Cryptography

Mathma Talk
Science Lecture Theatre.
1900. Tuesday 23rd February 2016.

Dr Andrew French

References & further reading

The (Quantum) future of cryptography

Privacy vs security

Recent legislation

Ethical issues

Cryptography

The study and practice of techniques for secure communication
In other words, the reading and writing of SECRET CODES*

A brief history of Cryptography

Case studies

1. Substitution cipher
2. Frequency analysis & code breaking
3. Vigenère & polyalphabetic ciphers
4. Steganography
5. Enigma & the story of Bletchley Park
6. Modern encryption & internet security

*this is the *colloquial* meaning of *code*
In **cryptography**, *code* means a transformation of a *word* or *phrase*. e.g. 'CAT' becomes 'MOUSE'. A *cipher* is the transformation of individual *characters*, or even *bits* of data. e.g. CODE → DPEF

A brief history of cryptography

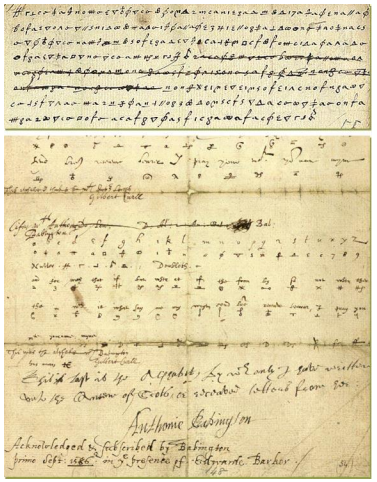
Cryptography, the study and practice of techniques for secure communication, is related to *Cryptanalysis* (from the Greek *kryptós*, "hidden", and *analýein*, "to loosen" or "to untie“) which is the study of the systems used for cryptography.

Cryptography is therefore the study of *codes*, *ciphers, algorithms* (mathematical recipes) and *computational machines*

The ATBASH Cipher

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

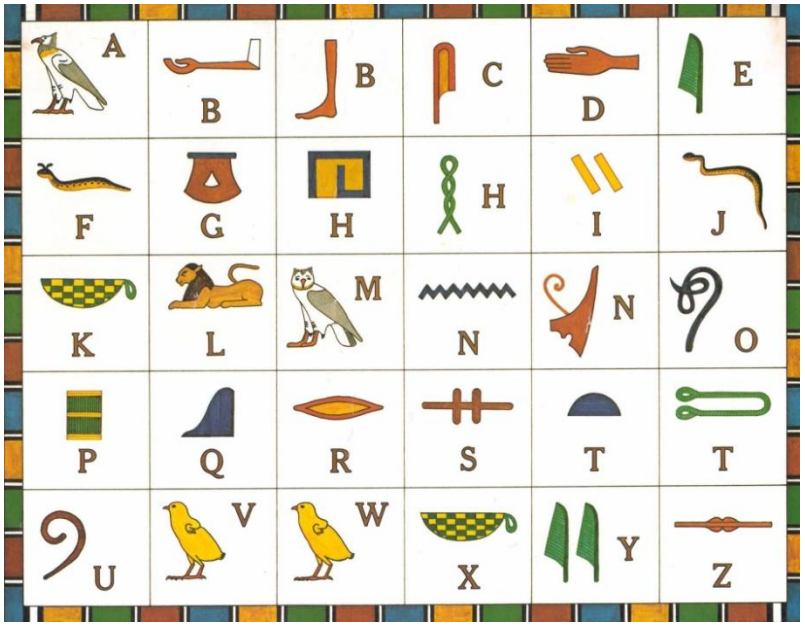
Ancient
1900BC – 850AD
Egyptian
Sumerian
Hebrew
Greek/Roman
Arabic



Medieval – Renaissance
1300-1800

20th Century
WWI,WWII
code breaking
Enigma
RSA
Birth of the internet

21st Century
Growth of the internet
Secure Wi-Fi
Quantum cryptography



The ATBASH Cipher

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

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

Scytale

1900 BC Non-standard hieroglyphs in the *Old Kingdom of Egypt*
(Hieroglyphs themselves translated via the *Rossetta Stone* by Champollion/Young 1820)

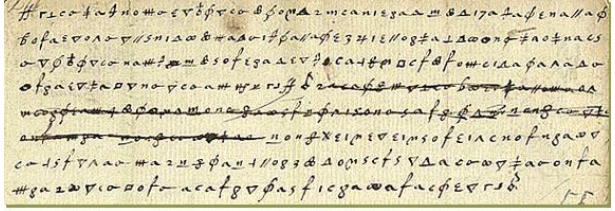
1500 BC
Mesopotamian recipe for pottery glaze

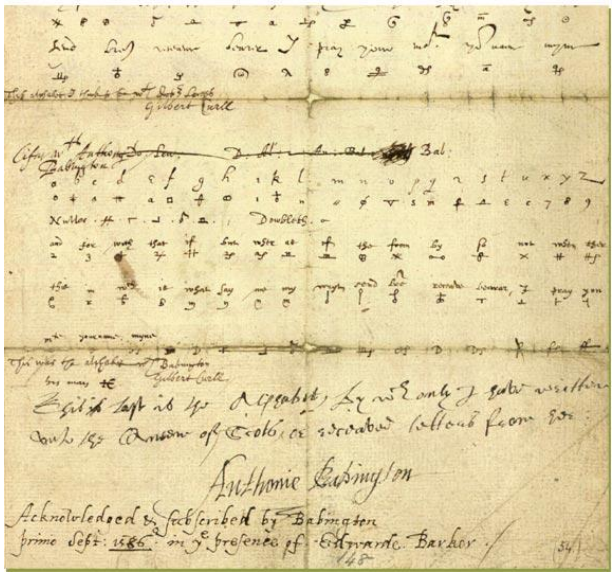
600-500 BC
Hebrew *Atbash* cipher

500BC – 450AD
Ancient Greek & Roman cryptography:

- *Scytale* transposition cipher
- *Caeser Shift* substitution cipher
- Secret messages tatooed on a slave's head that are hidden when the hair regrows i.e *steganography*

850AD Arabic / Muslim philosophy
Al-Kindi "*Manuscript on Deciphering Cryptographic Messages*"





1312-1361 Ibn al-Durayhim
1355-1418 Ahmad al-Qalqashandi
Frequency analysis, substitution ciphers

1404-1472 Leon Battista Alberti
1523-1596 Blaise de Vigènere
Polyalphabetic cipher

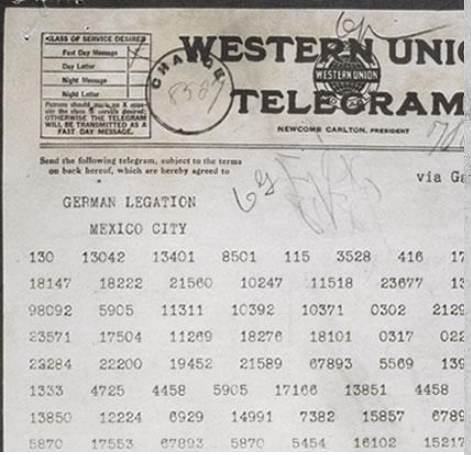
1586 Thomas Phelippes deciphers letters from Mary Queen of Scots relating to the 'Babingdon plot' to assassinate Elizabeth I

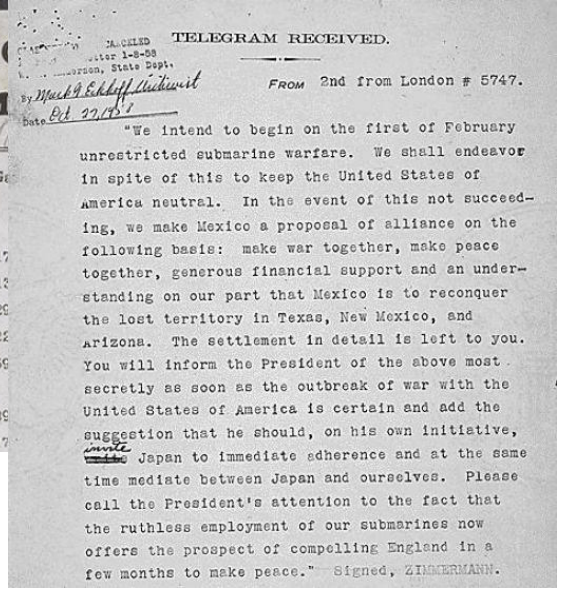
1600-1682 Antoine Rossignol & *The Great Cipher* (broken by Étienne Bazeries in 1900)

