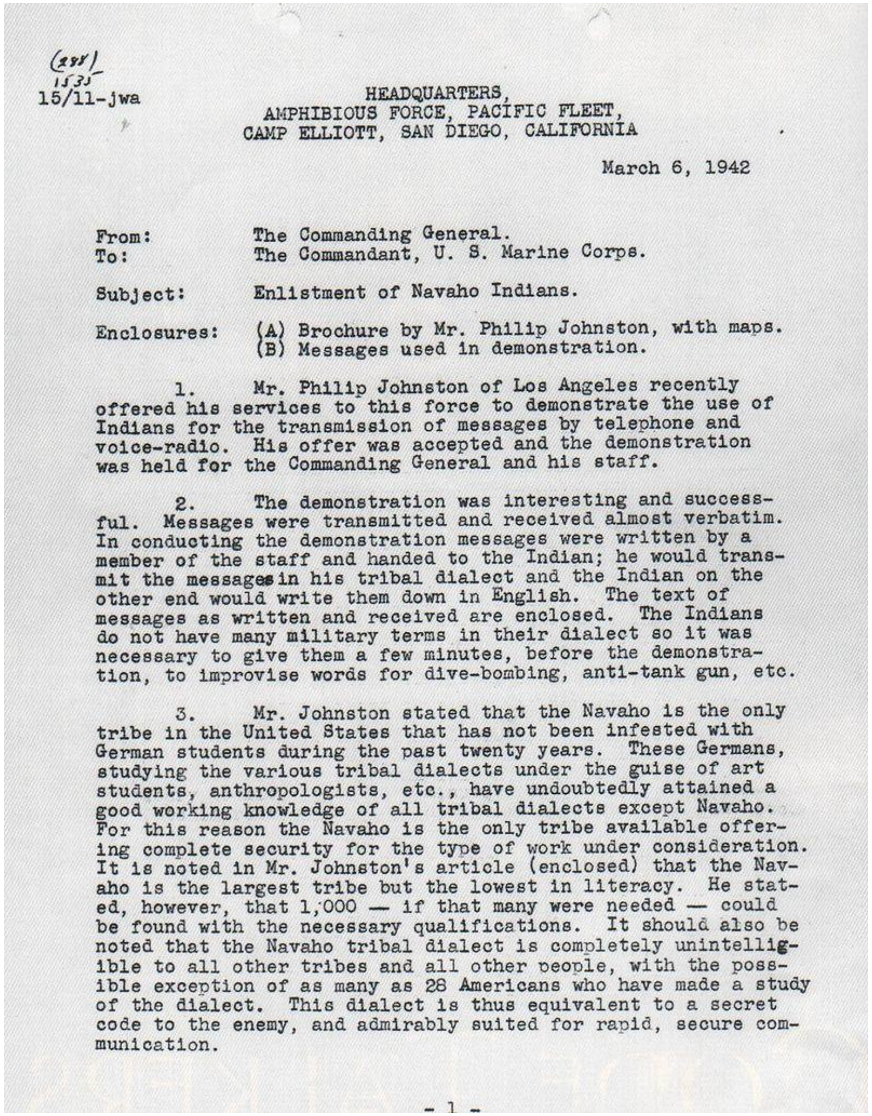

Japanese Ambassador, General Oshima Hiroshi meeting with Hitler and von Ribbentrop Berlin, 22 February 1939
Oshimas PURPLE messages to and from Tokyo were read by U.S. Army Cryptanalysts throughout World War II
"PURPLE"
PURPLE

WWII (1939 to 1945): Japan

- Breaking of Japanese codes played key role in US victory in the Battle of Midway, which was a turning point of the war in the Pacific Theatre.

WWII (1939 to 1945): U.S.

- Navajo code talkers:
  - Language of the Navajo Indians used as means of enciphering messages.
  - Proposed by Philip Johnston at the start of WWII;
  - Based on the premise that no German or Japanese knew the language.
  - Never broken



(288)
1535
15/11-jwa

HEADQUARTERS,
AMPHIBIOUS FORCE, PACIFIC FLEET,
CAMP ELLIOTT, SAN DIEGO, CALIFORNIA

March 6, 1942

From: The Commanding General.
To: The Commandant, U. S. Marine Corps.

Subject: Enlistment of Navaho Indians.

Enclosures: (A) Brochure by Mr. Philip Johnston, with maps.
(B) Messages used in demonstration.

1. Mr. Philip Johnston of Los Angeles recently offered his services to this force to demonstrate the use of Indians for the transmission of messages by telephone and voice-radio. His offer was accepted and the demonstration was held for the Commanding General and his staff.

2. The demonstration was interesting and successful. Messages were transmitted and received almost verbatim. In conducting the demonstration messages were written by a member of the staff and handed to the Indian; he would transmit the messages in his tribal dialect and the Indian on the other end would write them down in English. The text of messages as written and received are enclosed. The Indians do not have many military terms in their dialect so it was necessary to give them a few minutes, before the demonstration, to improvise words for dive-bombing, anti-tank gun, etc.

3. Mr. Johnston stated that the Navaho is the only tribe in the United States that has not been infested with German students during the past twenty years. These Germans, studying the various tribal dialects under the guise of art students, anthropologists, etc., have undoubtedly attained a good working knowledge of all tribal dialects except Navaho. For this reason the Navaho is the only tribe available offering complete security for the type of work under consideration. It is noted in Mr. Johnston's article (enclosed) that the Navaho is the largest tribe but the lowest in literacy. He stated, however, that 1,000 — if that many were needed — could be found with the necessary qualifications. It should also be noted that the Navaho tribal dialect is completely unintelligible to all other tribes and all other people, with the possible exception of as many as 28 Americans who have made a study of the dialect. This dialect is thus equivalent to a secret code to the enemy, and admirably suited for rapid, secure communication.

- 1 -

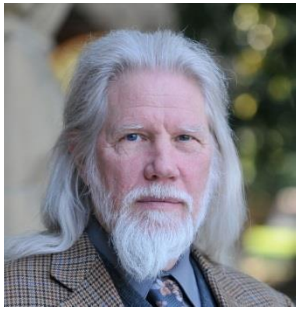
Philip Johnston's letter proposing the use of Navajo language

Modern Times: Public Key Cryptography

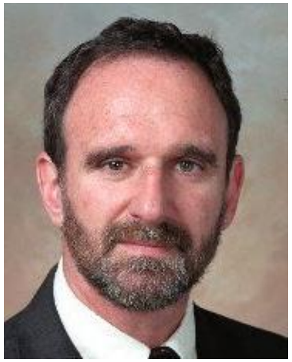
- ***Major*** revolution is cryptography
- Idea:
  - Two mathematically linked keys
  - What one key can encrypt, the other can decrypt
  - The same key cannot be used to both encrypt and decrypt
- Discovered by the public and classified communities.

