Cryptography: The science of secrecy

Hugo Touchette

School of Mathematical Sciences, Queen Mary, University of London

Queen Mary, University of London
March 2008

About myself

Hugo Touchette
Lecturer in applied mathematics

Research job

- Theoretical physics
- Chaotic systems
- Statistical physics
- Probability and statistics

Education

- B.Sc. Physics (Canada) 3 years
- M.Sc. Mechanical Engineering (USA) 2 years
- Ph.D. Physics and Computer Science (Canada) 3 years
- Post-doc Mathematics (UK) 2 years

What is cryptography?

Cryptography

- Art or science of secret communication
- Art or science of secret codes (ciphers)
- Art or science of code breaking
- Art or science of hiding messages (steganography)
- Art or science of protecting information from unauthorised interception or tampering

Why maths?

Design of ciphers

- Use symbols to encrypt messages
- Use numbers to encrypt messages
- Encrypt messages through a mathematical problem

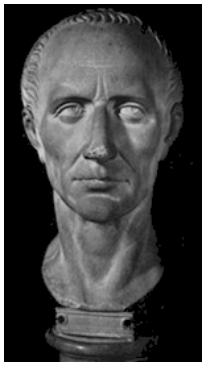
Security of ciphers

- What symbols/numbers to use?
- What encryption method to use?
- Is the cipher/code secure?
- How easy is breaking the code?

Breaking ciphers

- Systematic study of ciphers
- Systematic methods for breaking ciphers

Caesar challenge



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

↓

? ?

Cryptotext

The science of cryptography

Cryptography

Protection of information from unauthorised interception or tampering

crypto	graphy
$\kappa\rho\nu\pi\tau o$	$\gamma\rho\alpha\phi\iota\alpha$
hidden	writing

Cryptoanalysis

Science of breaking secret ciphers

Cipher

Encryption method or secret code

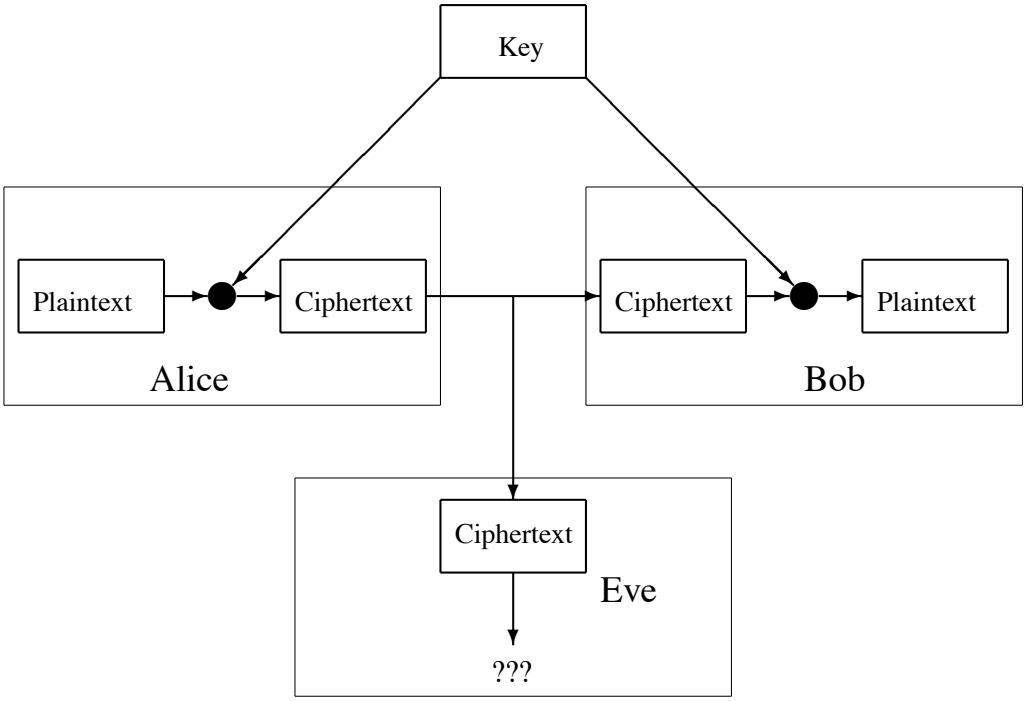
Plaintext

Text to encrypt

Cryptotext or cryptogram

Encrypted text

Cryptography (cont'd)