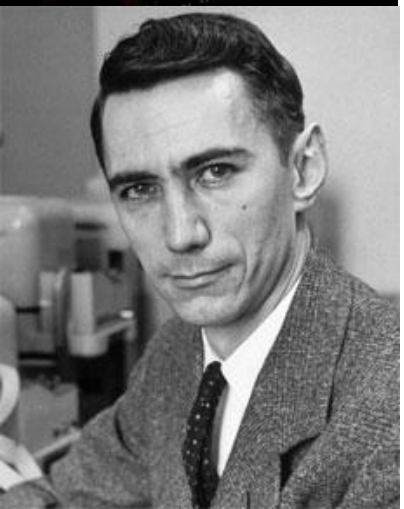
1860s Charles Babbage, Friedrich Kasiski break *le chiffre indéchiffrable*—"the indecipherable (polyalphabetic) cipher"

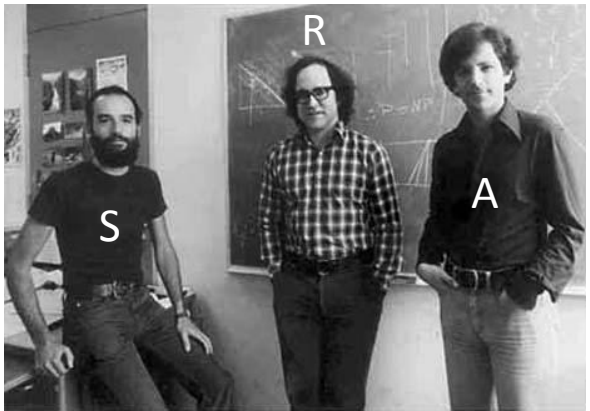
Blaise de Vigènere

Antoine Rossignol


WESTERN UNION
TELEGRAM
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416
18147 18222 21560 10247 11518 23677
98092 5905 11311 10392 10371 0302
23571 17504 11269 18276 18101 0317
23284 22200 19452 21589 67893 5569
1333 4725 4458 5905 17166 13851 4458
13850 12224 6929 14991 7382 15857
5870 17553 67893 5870 5454 16102


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 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.





1917
Breaking the encoded *Zimmermann Telegram* brought the USA into WWI

1919 UK Government Communications Headquarters (GCHQ) founded

1940s
Enigma and *Lorenz* ciphers broken by the Allies at Bletchley Park during WWII

1945 Claude Shannon "A mathematical theory of cryptography"

1952 US National Security Agency (NSA) founded

1970s Data Encryption Standard (DES)

1976 Public Key Cryptography, RSA
(Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman)

1970s-1990s Network infrastructure developed that became the **Internet**

*Wired Equivalent Privacy (**WEP**) is a security algorithm for IEEE 802.11 wireless networks.

1989 Tim Berners-Lee invents the World Wide Web (WWW)

Mid 1990s
Exponential expansion of the Internet

2000s
Secure Socket Layer (SSL)
WEP* Wi-Fi encryption

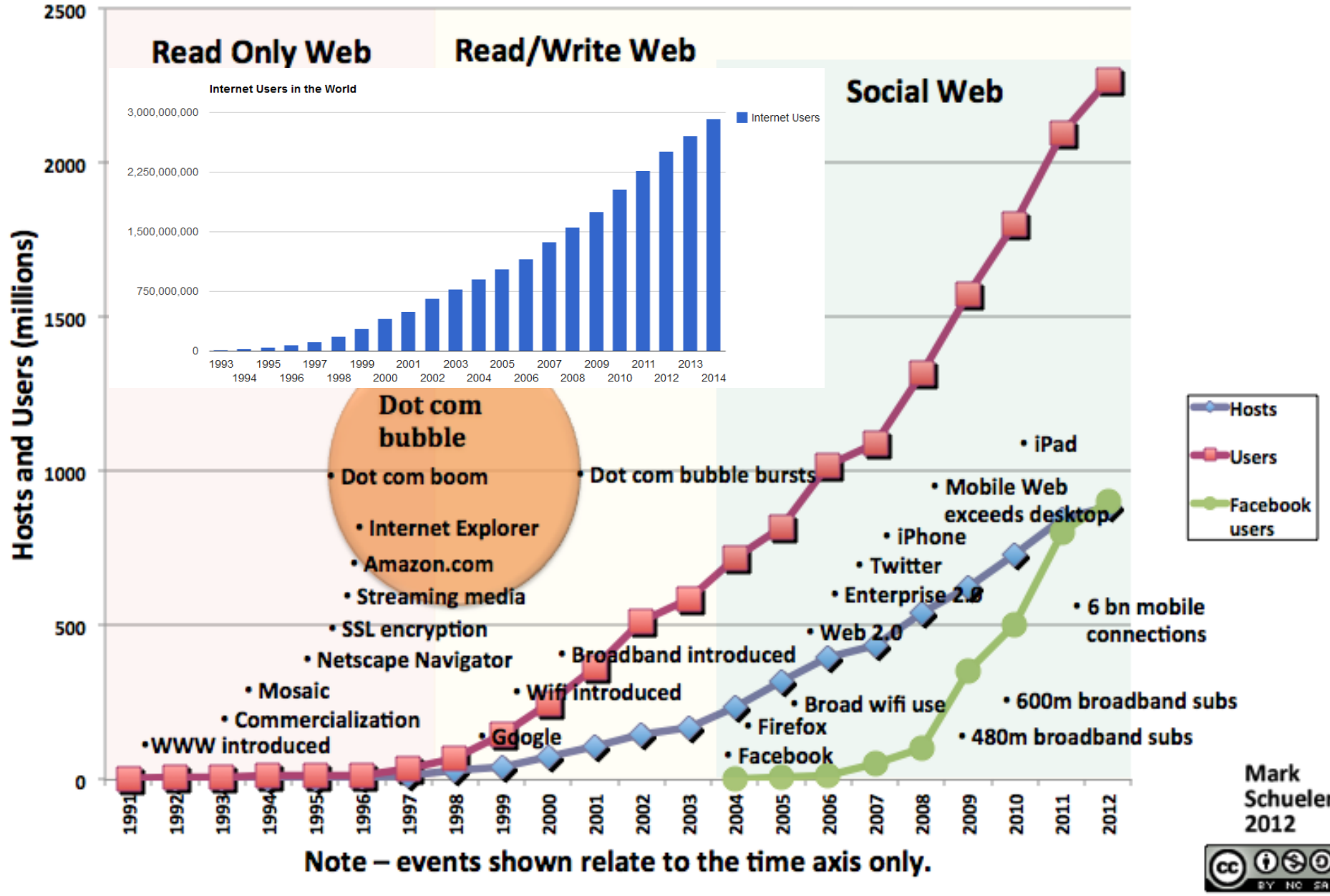
2001 Advanced Encryption Standard (AES)

2011 *Tempora* (formerly) secret fibre-optic cable internet mass 'wiretap' by GCHQ, NSA etc

2014 First commercial quantum cryptography system

2013 Edward Snowdon discloses NSA classified documents

Internet Growth - Usage Phases - Tech Events



Mark Schueler 2012

Case study #1: The substitution cipher

A cipher transforms the letters of a **plaintext** from one **alphabet** to another
It is important the **plaintext alphabet** and **cipher alphabet** are *shuffled* versions of the same letters, otherwise decryption could not occur unambiguously

```
This is not a very secret message
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

plaintext

↓

Encryption, using the **cipher key**

↓

```
Uijt jt opu b wfsz tfdsfu nfttbhf
BCDEFGHIJKLMNOPQRSTUVWXYZA
```

ciphertext

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz

BCDEFGHIJKLMNOPQRSTUVWXYZA
bcdefghijklmnopqrstuvwxyza
```

plaintext alphabet

cipher alphabet

In this example
a *Caesar Shift* is used
i.e. an 'circular' alphabetic shift by one letter

a → b
b → c
z → a etc

Case study #1: The substitution cipher

Manual encryption of a plaintext using a substitution cipher is straightforward, but clearly tedious for messages of more than ten or so characters!
A *machine* is ideally suited for this repetitive task.