Modern Times: Public Key Cryptography

- Public discovery:
  - 1976: Whitfield Diffie and Martin Hellman publish a paper proposing the idea of public key cryptography.
  - 1977: Ron Rivest, Adi Shamir and Leonard Adleman, develop the RSA scheme based on the difficulty of factoring products of large primes (they also found the RSA company)
  - Many other schemes followed… (e.g., Elgamal)

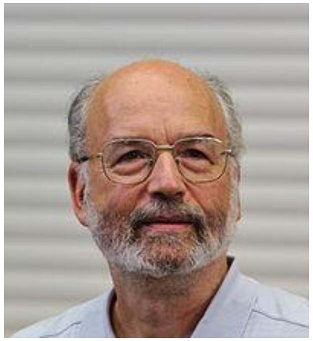


Whitfield Diffie

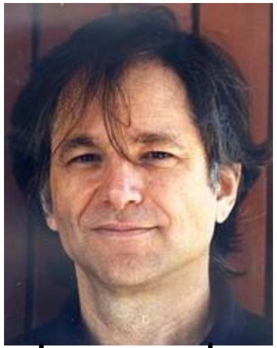


Martin Hellman

Ron Rivest



Adi Shamir



Leonard Adleman

Modern Times: Public Key Cryptography

- Classified discovery:
  - 1970: British cryptographer James H. Ellis of the UK Government Communications Headquarters (GCHQ) proposed the idea of "non-secret encryption".
  - 1973: Clifford Cocks of GCHQ implements an equivalent of RSA.
  - 1974: Malcolm J. Williamson of GCHQ implements what became known as the Diffile-Hellman key exchange (shared with NSA).
  - Importance of disregarded due to low computing power and focus on the military.

James H. Ellis

Clifford Cocks

Malcolm J. Williamson

Modern Times: Pretty Good Privacy (PGP)

- 1991: Pretty Good Privacy:
  - First publically available encryption program.
  - Developed by Philip Zimmerman
  - Distributed in U.S. and overseas:
    - Zimmerman investigated for violating the Arms Export Control Act, which at the time prohibited export of strong cryptography overseas.
    - Case dropped without charges
- 1996: Zimmermann founded PGP Inc. dedicated to the development of PGP
  - Became Symantec after a series of acquisitions
- 2013: Zimmermann found Dark Make Alliance to develop PGP replacement.

Philip Zimmerman

Modern Times: Today

- Primary goals:
  - Confidentiality: only authorized parties can access the information
  - Non-repudiation: inability to plausibly deny sending a particular message
  - Authenticity: ensuring that the party being communicated with are who they claiming to be
  - Integrity: protecting data from unauthorized modification
- Many protocols for securing network communications (e.g., OAuth, Kerberos, WPA)
- Blockchain technology for secure record keeping
- The next revolution: Quantum cryptography?

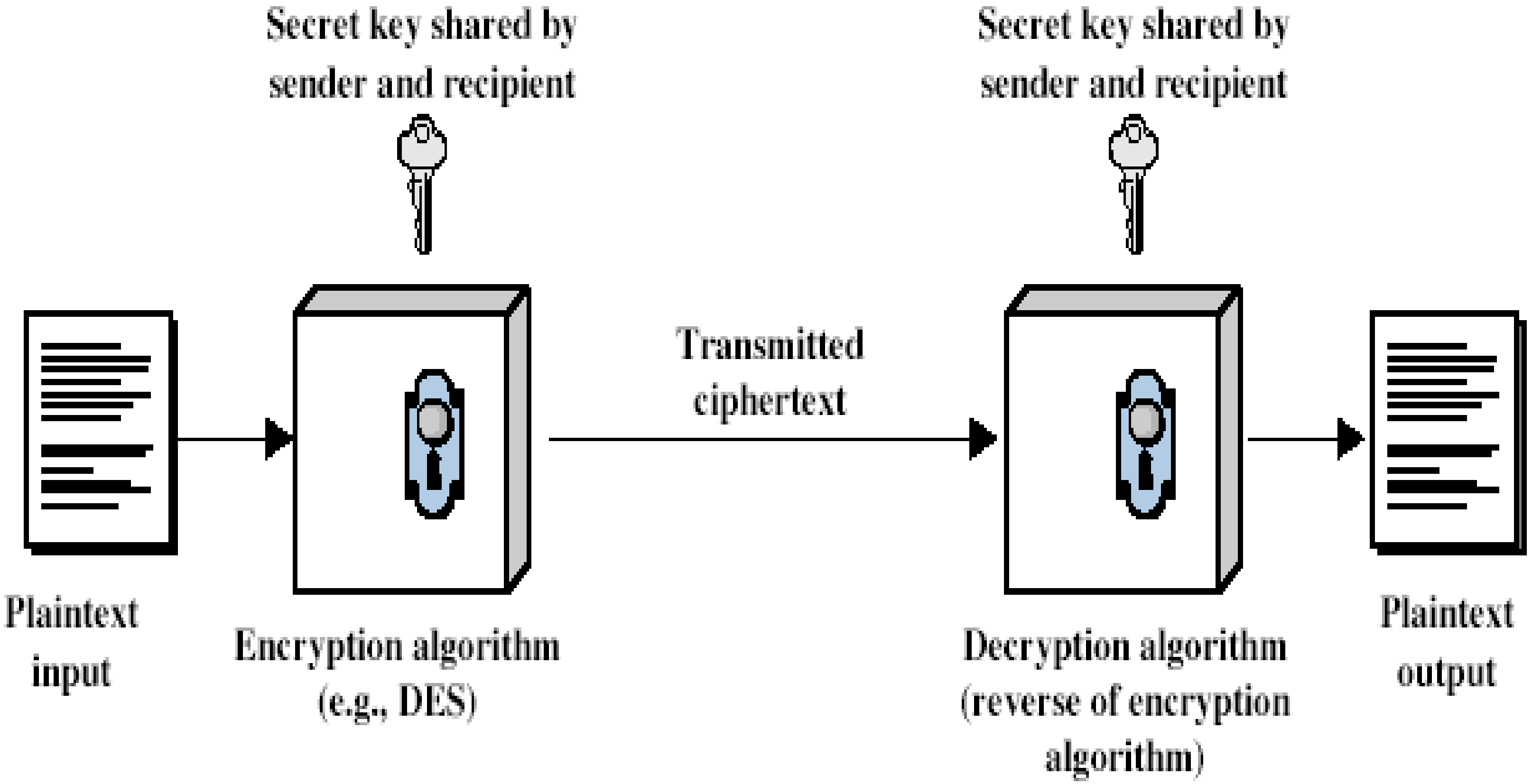
Cryptology Fundamentals and Classical Ciphers

Symmetric Encryption

- A form of cryptosystem in which encryption and decryption are performed using the same key – single-key encryption
- Was only type prior to invention of public-key in 1970's, and by far most widely used.