Cryptography (cont'd)

Steganography

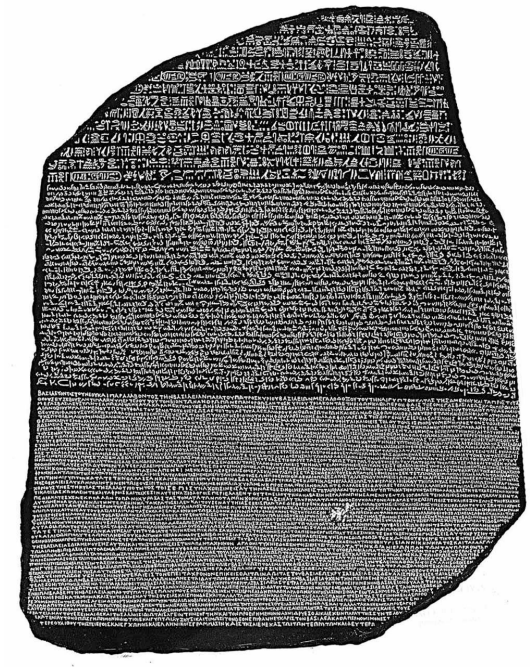
The concealing or covering of a message

Examples

- Invisible ink
- The prepared letters bring news of amounts
  The prepared letters bring news of amounts
  retreat
- Watermarks (in images or music files)

Ancient "ciphers"

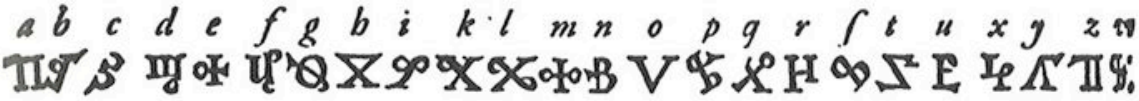
Cretan disk, 17th century BC



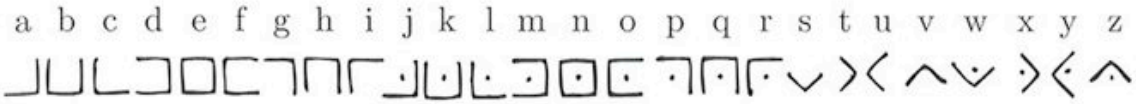
Rosetta stone, 196 BC
Hieroglyph, demotic, greek

Old ciphers

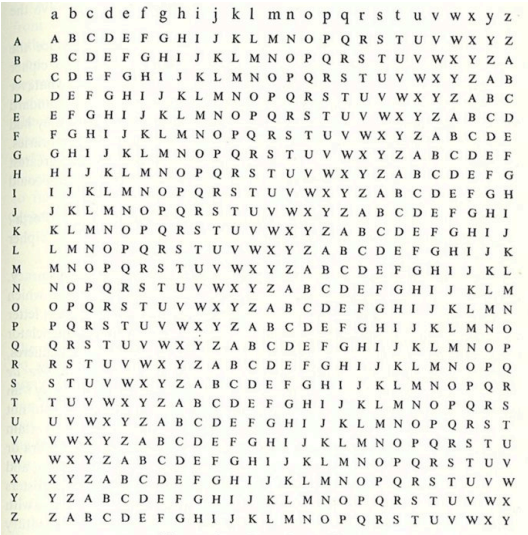
- Charlemagne's cipher (742-814):



- Freemason's pigpen cipher (1700s):



Old ciphers (cont'd)