Note this 'machine' has encrypt and decrypt modes

View original and modified files in a text editor

Choose `.txt` file to encrypt using a standard windows explorer

Choose cipher key (encoded in a `.txt` file)

Generate random *polyalphabetic* cipher key (see Case Study 3)

Display encryption or decryption time.
0.006s for the previous example!

plaintext alphabet

```
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz
!.,"?#@><;:()£$%^&*_-{}[]~1234567890\/|+=
```

cipher alphabet

```
ptkq+|Rc,B%h^F.oW]>{~_;&ZQD8s#[3\unIUX2gw":=d$6/
5@1Cx!OKMzS(PYN<0y9mVJvH-Ar4*L)abi7}lTGE£j?ef
```

Extending the alphabet and randomizing the order can make a cipher harder to break.

However, repetitions of common words such as `and` can catalyse an attempt to find the cipher alphabet. In our case **`and`** → **`t8c`**. We could try the same for `of`, **`by`**, `to` etc.

Also, the *text structure* (sentence length, paragraphs) also gives clues to what is written

The Comedy of Errors **by** William Shakespeare

ACT I
SCENE I. A hall in DUKE SOLINUS'S palace.

Enter DUKE SOLINUS, AEGEON, Gaoler, Officers, **and** other Attendants
AEGEON
Proceed, Solinus, to procure my fall
And **by** the doom of death end woes **and** all.

2oB +#QBc@ #h ,II#IX **q@** d]&&]tQ Uot_BX3BtIB

p+2 W
U+,D, W! p ot&&]8 Rw~, Us;WDwU'U 3t&t|B!

,8gBI Rw~, Us;WDwUO p,^,sDO ^t#&BIO shh]|BIXO **t8c**
#goBI pggB8ct8gX
p,^,sD
[I#|BBcO U#&]8"XO g# 3I#|"IB Q@ ht&&
p8c **q@** goB c##Q #h cBtgo B8c $#BX **t8c** t&&!

To remove structure, we can incorporate the **line return** character into our alphabet i.e. `char(10)` or `char(13)` in many programming languages

ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

www.theASCIIcode.com.ar

most consulted

ñ	ényo, n with tilde	(alt + 164)
■	black square	(alt + 254)
2	superscript two, square	(alt + 253)
º	degree symbol	(alt + 248)
'	apostrophe, single quote	(alt + 39)
µ	letter Mu, micro, micron	(alt + 230)
©	copyright symbol	(alt + 184)
®	registered trademark	(alt + 169)
3	superscript three, cube	(alt + 252)
á	a with acute accent	(alt + 160)

frequently-used (spanish language)

ñ	alt + 164
Ñ	alt + 165
@	alt + 64
¿	alt + 168
?	alt + 63
¡	alt + 173
!	alt + 33
:	alt + 58
/	alt + 47
\	alt + 92

vowels acute accent (spanish language)

á	alt + 160
é	alt + 130
í	alt + 161
ó	alt + 162
ú	alt + 163
Á	alt + 181
É	alt + 144
Í	alt + 214
Ó	alt + 224
Ú	alt + 233

vowels with diaresis

ä	alt + 132
ë	alt + 137
ï	alt + 139
ö	alt + 148
ü	alt + 129
Ä	alt + 142
Ë	alt + 211
Ï	alt + 216
Ö	alt + 153
Ü	alt + 154

mathematical symbols

½	alt + 171
¼	alt + 172
¾	alt + 243
¹	alt + 251
³	alt + 252
²	alt + 253
ƒ	alt + 159
±	alt + 241
×	alt + 158
÷	alt + 246

commercial / trade symbols

$	alt + 36
£	alt + 156
¥	alt + 190
¢	alt + 189
¤	alt + 207
®	alt + 169
©	alt + 184
ª	alt + 166
º	alt + 167
°	alt + 248

quotes and parenthesis

"	alt + 34
'	alt + 39
(	alt + 40
)	alt + 41
[	alt + 91
]	alt + 93
{	alt + 123
}	alt + 125
«	alt + 174
»	alt + 175

The Comedy of Errors by William Shakespeare

ACT I
SCENE I. A hall in DUKE SOLINUS'S palace.

Enter DUKE SOLINUS, AEGEON, Gaoler, Officers, and other Attendants
AEGEON
Proceed, Solinus, to procure my fall
And by the doom of death end woes and all.

DUKE SOLINUS
Merchant of Syracuse, plead no more;
I am not partial to infringe our laws:
The enmity and discord which of late
Sprung from the rancorous outrage of your duke
To merchants, our well-dealing countrymen,
Who wanting guilders to redeem their lives
Have seal'd his rigorous statutes with their bloods,
Excludes all pity from our threatening looks.
For, since the mortal and intestine jars
'Twixt thy seditious countrymen and us,
It hath in solemn synods been decreed
Both by the Syracusians and ourselves,
To admit no traffic to our adverse towns Nay, more,
If any born at Ephesus be seen
At any Syracusian marts and fairs;
Again: if any Syracusian born
Come to the bay of Ephesus, he dies,
His goods confiscate to the duke's dispose,
Unless a thousand marks be levied,
To quit the penalty and to ransom him.
Thy substance, valued at the highest rate,
Cannot amount unto a hundred marks;
Therefore by law thou art condemned to die.

Encrypt →

← Decrypt

char(10),char(13)

plaintext alphabet

AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz!.,"?#@><;:()£$%^&*_-{}[]~1234567890\/|+=
y9$X*]qu}lok8IULMj>,R_sxViaNv6-F)d(rWOmQA"J/!<1\wBb@e#g
.hST+=H;D~:{7t3[z02c&YECK G%54|P^nZf?p£

ciphertext alphabet

mLl?*6iluB?6k?}rr6rO?XB?!jxxj9i?WL9_lOFl9rl?£p£py*
m?M£pW*}a}?M#?y?L9xx?jN?qAR}?WvsMaAW'W?F9x9
]l#£p£p}NQlr?qAR}?WvsMaAWg?y}8}vag?896xlrg?vkkj]l
rOg?9Nu?6QLlr?yQQlNu9NQO?£py}8}va?£p-
r6]llug?W6xjN"Og?Q6?Fr6]"rl?iB?k9xx£pyNu?XB?QLl?u
66i?6k?ul9QL?lNu?<6lO?9Nu?9xx#£p£pqAR}?WvsMaA
W?£pVlr]L9NQ?6k?WBr9]"Olg?Fxl9u?N6?i6rl=£pM?9i?
N6Q?F9rQj9x?Q6?jNkrjNIl?6"r?x9<OH£pmLl?lNijQB?9N
u?ujO]6ru?<Lj]L?6k?x9Ql£pWFr"NI?kr6i?QLl?r9N]6r6"O
?6"Qr9Il?6k?B6"r?u"_l£pm6?ilr]L9NQOg?6"r?<lxxzul9xj
NI?]6"NQrBilNg£p!L6?<9NQjNI?l"jxulrO?Q6?rlulli?QLljr
?xj/lO£pU9/l?Ol9x'u?LjO?rjI6r6"O?OQ9Q"QlO?<jQL?QLl
jr?Xx66uOg£p}\]x"ulO?9xx?FjQB?kr6i?6"r?QLrl9QlNjNI?
x66_O#£po6rg?OjN]l?QLl?i6rQ9x?9Nu?jNQlOQjNl?,9rO
£p'm<j\Q?QLB?OlujQj6"O?]6"NQrBilN?9Nu?"Og£pMQ?
L9QL?jN?O6xliN?OBN6uO?XllN?ul]rllu£p$6QL?XB?QLl?
WBr9]"Oj9NO?9Nu?6"rOlx/lOg£pm6?9uijQ?N6?Qr9kkj]
?Q6?6"r?9u/lrOl?Q6<NO?a9Bg?i6rlg£pMk?9NB?X6rN?
9Q?}FLlO"O?Xl?OllN£pyQ?9NB?WBr9]"Oj9N?i9rQO?9N
u?k9jrO=£pyI9jNH?jk?9NB?WBr9]"Oj9N?X6rN£p*6il?Q
6?QLl?X9B?6k?}FLlO"Og?Ll?ujlOg£pUjO?I66uO?]6NkjO]
9Ql?Q6?QLl?u"_l'O?ujOF6Olg£pANxlOO?9?QL6"O9Nu?i
9r_O?Xl?xl/jlug£pm6?d"jQ?QLl?FlN9xQB?9Nu?Q6?r9N
O6i?Lji#£pmLB?O"XOQ9N]lg?/9x"lu?9Q?QLl?LjILlOQ?r9
Qlg£p*9NN6Q?9i6"NQ?"NQ6?9?L"Nurlu?i9r_O=£pmLlrl
k6rl?XB?x9<?QL6"?9rQ?]6NuliNlu?Q6?ujl

```
fid = fopen( filename, 'r' ); %Open file filename (read only)

%Store filename text in a row vector A of characters, then close file
A = fscanf(fid, '%c'); fclose(fid);
```