Symmetric Cipher Model

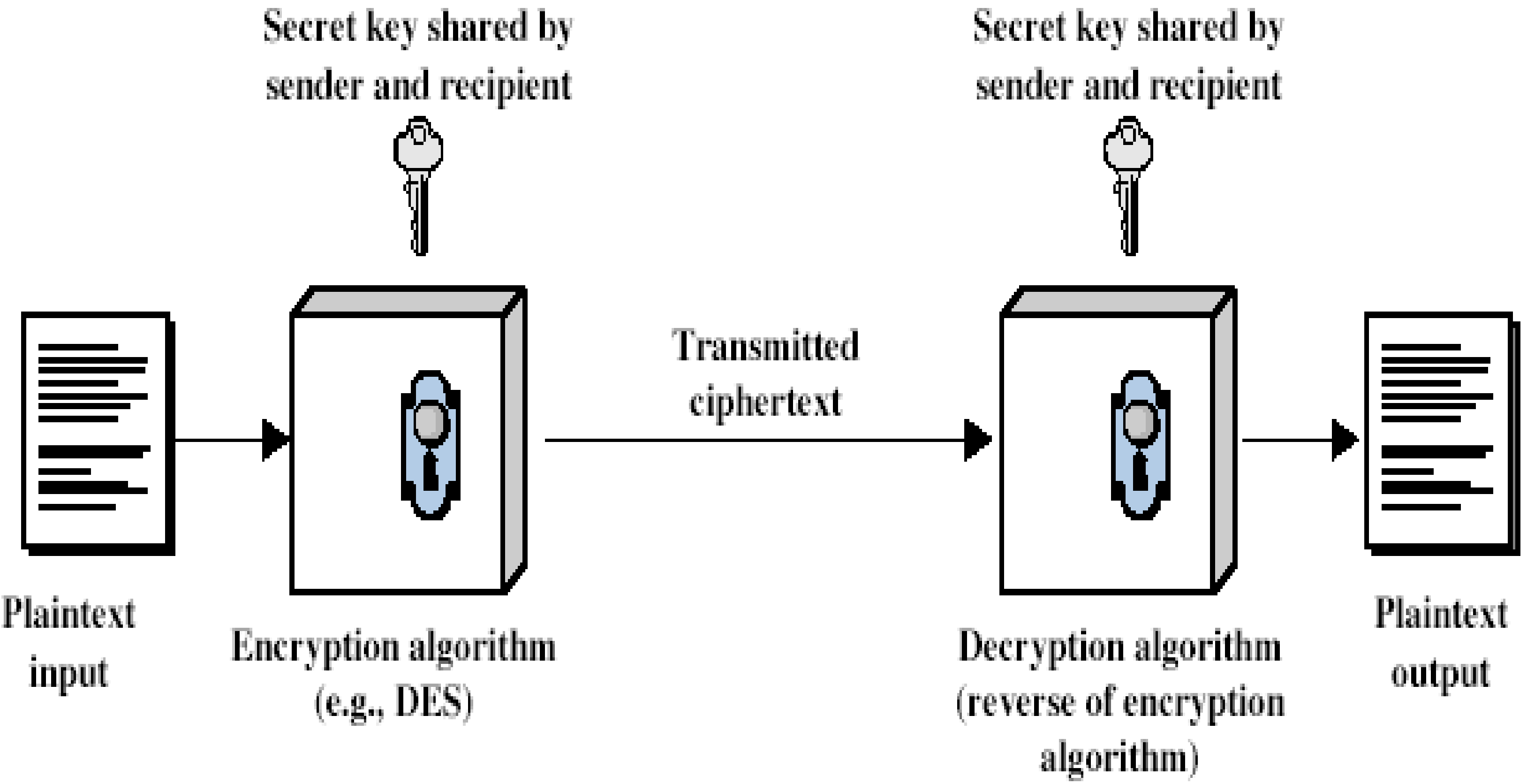
- Encryption algorithm: performs various substitutions and transformation on the plaintext.
- Secret key: the input of encryption algorithm. The key is independent of the plaintext and the alg..



Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Symmetric Cipher Model

- Decryption algorithm: the ciphertext and the secret key and produces the original plaintext.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Requirements

- Two requirements for secure use of symmetric encryption:
  - A strong encryption algorithm: the opponent should be unable to decrypt ciphertext or discover the key even if he/she has a number of ciphertexts and the plaintext that produced each ciphertext.
  - Assume encryption algorithm is known
  - Mathematically have:

X: message, K: encryption key, Y: ciphertext

$$Y = E(K,X)$$

$$X = D(K,Y)$$

An opponent can observe Y, but do not have access to K or X.

Key Clustering

- When two different keys produce the same plaintext

Requirements

- Two requirements for secure use of symmetric encryption:
  - A secret key known only to sender/receiver
    - Sender and receiver must have obtained copies of secret key in a secure fashion and must keep the key secure.
    - A third party could generate the key and securely deliver it to both source and destination.
    - If someone can discover the key and knows the algorithm, all communication using this key is readable.

Requirements: Kerckhoff's Principle

- ***A cryptographic system must remain secure even if everything about it except the secret key is known***
- Was first stated in the 19th century mathematician Auguste Kerckhoffs
- All modern cryptographic algorithms and protocols abide by it
- Is ***the opposite of "security by obscurity" (flawed) principle*** where security depends on the attacker not knowing the details of the cryptographic system function

Auguste Kerckhoff

Image source:
https://www.jungfrauzeitung.ch/gosimg100E015a01ad806680b300001201041r.jpg

Unconditional Security

- Unconditional security
  - No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to determine the corresponding plaintext.

Unconditional Security

- Unconditional security
  - No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to determine the corresponding plaintext.
  - No encryption algorithm is unconditionally secure except the one-time pad.

Computational Security

- Computational security
  - Given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken
    - 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

Brute Force Search

- Simply try every key until an intelligible translation of the ciphertext into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success - proportional to key size
- DES: 56-bit, triple DES: 168-bit, AES: > 128 bits
- Time required for various key spaces:

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} µs= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs= 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs= 5.9×10^{36} years	5.9×10^{30} years

Brute Force Search

- Simply try every key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success - proportional to key size
- DES: 56-bit, triple DES: 168-bit, AES: > 128 bits
- Time required for various key spaces:

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} µs= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs= 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs= 5.9×10^{36} years	5.9×10^{30} years

Substitution Cipher

Classical Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols

Caesar Cipher

- The earliest known substitution cipher (by Julius Caesar)
- First attested use in military affairs
- Replaces each letter with the letter standing K places further down the alphabet.
- When K = 3, 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

- Example:

Plaintext: meet me after the toga party

Caesar Cipher

- The earliest known substitution cipher (by Julius Caesar)
- First attested use in military affairs
- Replaces each letter with the letter standing K places further down the alphabet.
- When K = 3, 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

- Example:

Plaintext: meet me after the toga party

Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	I	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