	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

Vigenère's table, 1586

Wheatstone wheel, 1867

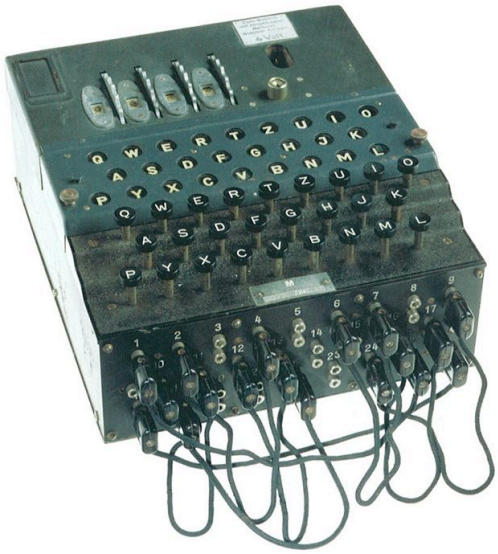
WWI and WWII ciphers

Cylinder cipher M-94, 1922

Strip cipher M-138-T4, WWII

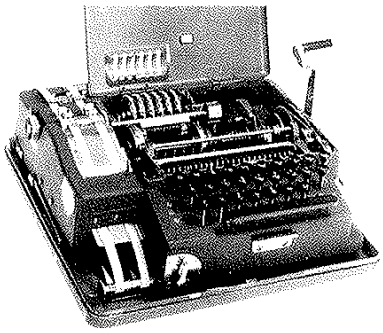
WWI and WWII ciphers (cont'd)

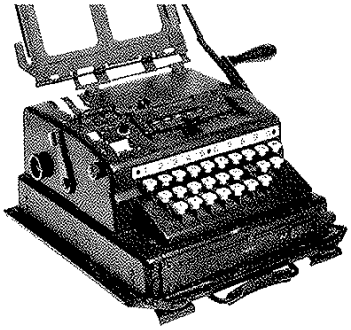
ENIGMA, 1937



ENIGMA M4, German marine, 1944

WWI and WWII ciphers (cont'd)





Hagelin BC-543 (USA) and German copy

Hagelin C-26, Stockholm, 1936

WWI and WWII ciphers (cont'd)

British Typex (British version of ENIGMA)

Caesar's cipher

Principle

- Shift all the letters of the plaintext by a constant number of places
- Key = shifted positions

Key 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
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

Key 4

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 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

Example

HELLO
KHOOR (key 3)
LIPPS (key 4)

Number of keys

Key 0

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 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 1

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 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

⋮

How many different Caesar's ciphers are there?

Solution

26 letters = 26 keys = 26 ciphers
−1 trivial cipher (no shift)
= **25 ciphers**

Breaking Caesar's cipher

Exhaustive key search

- Decode the cryptotext using each of the 25 keys
- Select the correct plaintext

Example

Cryptotext	Plaintext
XMZVH	WLYUG JYLHT QFSOA MBOKW NCPLX VKXTF IXKGS DSFBN ZOBXJ UJWSE HWJFR PERNZ APCYK TIVRD GVIEQ CREAM YNAWI SHUQC FUHDP ODQMY KZMIU RGTPB ETGCO BQDZL LANJV

Substitution ciphers

Principle

- Replace each letter by a different letter
- Do not use the same letter twice
- Key = substitution table

Example

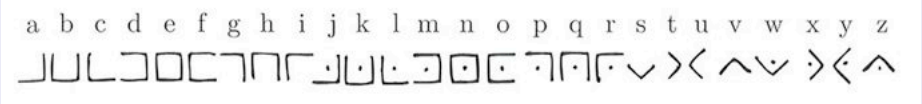
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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

HELLO PDWWG

Symbolic substitutions

Charlemagne



Freemasons

Number of substitution ciphers

How many substitution ciphers are there?

Gross estimate

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

_ _

- 26 choices for A
- 25 choices for B
- 24 choices for C

  ⋮

$26 \times 25 \times 24 \times \cdots \times 2 \times 1 = 26!$ ciphers
-1 trivial cipher (identity)
$= 26! - 1 = 403291461126605635583999999$ ciphers