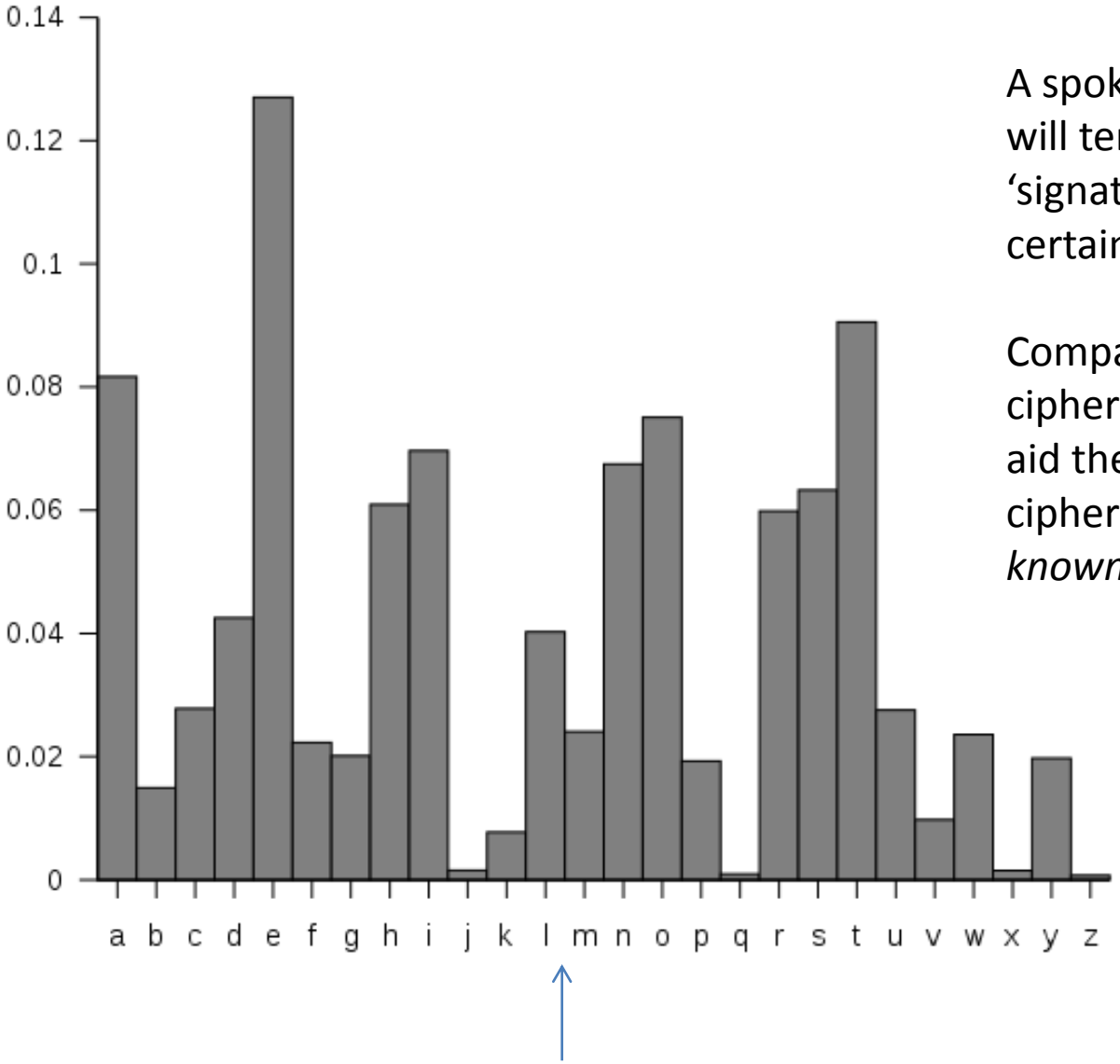
e.g A = 'The Comedy of Errors .....'

```
%Open file for writing
fid = fopen( strrep( filename,'.txt',['-',cipher_mode,'.txt'] ), 'w' );

%Step through cipher_key, replacing instances of the
%characters with their plaintext or enciphered equivalents
B = A; dim = size(cipher_key);
if strcmp(cipher_mode,'encrypt')==1
    %Encrypt file contents
    for n=1:dim(1)
        indices = strfind( A, cipher_key{n,1} );
        B(indices) = cipher_key{n,2};
    end
else
    %Decrypt file contents
    for n=1:dim(1)
        indices = strfind( A, cipher_key{n,2} );
        B(indices) = cipher_key{n,1};
    end
end

%Write encrypted character array B to a appended, then close file
fwrite(fid, B ); fclose(fid);
```

e.g. plaintext.txt would become plaintext-encrypt.txt

MATLAB code for `cipher.m`

Case study #2: Frequency analysis & code breaking

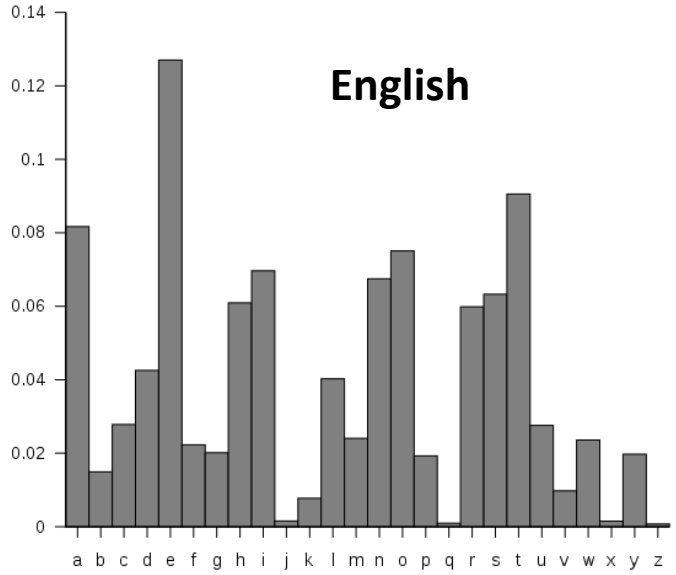


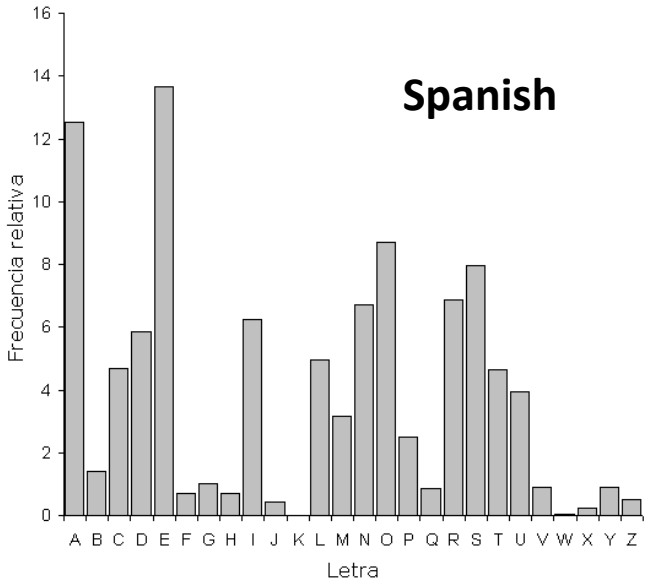
A spoken/written human language will tend to have a characteristic 'signature' regarding the usage of certain characters.