- Then have Caesar cipher as:
  - Plaintext: pt, ciphertext: ct

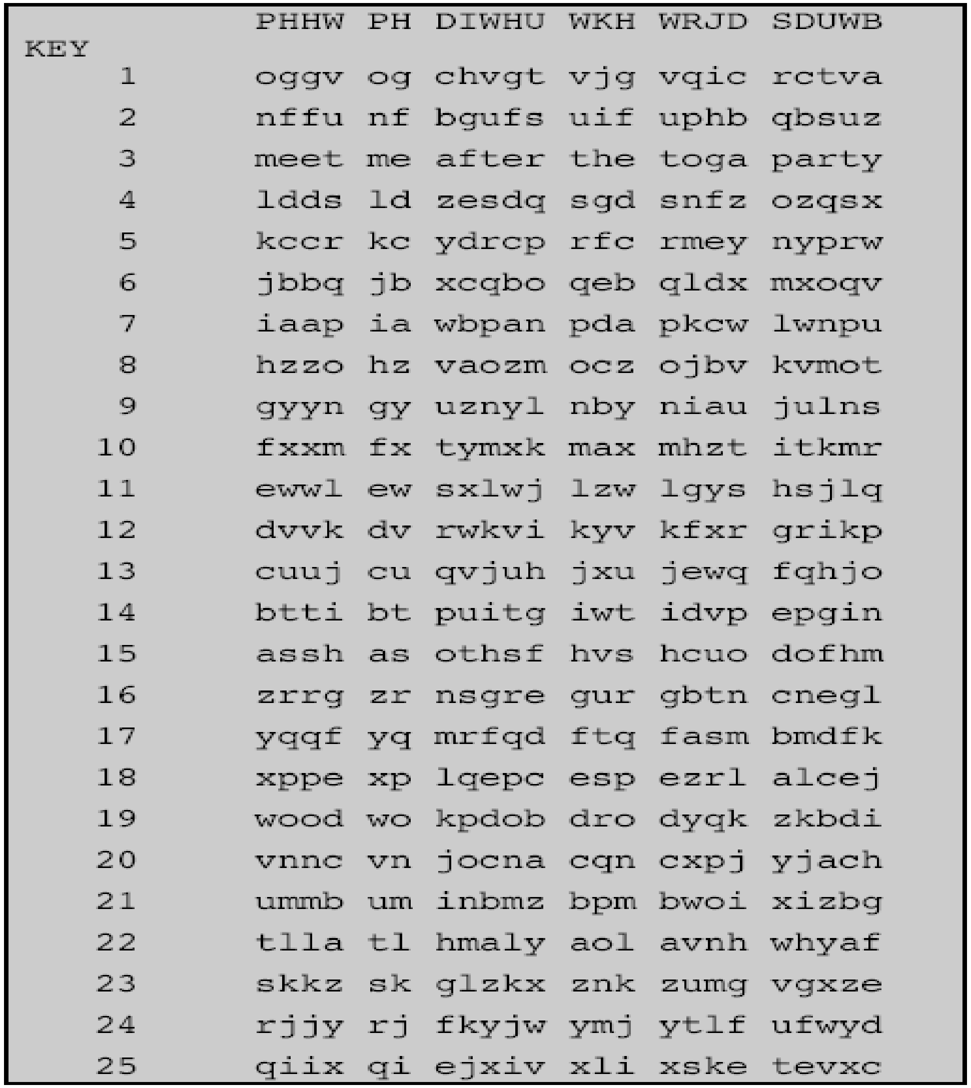
Encryption: ct = E(pt) = (pt + k) mod 26

Decryption: pt = D(ct) = (26+ (ct – k)) mod 26

Cryptanalysis of Caesar Cipher

Cryptanalysis of Caesar Cipher

- A brute force search can be easily performed: simply try all the 25 possible keys - far from security.
  - The language of the plaintext is known and easily recognizable.
- The input may be compressed, make recognition difficult, e.g., E.g. .zip file.



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

Monoalphabetic Cipher

- Allow an arbitrary substitution rather than just shifting the alphabet
- Each plaintext letter maps to a random ciphertext letter

```
Plain: abcdefghIjklmnopqrstuvwxyz
Cipher:DKVQFIBJWPESCXHTMYAUOLRGZN
```

E.g.,

If we wish to replace letters

Monoalphabetic Cipher

- Allow an arbitrary substitution rather than just shifting the alphabet
- Each plaintext letter maps to a random ciphertext letter

Plain: **abcdefghIjklmnopqrstuvwxyz**

Cipher:**DKVQFIBJWPESCXHTMYAUOLRGZN**

E.g.

If we wish to replace letters

WI RF RWAJ UH YFTSDVF SFUUFYA

Monoalphabetic Cipher Security

- The cipher line can be any permutation of the 26 alphabetic characters
  - 26! = $4*10^{26}$ mappings
- With so many mappings, might think is secure

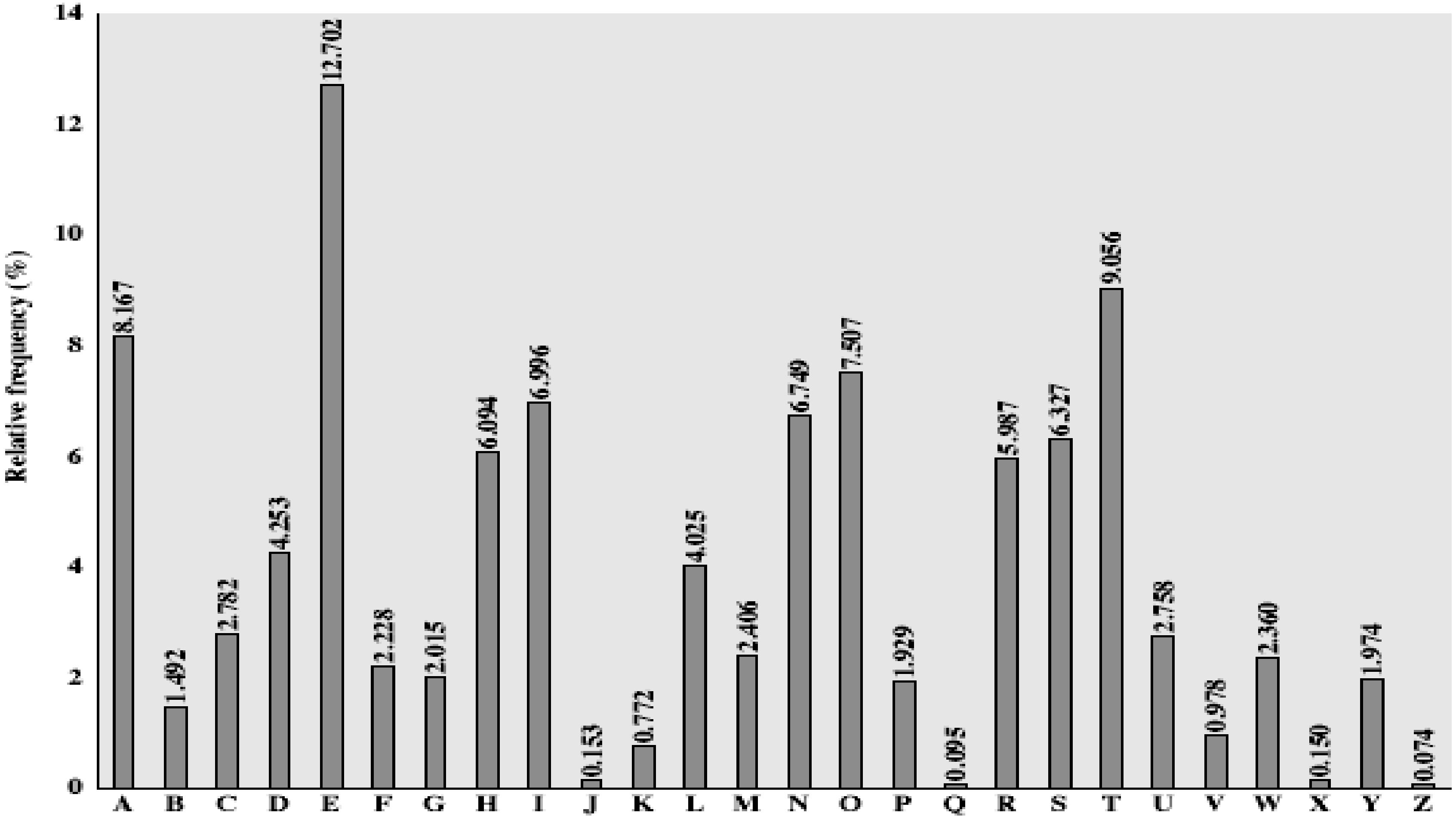
Monoalphabetic Cipher Security

- The cipher line can be any permutation of the 26 alphabetic characters
  - 26! = $4*10^{26}$ keys
- With so many keys, might think is secure
- But would be WRONG – if the cryptanalyst knows the nature of the plaintext (e.g., noncompressed English text), then the analyst can exploit the regularities (frequency of letters) of the language