Number of substitution ciphers

Dangerous substitutions

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

Correct estimate

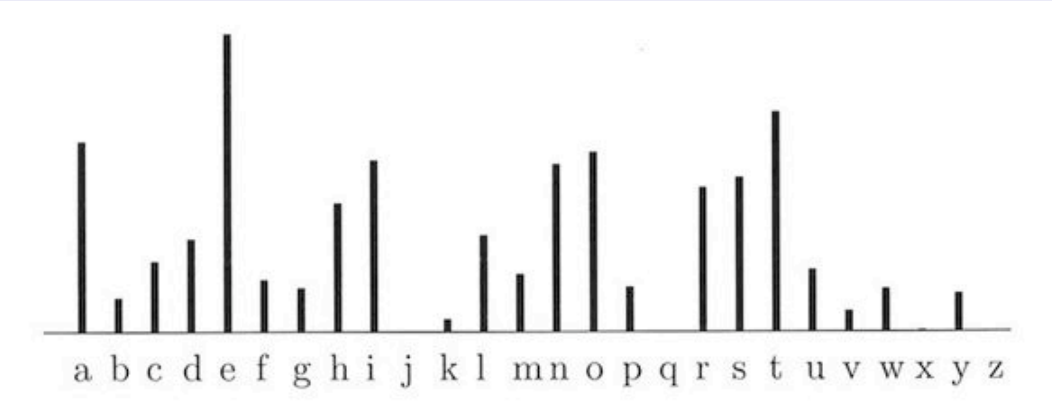
$26! - 1 -$ # dangerous ciphers

Breaking substitution ciphers

Basic observation

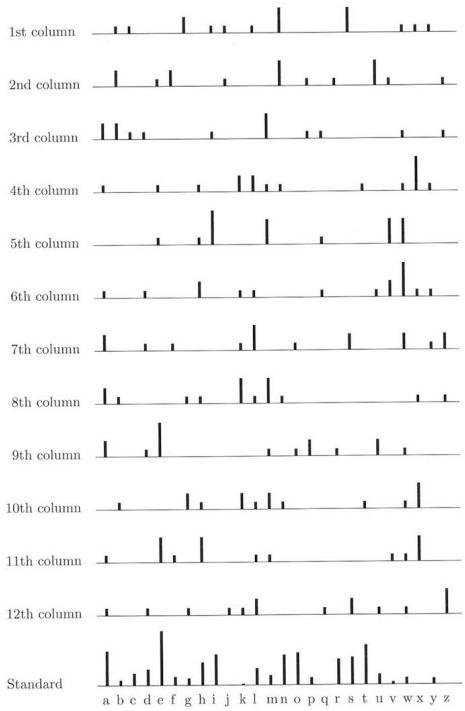
- Plaintext: Some letters appear more often than others
- Cryptotext: Some letters will also appear more often than others