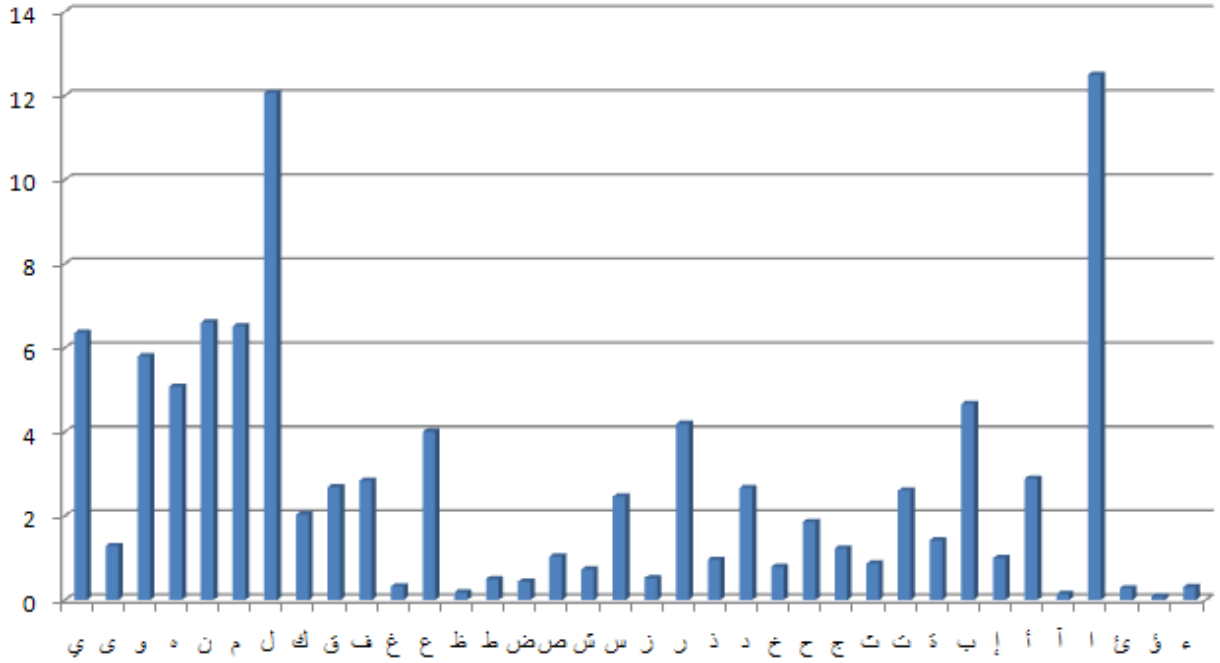
Comparing the **letter statistics** of a ciphertext with this signature can aid the process of deducing the cipher alphabet, *if the encryption is known to be a substitution cipher.*

Bar chart describing fractions of alphabetic characters in a typical extended piece of written English

Different languages have different character usage statistics i.e. different ‘signatures’

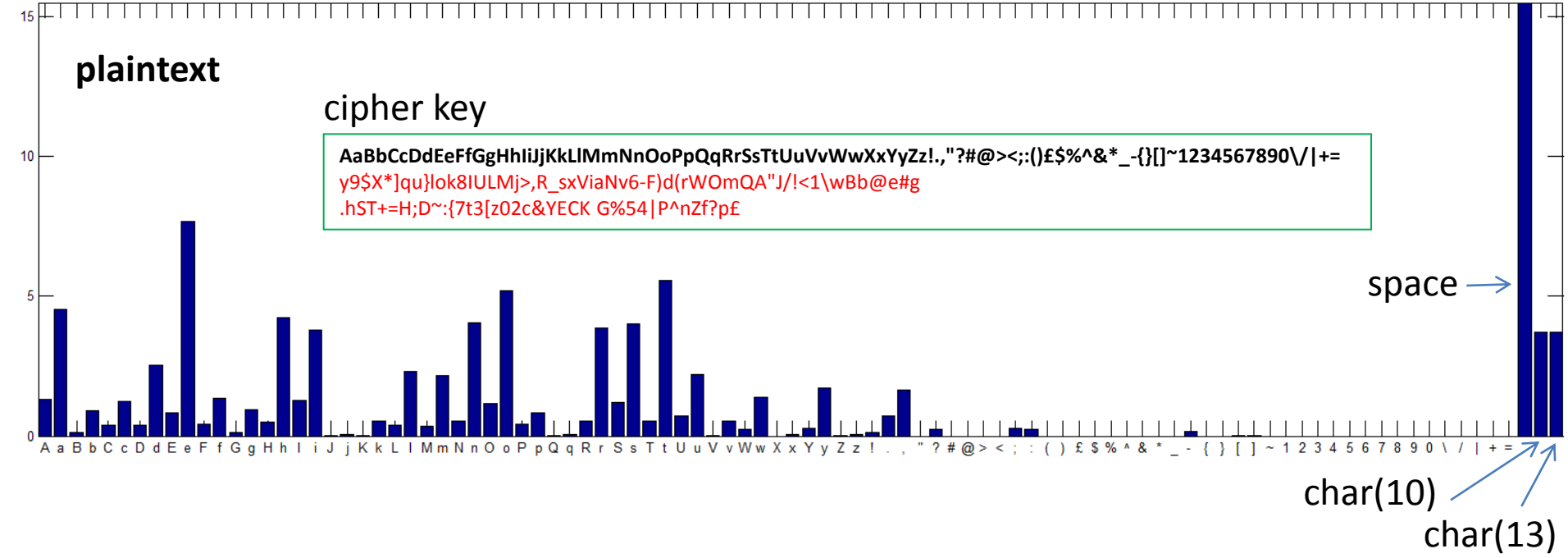






Arabic

Frequency analysis for *A Comedy of Errors*



Case study #3: Vigenère & polyalphabetic ciphers

How do we construct a code that is more resistant to frequency analysis? One answer is to use *more than one cipher alphabet.*

A **polyalphabetic** cipher *cycles* between *N* different alphabets in a fixed sequence. The first character of the plaintext is encoded with alphabet 1, the second character with alphabet 2 etc.

Example:

plaintext alphabet `abcdefghijklmnopqrstuvwxyz`
cipher alphabet 1 `cdefghijklmnopqrstuvwxyzab`
cipher alphabet 2 `mnopqrstuvwxyzabcdefghijkl`
cipher alphabet 3 `wxyzabcdefghijklmnopqrstuv`

These examples are Caesar Shifts of the plaintext alphabet

plaintext:

`a polyalphabetic cipher is harder to break`
`abcdefghijklmnopqrstuvqxyz`

ciphertext:

`c mqyvcymjnyggfe zkcege kf jnofro gl oognh`
`xdpagsdjvgmyjpbmsepvhsskvb`

So although we have **oo** in the ciphertext, this means *two* different letters in the plaintext

Case study #3: Vigenère & 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
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

Blaise de Vigènere
1523-1596
Diplomat,
Cryptographer,
Alchemist(!)

The Vigènere Square

i.e. *all* A-Z
Caesar Shift
cipher alphabets

Case study #3: Vigenère & 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
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 Vigènere Square can be used to generate cipher keys. The cycle of alphabets correspond to the repetition of a **codeword**.

If the codeword is POLY, alphabets are

#1: **P**QRSTUVWXYZABCDEFGHIJKLMNO
#2: **O**PQRSTUVWXYZABCDEFGHIJKLMN
#3: **L**MNOPQRSTUVWXYZABCDEFGHIJK
#4: **Y**ZABCDEFGHIJKLMNOPQRSTUVWX

plaintext:

MR VIGENERE WAS A VERY CLEVER CHAP
POLYPOLYPOLYPOLYPOLYPOLYPOLYPOLYPO
ABCDEFGHIJKLMNOPQRSTUVWXYZ
LYPOLYPOLYPOLYPOLYPOLYPOLY

Repetition of codeword POLY defines the alphabet used to encrypt the plaintext characters

ciphertext:

BF TXUPLTFP LOD P GCGM AASGCG NFPD
LZRRPDVVTHZZXLDDBPHHFTLLJX

Case study #3: Vigenère & polyalphabetic ciphers

The Vigenère cipher was thought to be *le chiffre indéchiffrable*—
"the indecipherable cipher"

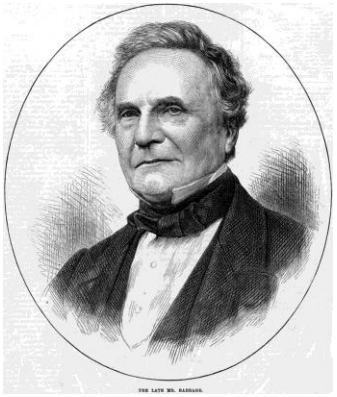
However, an attack was devised in the 1860s by Charles Babbage and Friedrich Kasiski.