Language Redundancy and Cryptanalysis

- Human languages are redundant. Letters are not equally commonly used.
- In English E is by far the most common letter, followed by T,A,O,I,N,S,R, other letters like Z,J,K,Q,X are fairly rare.
    - If the message is long enough, this technique alone may be sufficient.

English Letter Frequencies



Use in Cryptanalysis

- Main concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- Calculate letter frequencies for ciphertext
- Compare counts/plots against known values

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH
  ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH
  ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH
  ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P →e, Z → t, {S,U,O,M,H} → {a,h,i,n,o,r,s}
- Most common pair: ZW →   and hence ZWP → , ZWSZ →

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P →e, Z → t, {S,U,O,M,H} → {a,h,i,n,o,r,s}
- Most common pair: ZW → th and hence ZWP → , ZWSZ →

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P → e, Z → t, {S,U,O,M,H} → {a,h,i,n,o,r,s}
- Most common pair: ZW → th and hence ZWP → the, ZWSZ →

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPH ZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

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	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}
- Most common pair: ZW ➔ th and hence ZWP ➔the, ZWSZ ➔ that
- Finally: it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Playfair Cipher

- Not even the large number of mappings ($4*10^{26}$ mappings) in a monoalphabetic cipher provides security
- One approach to improving security is to encrypt multiple letters – e.g., Playfair Cipher.

Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword
- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom
- Fill rest of matrix with other letters
- Eg. using the keyword MONARCHY
- I and j count as one 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 Cipher: Encryption

- Plaintext is encrypted two letters at a time
  - If a pair is a repeated letter, insert filler x, e.g., bolloon ➔ bo lx lo on
  - If both letters fall in the same row, replace each with letter to right with the first element of the row circularly following the last, e.g. ar ➔ rm
  - If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), e.g. mu ➔ cm

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: Encryption

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair, e.g., hs ➔ bp, ea → im (or jm)

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: Encryption

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair, e.g. hs ➔ bp, ea → im (or jm)

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

- To decrypt, use the inverse of the encryption rules and drop any extra x that does not make sense in the final message.
  - Decrypts two letters at a time
  - If both letters fall in the same row, replace each with letter to left, e.g., rm → ar
  - If both letters fall in the same column, replace each with the letter above it, e.g., cm → mu

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

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair
  - E.g. bp ➔ hs, im → ea

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

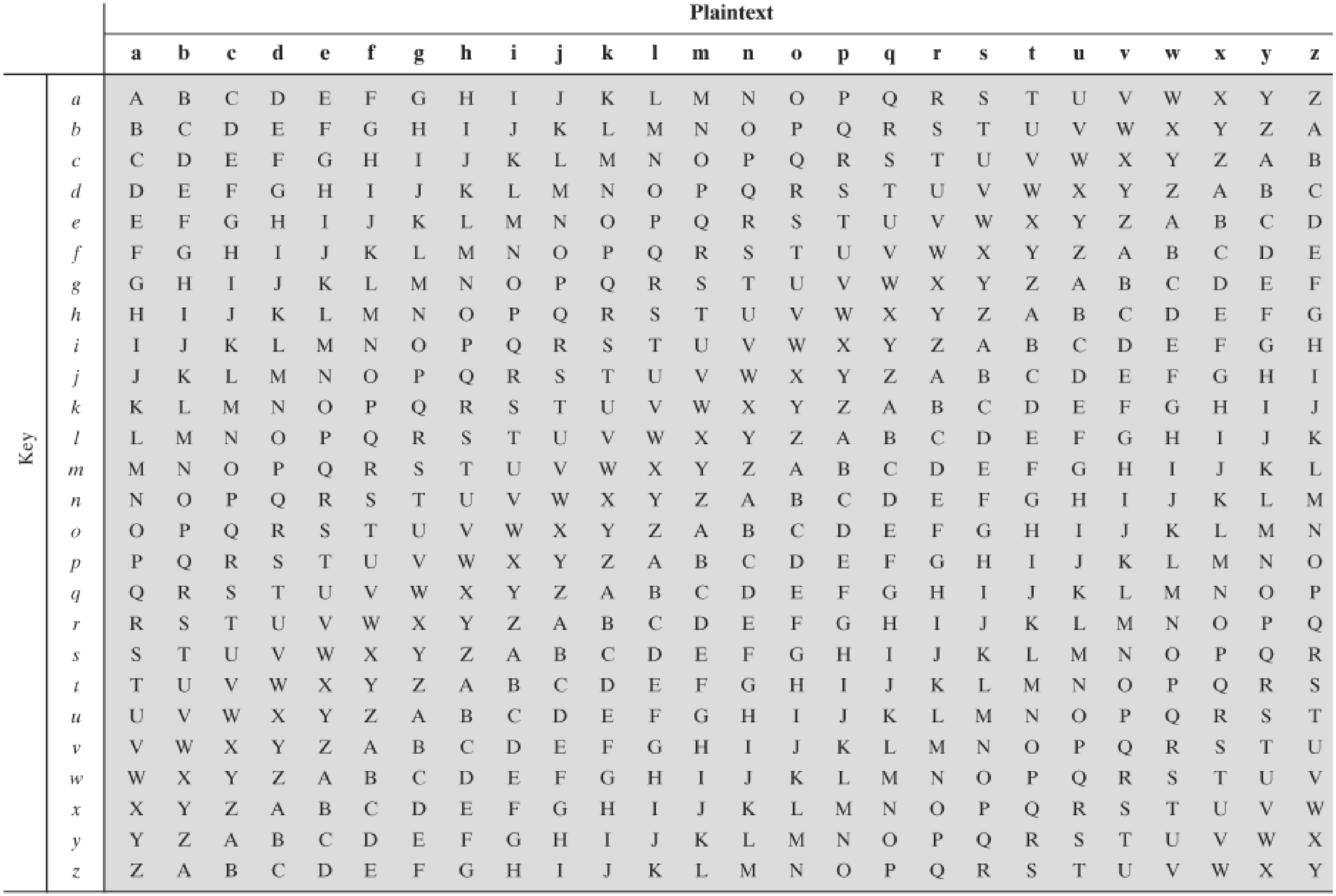
Security of Playfair Cipher

- Security much improved over monoalphabetic
- Would need a 676 (26*26) entry frequency table to analyse (verses 26 for a monoalphabetic)
- Was widely used for many years
  - eg. by US & British military in WW1
- It is relatively easy to break because it still leaves much of the structure of the plaintext language intact.