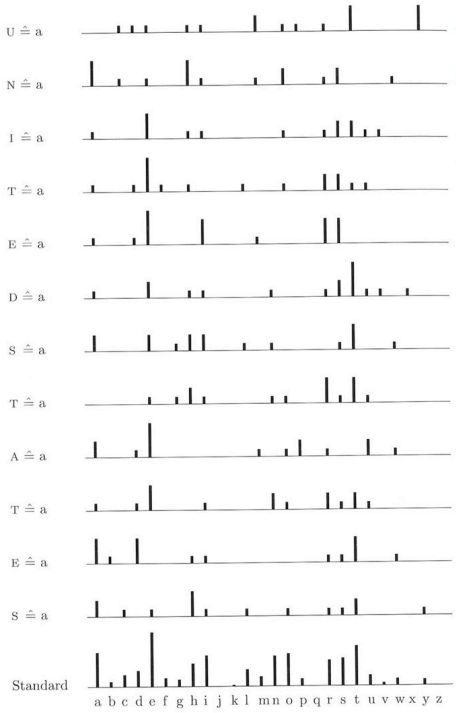
Frequency table of English



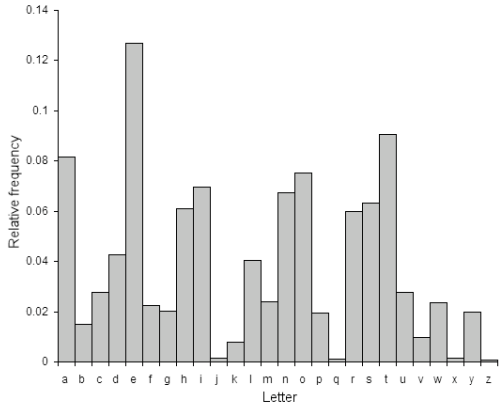
Decoding technique

1. Count the number of times each symbol appears in the cryptotext
2. Decode by matching with the frequency table

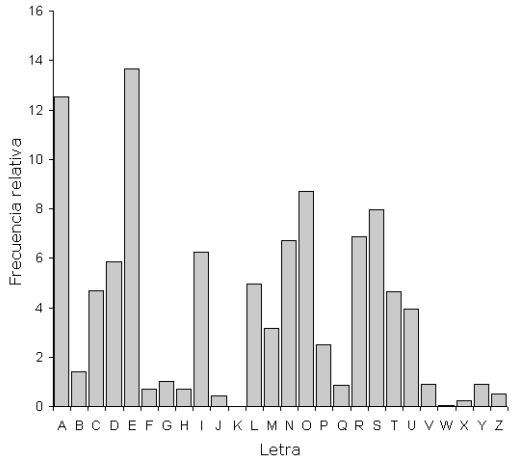




Other languages



English



Spanish

Stream ciphers

Principle

- Shift each letter of the cryptotext differently
- Caesar's cipher with different key for each letter
- Key = shift sequence

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

Plaintext	HELLO
Key	23582
Cryptotext	JHQTQ

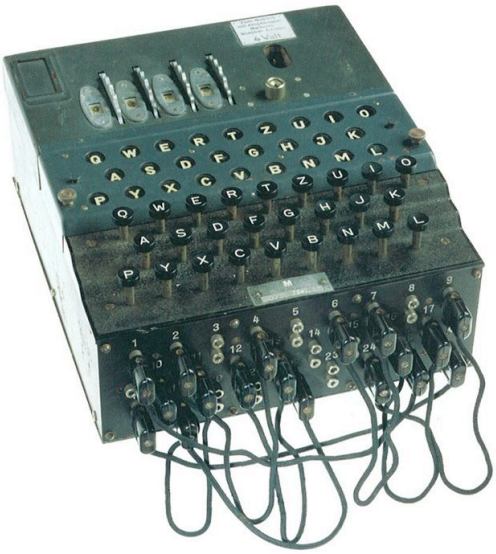
Other representation of the key

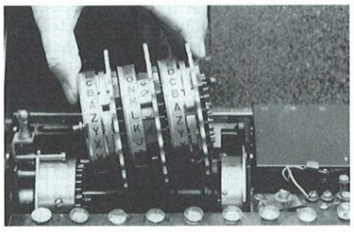
	AAAAA
Key	23582
Key	CDFIC

Vigenère table

	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

The ENIGMA machine





- Mechanical + electrical encoding
- Series of substitution ciphers
- Polyalphabetic substitution
- Invented by Arthur Scherbius, 1919
- Extensively used in WWII