It is based upon finding **repeated strings** of characters with the ciphertext. This can be used to work out the **repeat length** of a polyalphabetic cipher.

(For the previous example of codeword `POLY`, the repeat length is 4)

Once this is known, characters can be separated out, with each set corresponding to a unique alphabet.

Frequency analysis can then be used to work out each of the cipher alphabets.



Charles Babbage
1791-1871

Inventor of the first programmable
(mechanical) computer

Case study #4: **Steganography -** *the practice of concealing messages or information within other non-secret text or data*

If one receives an obviously encrypted message, one's interest is immediately piqued.....
It is perhaps preferable to *hide* a secret message in *normal communications.*
The secret bit is *not expected*, and hence is overlooked.

In ancient times, a message might be tattooed on the head of a slave.
The slave could be sent to the recipient after a hair regrowing period,
who would know to shave the slave upon arrival.

Other physical examples of steganography might be the use of *invisible ink* (which is revealed using UV light or application of a chemical), *microdots*, or simply in a *letter*

*"**T**oday **h**er **i**nterest **s**oared, **i**n **S**pain **a** **s**eedy **E**uropean **c**orporate **r**ogue **e**ntered **T**oledo **c**arrying **O**lga's **d**istinctive **e**merald ..."*

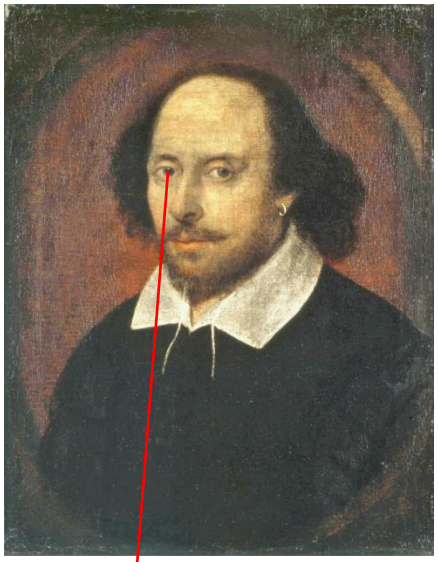
This iS a secreT cOde

However, this is all rather time consuming! The digital age provides us with an excellent method for hiding messages: *Photographs*

Case study #4: Modern steganography – concealing messages in digital photographs

What is the difference between these images?
The one on the left *also contains the entire works of Shakespeare.*

Case study #4: Modern steganography – concealing messages in digital photographs



Digital (colour) images consist of three matrices of numbers. These correspond to intensities of the colours Red, Green and Blue

A typical (JPEG) image from a 12 MegaPixel digital camera might have three 4000 x 3000 matrices of integer numbers within the range 0 ...255

Zooming in reveals the pixels

Blue matrix

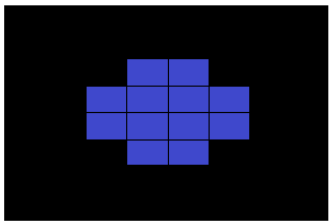
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	255	255	0	0	0
0	0	255	255	255	255	0	0
0	0	255	255	255	255	0	0
0	0	0	255	255	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

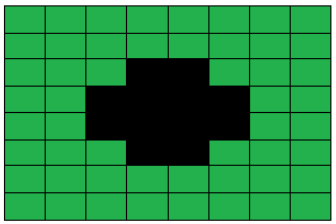
Green matrix

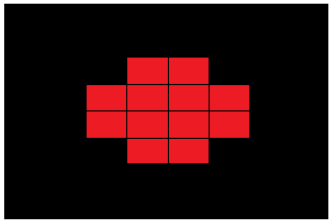
255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255
255	255	255	0	0	255	255	255
255	255	0	0	0	0	255	255
255	255	0	0	0	0	255	255
255	255	255	0	0	255	255	255
255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255

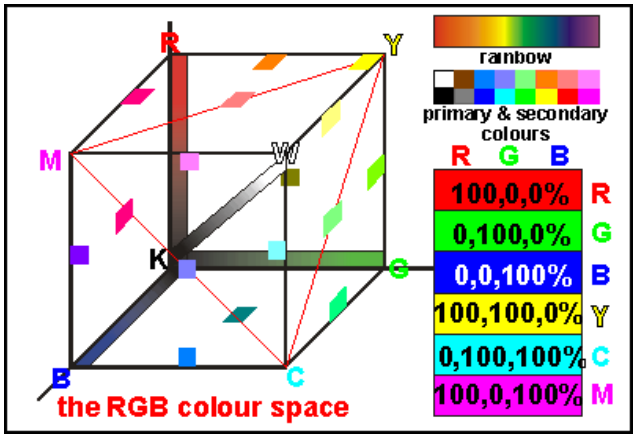
Red matrix

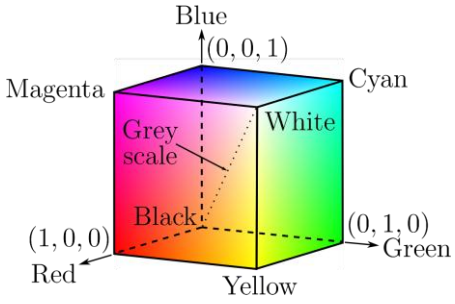
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	255	255	0	0	0
0	0	255	255	255	255	0	0
0	0	255	255	255	255	0	0
0	0	0	255	255	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0



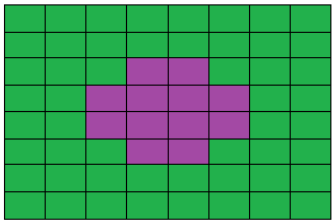








Resultant Image



Case study #4: Modern steganography – concealing messages in digital photographs

The trick of 'digital steganography' is to modify the R,G,B pixel values by a *small amount* corresponding to the ASCII codes of characters which form a message. The difference between an encrypted image and a 'genuine' one might be imperceptible to the human eye, but a computer can use the numerical difference to encode or extract a message.

The Project Gutenberg eBook of the *Complete Works of Shakespeare* contains **5,589,886** characters (which includes line returns and spaces).

Each character has an **ASCII code** between 0 and 255.

- To encode an image, use the three integers which make up the ASCII code of a character. For example `a` is **097**, therefore the numbers are **0,9,7**

- After making sure the maximum colour intensity is **246** (any R,G,B values above 246 are set at 246), I will **add** my three ASCII numbers, respectively, to the R,G,B values

- This means I can store **one character** of my **plaintext** in **every pixel in the image**.

Given a 6 million pixel image is fairly low-resolution these days, storing the *Complete Works of Shakespeare* is quite easy.

ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

www.theASCIIcode.com.ar

most consulted

ñ	ényе, n with tilde	(alt + 164)
■	black square	(alt + 254)
2	superscript two, square	(alt + 253)
º	degree symbol	(alt + 248)
'	apostrophe, single quote	(alt + 39)
µ	letter Mu, micro, micron	(alt + 230)
©	copyright symbol	(alt + 184)
®	registered trademark	(alt + 169)
3	superscript three, cube	(alt + 252)
á	a with acute accent	(alt + 160)

frequently-used (spanish language)

ñ	alt + 164
Ñ	alt + 165
@	alt + 64
¿	alt + 168
?	alt + 63
¡	alt + 173
!	alt + 33
:	alt + 58
/	alt + 47
\	alt + 92

vowels acute accent (spanish language)

á	alt + 160
é	alt + 130
í	alt + 161
ó	alt + 162
ú	alt + 163
Á	alt + 181
É	alt + 144
Í	alt + 214
Ó	alt + 224
Ú	alt + 233

vowels with diaresis

ä	alt + 132
ë	alt + 137
ï	alt + 139
ö	alt + 148
ü	alt + 129
Ä	alt + 142
Ë	alt + 211
Ï	alt + 216
Ö	alt + 153
Ü	alt + 154

mathematical symbols

½	alt + 171
¼	alt + 172
¾	alt + 243
¹	alt + 251
³	alt + 252
²	alt + 253
ƒ	alt + 159
±	alt + 241
×	alt + 158
÷	alt + 246

commercial / trade symbols

$	alt + 36
£	alt + 156
¥	alt + 190
¢	alt + 189
¤	alt + 207
®	alt + 169
©	alt + 184
ª	alt + 166
º	alt + 167
°	alt + 248

quotes and parenthesis

"	alt + 34
'	alt + 39
(	alt + 40
)	alt + 41
[	alt + 91
]	alt + 93
{	alt + 123
}	alt + 125
«	alt + 174
»	alt + 175

Case study #4: Modern steganography – concealing messages in digital photographs

Original image
e.g. 3000 x 2000 pixels

R: 155, G: 23, B: 190

Secret message e.g. 5,589,886 characters for the *Complete Works* ....