Polyalphabetic Ciphers

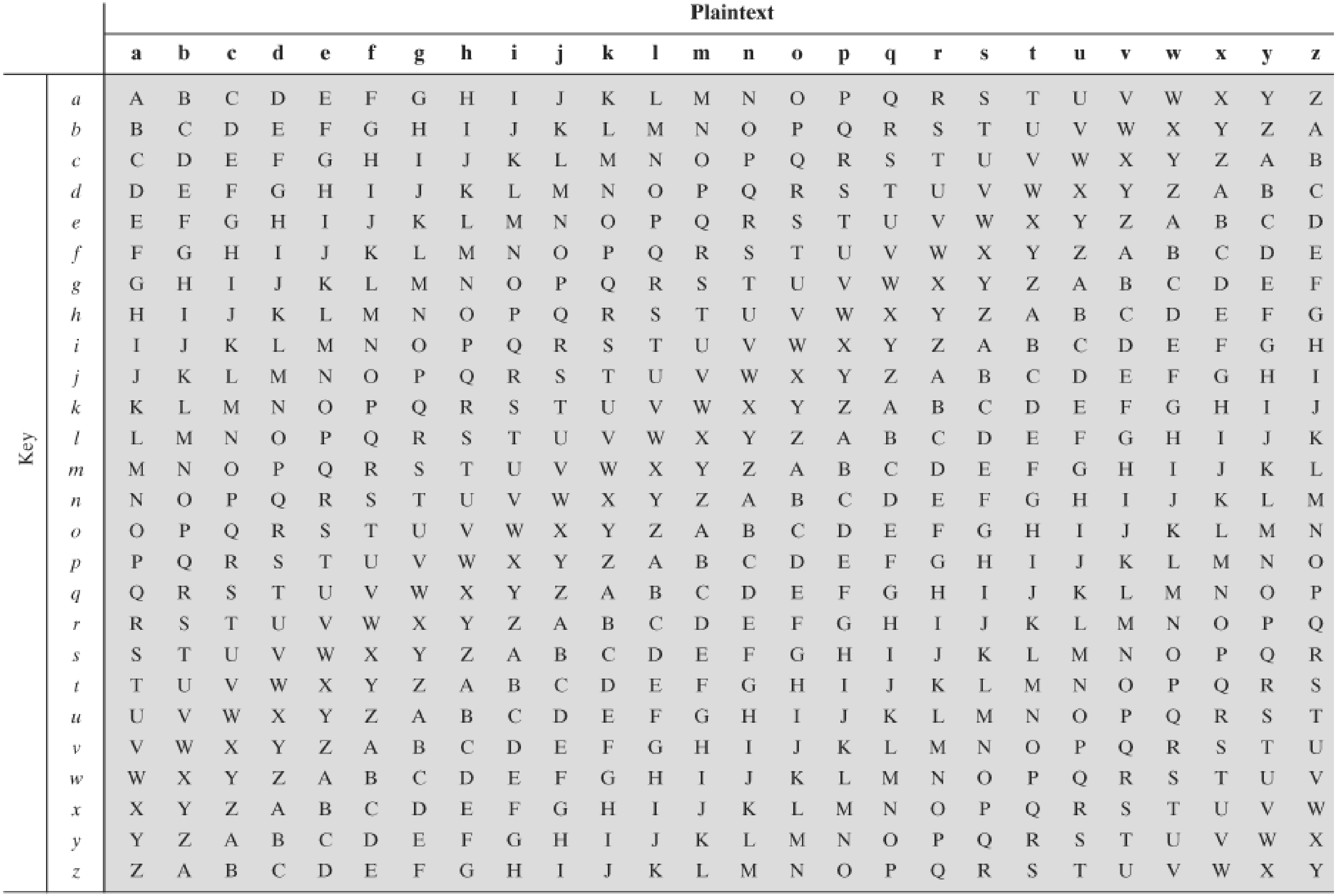
- Improve security using multiple monoalphabetic substitutions.
- Features
  - A set of related monoalphabetic substitution rules is used
  - A key determines which particular rule is chosen for a given transformation
- Vigenère Cipher: Simplest polyalphabetic substitution cipher

Modern Vigenère Tableau



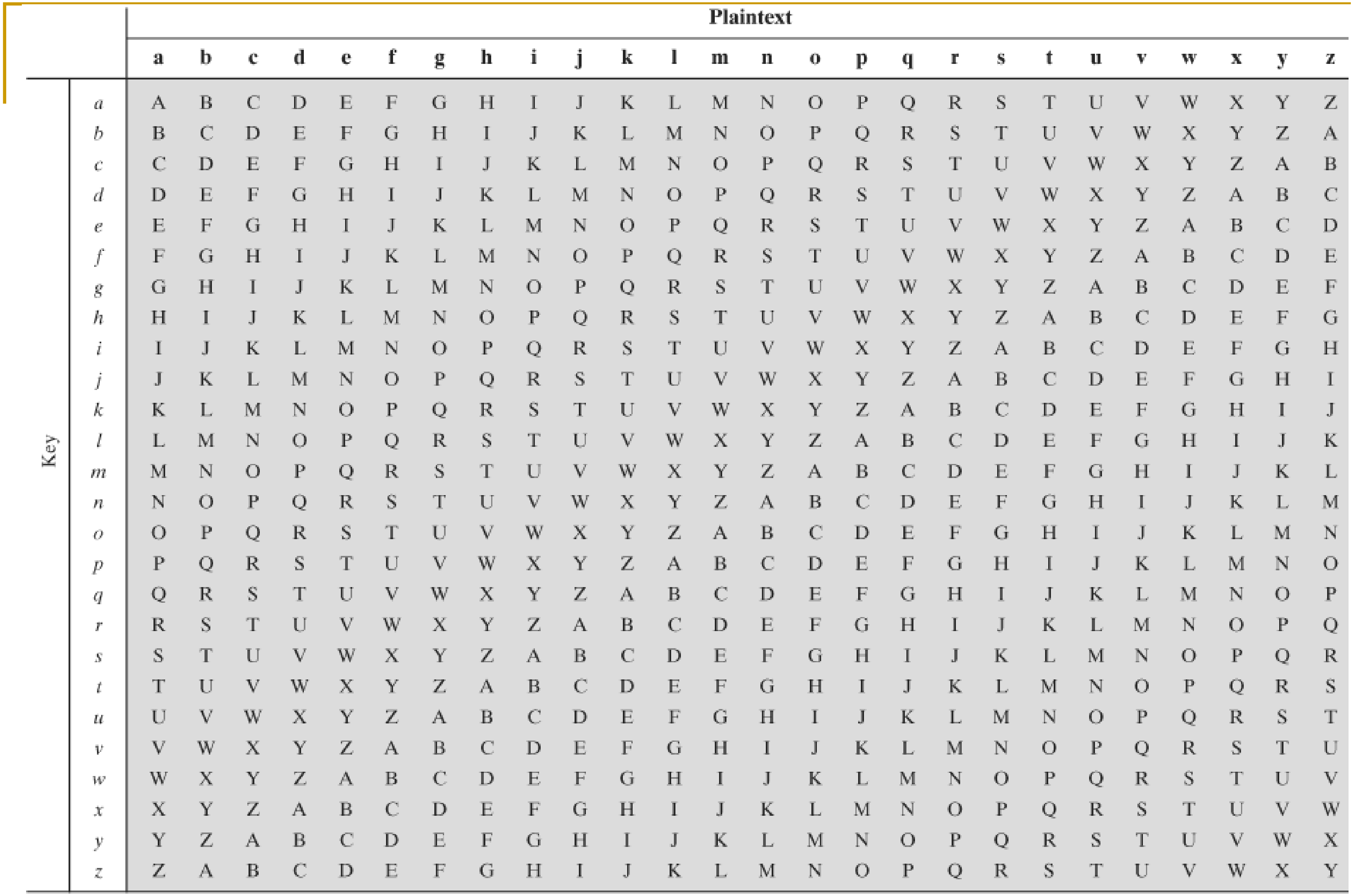
		Plaintext																								
		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key	*a*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W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