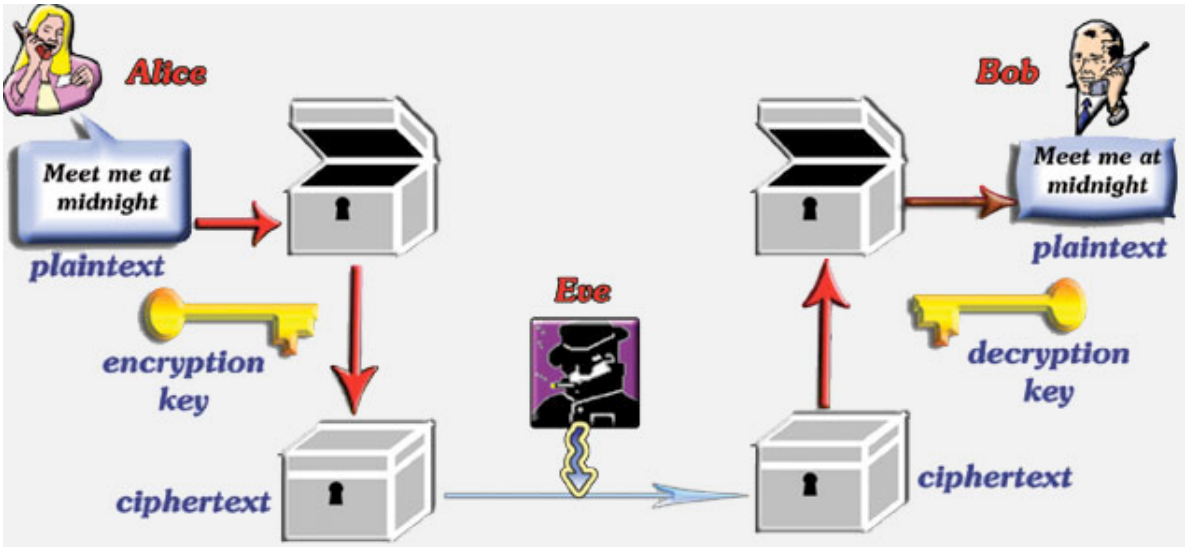
The code breakers of Bletchley Park

- Home of the British decrypting efforts during WWII
- Team led by British mathematician Alan Turing
- Broke the ENIGMA machine
- Now a museum: bletchleypark.org.uk

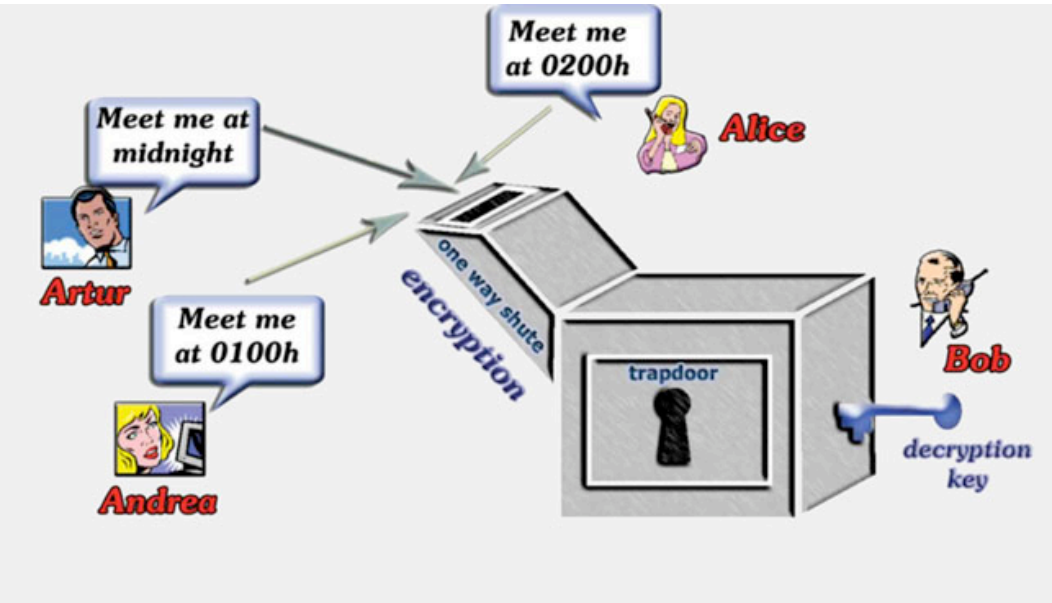
Applications of cryptography

- Internet (secure sites)
- WiFi connections
- Credit cards
- Information storage
  (hard drive encryption)
- Military/government communications

Private key cryptography



Public key cryptography



Further reading

All used for preparing this presentation.

- Fred Piper and Sean Murphy
  Cryptography: A Very Short Introduction
  Oxford University Press, 2002.
- Simon Singh
  The Code Book: The Secret History of Codes and Code-Breaking
  Fourth Estate Publ., 1999.
- David Kahn
  The Code-Breakers
  Scribner Publ., 1996.
- F. L. Bauer
  Decrypted Secrets: Methods and Maxims of Cryptology
  Springer, 2000.

Web links

- http://codesandciphers.org.uk
- Bletchley Park Museum, Milton Keynes
  http://bletchleypark.org.uk
- Caesar cipher
  http://secretcodebreaker.com/caesar.html
- Letter frequencies
  http://en.wikipedia.org/wiki/Letter_frequencies
  http://en.wikipedia.org/wiki/Frequency_analysis_(cryptanalysis)
- ENIGMA machine
  http://en.wikipedia.org/wiki/Enigma_machine