Each character converted to a three digit ASCII code. `a` is **097,** `A` **is 065**

Red colour
3000 x 2000 matrix
of values 0 .. 255

+0

Green colour
3000 x 2000 matrix
of values 0 .. 255

+6

Blue colour
3000 x 2000 matrix
of values 0 .. 255

+5

Step through the first 5,589,886 pixels of the 6,000,000 pixel image and add the ASCII code numbers to the R,G,B pixel values

Save the encoded image. It should look very similar!

R: 155, G: 29, B: 195

encoded

–

original

Compare the encoded image with an original. From the *differences* in R,G,B values work out the ASCII codes of the characters of the hidden message

64 x 82 pixel original image
(5248 pixels)

64 x 82 pixel encrypted image, with the first 5248 characters of *A Comedy of Errors*

The Comedy of Errors by William Shakespeare

ACT I
SCENE I. A hall in DUKE SOLINUS'S palace.

Enter DUKE SOLINUS, AEGEON, Gaoler, Officers, and other Attendants
AEGEON
Proceed, Solinus, to procure my fall
And by the doom of death end woes and all.

DUKE SOLINUS
Merchant of Syracuse, plead no more;
I am not partial to infringe our laws:
The enmity and discord which of late
Sprung from the rancorous outrage of your duke
To merchants, our well-dealing countrymen,
Who wanting guilders to redeem their lives
Have seal'd his rigorous statutes with their bloods,
Excludes all pity from our threatening looks.
For, since the mortal and intestine jars
'Twixt thy seditious countrymen and us,
It hath in solemn synods been decreed
Both by the Syracusians and ourselves,
To admit no traffic to our adverse towns Nay, more,
If any born at Ephesus be seen
At any Syracusian marts and fairs;
Again: if any Syracusian born
Come to the bay of Ephesus, he dies,
His goods confiscate to the duke's dispose,
Unless a thousand marks be levied,
To quit the penalty and to ransom him.
Thy substance, valued at the highest rate,
Cannot amount unto a hundred marks;
Therefore by law thou art condemned to die.

AEGEON
Yet this my comfort: when your words are done,
My woes end likewise with the evening sun.

DUKE SOLINUS
Well, Syracusian, say in brief the cause
Why thou departed'st from thy native home
And for what cause thou camest to Ephesus.

Plaintext stored via *steganography* in a 64 x 82 pixel image

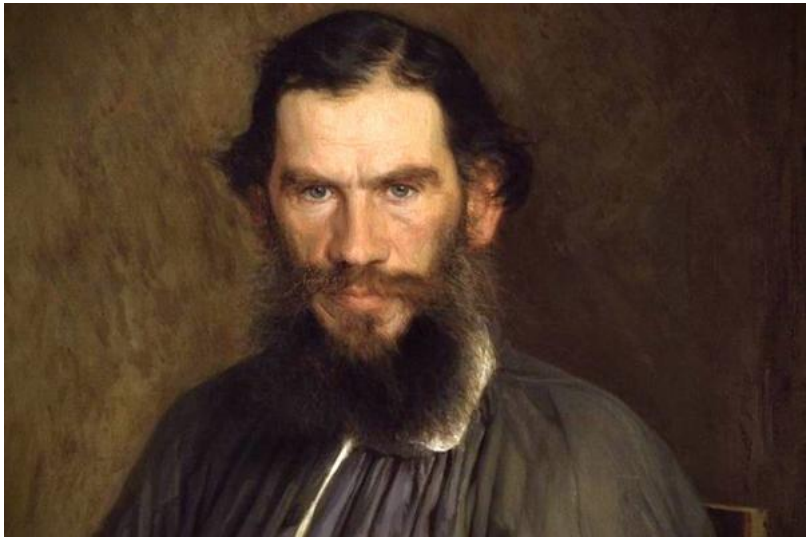
AEGEON
A heavier task could not have been imposed
Than I to speak my griefs unspeakable:
Yet, that the world may witness that my end
Was wrought by nature, not by vile offence,
I'll utter what my sorrows give me leave.
In Syracusa was I born, and wed
Unto a woman, happy but for me,
And by me, had not our hap been bad.
With her I lived in joy; our wealth increased
By prosperous voyages I often made
To Epidamnum; till my factor's death
And the great care of goods at random left
Drew me from kind embracements of my spouse:
From whom my absence was not six months old
Before herself, almost at fainting under
The pleasing punishment that women bear,
Had made provision for her following me
And soon and safe arrived where I was.
There had she not been long, but she became
A joyful mother of two goodly sons;
And, which was strange, the one so like the other,
As could not be distinguish'd but by names.
That very hour, and in the self-same inn,
A meaner woman was delivered
Of such a burden, male twins, both alike:
Those,--for their parents were exceeding poor,--
I bought and brought up to attend my sons.
My wife, not meanly proud of two such boys,
Made daily motions for our home return:
Unwilling I agreed. Alas! too soon,
We came aboard.
A league from Epidamnum had we sail'd,
Before the always wind-obeying deep
Gave any tragic instance of our harm:
But longer did we not retain much hope;
For what obscured light the heavens did grant
Did but convey unto our fearful minds
A doubtful warrant of immediate death;
Which though myself would gladly have embraced,
Yet the incessant weepings of my wife,

Weeping before for what she saw must come,
And piteous plainings of the pretty babes,
That mourn'd for fashion, ignorant what to fear,
Forced me to seek delays for them and me.
And this it was, for other means was none:
The sailors sought for safety by our boat,
And left the ship, then sinking-ripe, to us:
My wife, more careful for the latter-born,
Had fasten'd him unto a small spare mast,
Such as seafaring men provide for storms;
To him one of the other twins was bound,
Whilst I had been like heedful of the other:
The children thus disposed, my wife and I,
Fixing our eyes on whom our care was fix'd,
Fasten'd ourselves at either end the mast;
And floating straight, obedient to the stream,
Was carried towards Corinth, as we thought.
At length the sun, gazing upon the earth,
Dispersed those vapours that offended us;
And by the benefit of his wished light,
The seas wax'd calm, and we discovered
Two ships from far making amain to us,
Of Corinth that, of Epidaurus this:
But ere they came,--O, let me say no more!
Gather the sequel by that went before.

DUKE SOLINUS
Nay, forward, old man; do not break off so;
For we may pity, though not pardon thee.

AEGEON
O, had the gods done so, I had not now
Worthily term'd them merciless to us!
For, ere the ships could meet by twice five leagues,
We were encounterd by a mighty rock;
Which being violently borne upon,
Our helpful ship was splitted in the midst;
So that, in this unjust divorce of us,
Fortune had left to both of us alike
What to delight in, what to sorrow for.
Her part, poor soul! seeming as burdened
With lesser weight but not with lesser woe,
Was carried with more speed before the wind;
And in our sight they three were taken up
By fishermen of Corinth, as we thought.
At length, another ship had seized on us;
And, knowing whom it was their hap to save,
Gave healthful welcome to their shipwreck'd guests;
And would have reft the fishers of their prey,
Had not their bark been very slow of sail;
And therefore homeward did they bend their course.
Thus have you heard me sever'd from my bli

The Project Gutenberg eBook of *The King James Bible* (1,100,823 characters) stored in *The Last Supper* by Leonardo da Vinci



The Project Gutenberg eBook of *War & Peace* (3,291,645 characters) stored in a painting of Leo Tolstoy

The Project Gutenberg eBook of Arthur Conan-Doyle's *The Adventures of Sherlock Holmes* (594,930 characters) stored in a photograph of the actor Benedict Cumberbatch

Using MATLAB running on a Windows 7 (64bit) operating system (3.2GHz Intel i5, 8GB RAM) *War & Peace* took 4.4888 seconds to be encrypted. *The Adventures of Sherlock Holmes* took 2.4903s)

Case study #5: Enigma & the story of Bletchley Park

Images from http://www.bletchleypark.org.uk/

Bletchley Park housed the British codebreaking operation during WWII

A major challenge was posed by the **Enigma** and **Lorenz** encryption devices

The machines created at Bletchley to help break the codes are the *ancestors of modern computers*

1.59×10^{20} combinations for 3-rotor Enigma

Case study #5: Enigma & the story of Bletchley Park

Around **ten thousand people** worked at Bletchley Park and its associated outstations.