The set of related monoalphabetic substitution rules consists of 26 Caesar ciphers



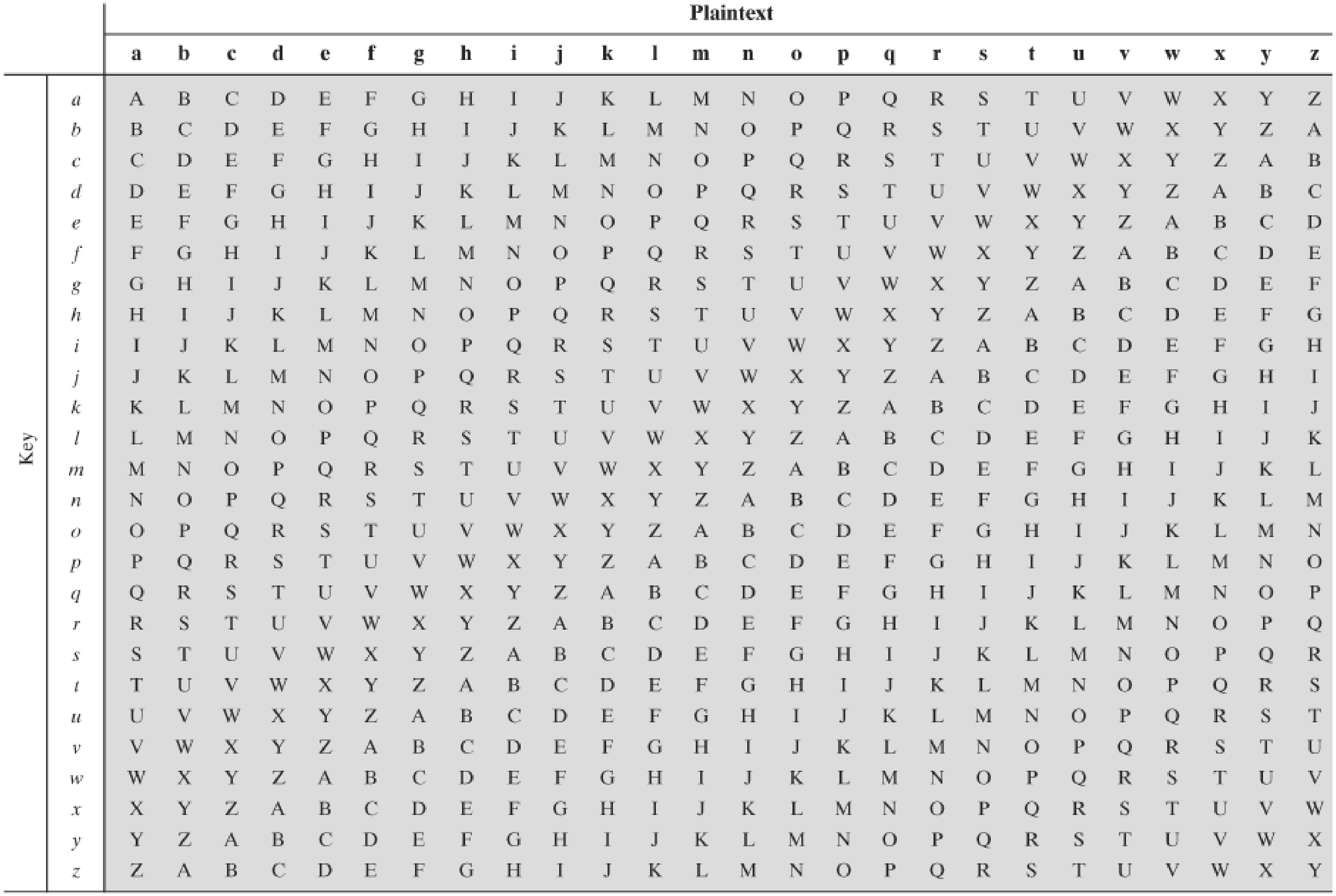
		Plaintext																									
		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key	a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X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

- Each Ceasar cipher is denoted by a key letter
- A normal alphabet for the plaintext runs across the top



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

Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of row labeled x and the column labeled y → the ciphertext is v.

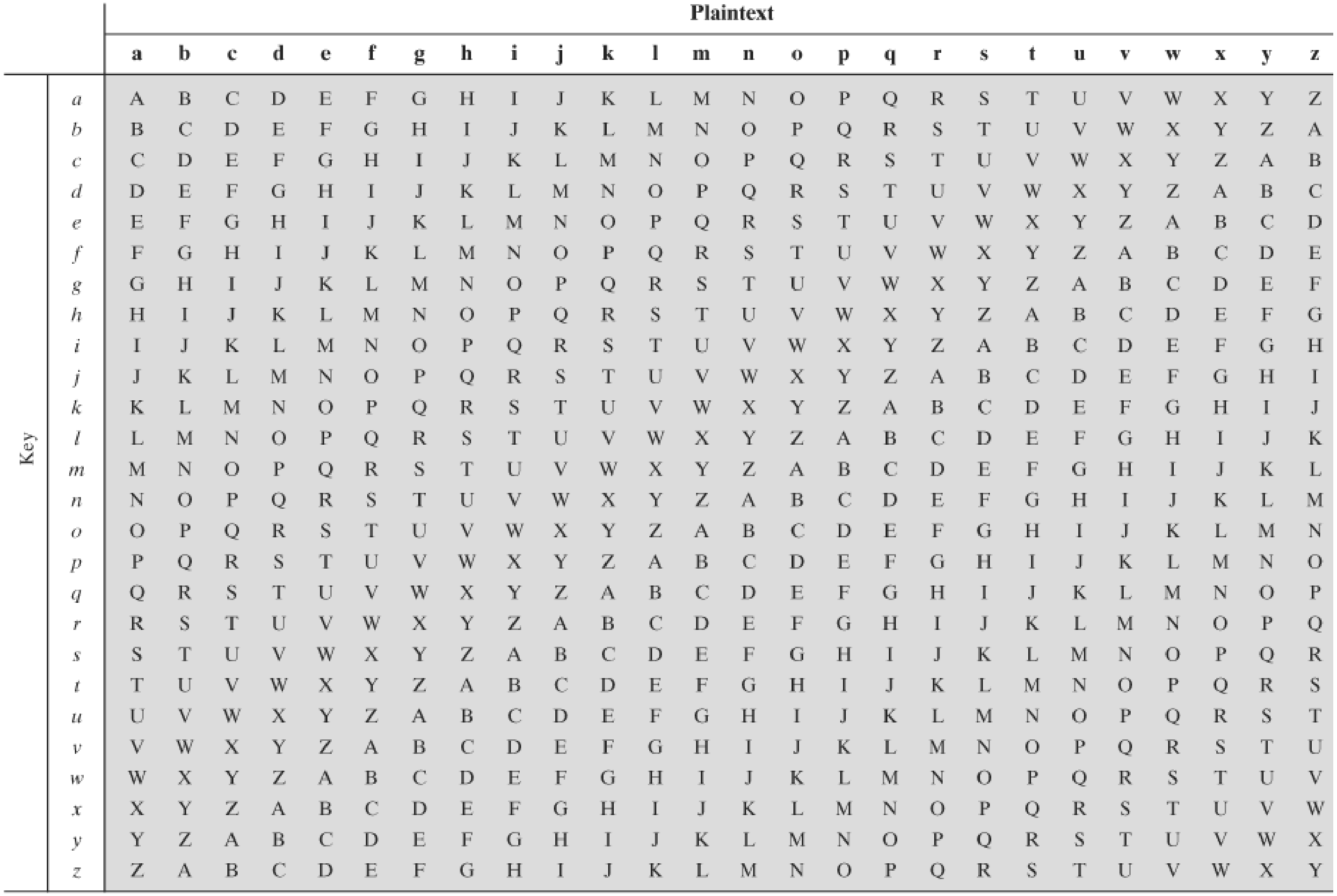


	Plaintext																									
Key	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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

- Write the plaintext out, write the keyword repeated above it
- E.g., using keyword *deceptive*

key: **deceptivedeceptivedeceptive**

plaintext: **wearediscoveredsaveyourself**



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

- Write the plaintext out, write the keyword repeated above it
- Eg using keyword *deceptive*

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

Vigenère Cipher: Decryption

Vigenère Cipher: Decryption

- Decryption:
  - The key letter identifies the row
  - The position of the ciphertext letter in that row determines the column
  - The plaintext letter is at the top of that column

Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter. Hence letter frequencies are obscured
- But not totally lost
- Suppose that the opponent believes that the ciphertext was encrypted using Vigenère Ciphers
  - If two identical sequences of plaintext occur at a distance that is an integer * length of keyword, they will generate identical ciphertext sequences.

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

Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter. Hence letter frequencies are obscured
- But not totally lost
- Suppose that the opponent believes that the ciphertext was encrypted using Vigenère Ciphers
  - If two identical sequences of plaintext occur at a distance that is an integer * length of keyword, they will generate identical ciphertext sequences.

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

Autokey Cipher: Encryption

- Ideally want a key as long as the message
- Vigenère proposed the autokey cipher
- A keyword is concatenated with the plaintext itself providing a running key.
- E.g., given key deceptive

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

How to decrypt a ciphertext?

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:       deceptive
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext:
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:       deceptive
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: w
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:          deceptivew
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext:  w
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:           deceptivew
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: we
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:       deceptivewe
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: we
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

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

Transposition Ciphers

- Consider classical transposition or permutation ciphers
- Hide the message by rearranging the letter order without altering the actual letters used

Transposition Ciphers

- Consider classical transposition or permutation ciphers
- Hide the message by rearranging the letter order without altering the actual letters used
- Can recognize these since have the same frequency distribution as the original text

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Then read the letters row by row
- E.g., Encrypt the message "meet me after the toga party" with a rail fence of 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
```

  - Ciphertext: **MEMATRHTGPRYETEFETEOAAT**

- Think: how to encrypt the above message using rail fence cipher of depth 3?

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Then read the letters row by row
- E.g., Encrypt the message "meet me after the toga party" with a rail fence of depth 3

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

  - Ciphertext: **MTAEHOPTEMFREGAYEETTTAR**
  - Think: how to decrypt a ciphertext

ciphertext: CPEERYOURCIMTSUT

Rail Fence cipher: Decryption

- How to decrypt a ciphertext
  - Let |**row**| be the number of rows
  - Compute the length of the ciphertext |**cipher**|
  - Compute the number of letters of each row
  - Write down the ciphertext row by row
  - Read the ciphertext diagonally

Rail Fence cipher: Decryption

- Example:

  ciphertext: **CPEERYOURCIMTSUT**

  |row| = 3

  ❖ **|cipher| = 16**

  ❖ **16/3= 5, 16 mod 3 = 1 ➔**

  1st row: 5+1 = 6 letters

  2nd row: 5 letters, 3rd row: 5 letters

  C P E E R Y

  O U R C I

  M T S U T

  ➔ Plaintext: **computersecurity**

Rail Fence cipher: Decryption

- Example:

  ciphertext: **CPEERYOURCIMTSUT**

  |row| = 3

  - **|cipher| = 16**
  - **16/3= 5, 16 mod 3 = 1 ➔**

    1st row: 5+1 = 6 letters

    2nd row: 5 letters, 3rd row: 5 letters

C P E E R Y

O U R C I

M T S U T

➔ Plaintext: **computersecurity**

Row Transposition Ciphers

- A more complex transposition
- 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 columns

Key:	3	4	2	1	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

Read the 3rd column

Ciphertext: **TTNAAPTMTSUOAODWCOIXKNLYPETZ**

- Think: how to decrypt a ciphertext?

ciphertext: ATHNIERIPTSISORPNSOCX

Row Transposition Ciphers: Decryption

- How to decrypt a ciphertext?
  ciphertext: ATHNIERIPTSISORPNSOCX

  - |cipher| = 21, |key| = 7 → |row| = 3

Key:	3	4	2	1	5	6	7
Ciphertext:	T	R	A	N	S	P	O
	S	I	T	I	O	N	C
	I	P	H	E	R	S	X

Plaintext: transpositionciphers

Product Ciphers

- Ciphers using substitutions or transpositions are not secure because of language characteristics
- Hence consider using several ciphers in succession to make harder
  - Two substitutions make a more complex substitution
  - Two transpositions make a 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

- Cryptography: make the message unintelligible.
- Steganography: Conceal the existence of the message.
- Example:

"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 dispatch to the Syndicate by Friday
20th or at the very latest, I'm told by the 21st.
Admin has improved here, thought 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."

Steganography

Example:

"PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY. "

Steganography

Example:

"PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY. "

PERSHING SAILS FROM NY JUNE I

Steganography

- Modern Examples:
  - Encoding hidden message in the pixels of the image.
  - Encoding hidden messages in the bits of sound files.
- Advantage: useful to parties who are more concerned with hiding the fact of their secret communication, rather than the contents of messages.
- Drawbacks:
  - Significant overhead to hide a small amount of information.
  - Once the scheme is known, the system is useless.

Additional References

- http://www.eventid.net/docs/desexample.htm
- http://www.iusmentis.com/technology/encryption/des/
- http://www.research.ibm.com/journal/rd/383/coppersmith.pdf

Acknowledgement

- Some slides are borrowed from Dr. Ping Yang