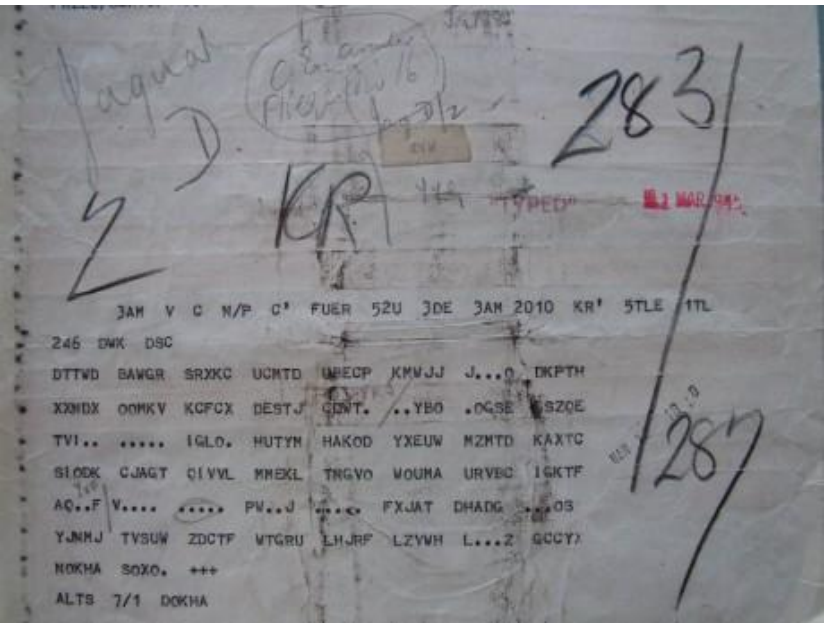
It is estimated that the codebreaking work may have shortened the war by *two years*, saving countless lives.

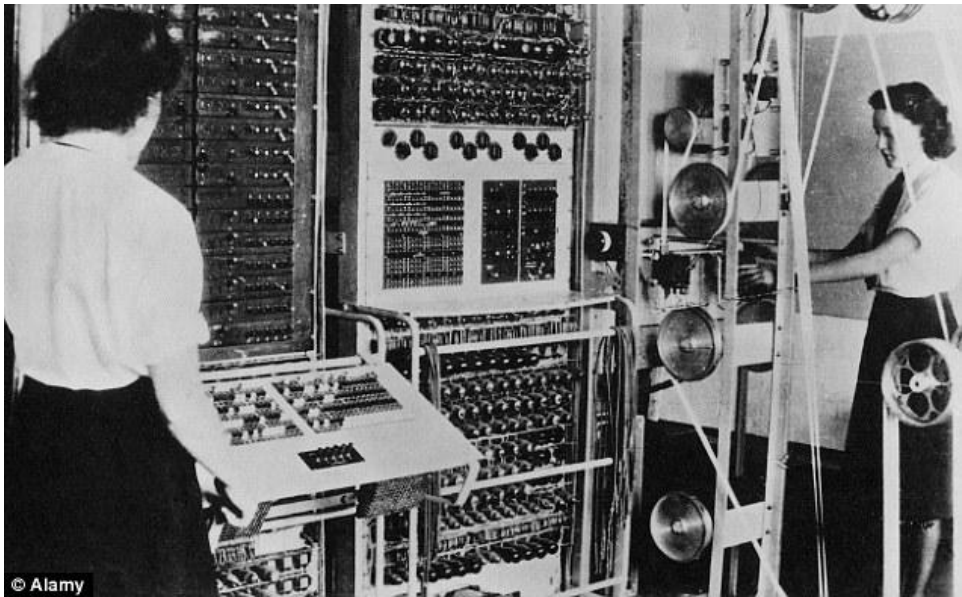
The success of the **D-Day landings** was in no small part due to a 'misinformation campaign' which misled the Axis about the intended target. This relied on not only breaking the **Enigma** code, but ensuring that the Axis were not aware that it had been broken.

Case study #5: **Enigma & the story of Bletchley Park**

‘Bombes’

‘Colossus’



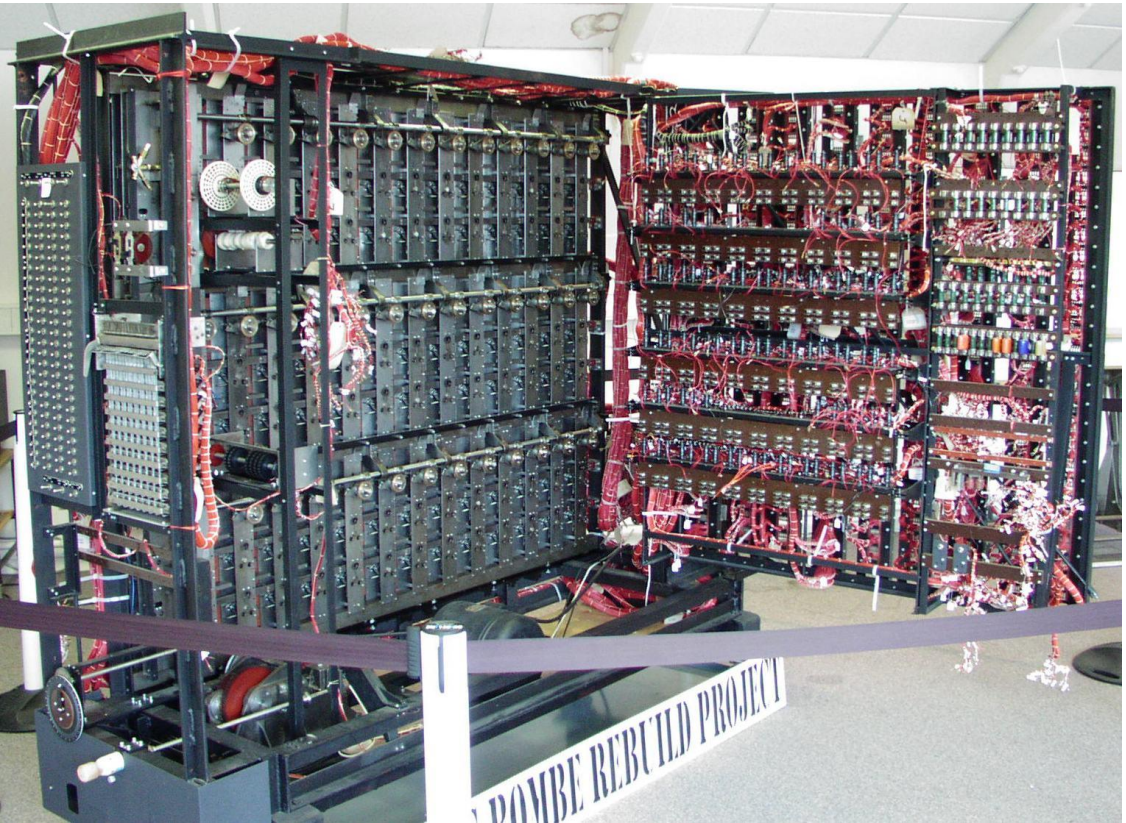


Case study #5: Enigma & the story of Bletchley Park

The Bombe machine was developed by **Alan Turing** and **Gordon Welchman** to speed up the breaking of Enigma.

The name was inspired by the 'bomba', an earlier machine used by the Polish *Cypher Bureau*.

Alan Turing
1912 - 1954



Bombes were used to identify Engima rotor settings that led to *contradictions* in the decryption of an intercepted plaintext. With these settings removed, a more manageable number could be investigated.

Case study #6: Modern encryption & internet security

Alice and Bob can communicate securely if they ***both have the same cipher key***. e.g a polyalphabetic cipher, based upon random alphabets with a large repeat sequence, will be computationally hard to break. In fact, a '**one time pad**', where a plaintext is encoded with a random alphabet the *same length* as the plaintext, is *impossible* to break.

However, how do you securely communicate the cipher key? (e.g. the randomized alphabets in the polyalphabetic cipher)

Communication channel (e.g. fibre optic cable, wireless link etc)

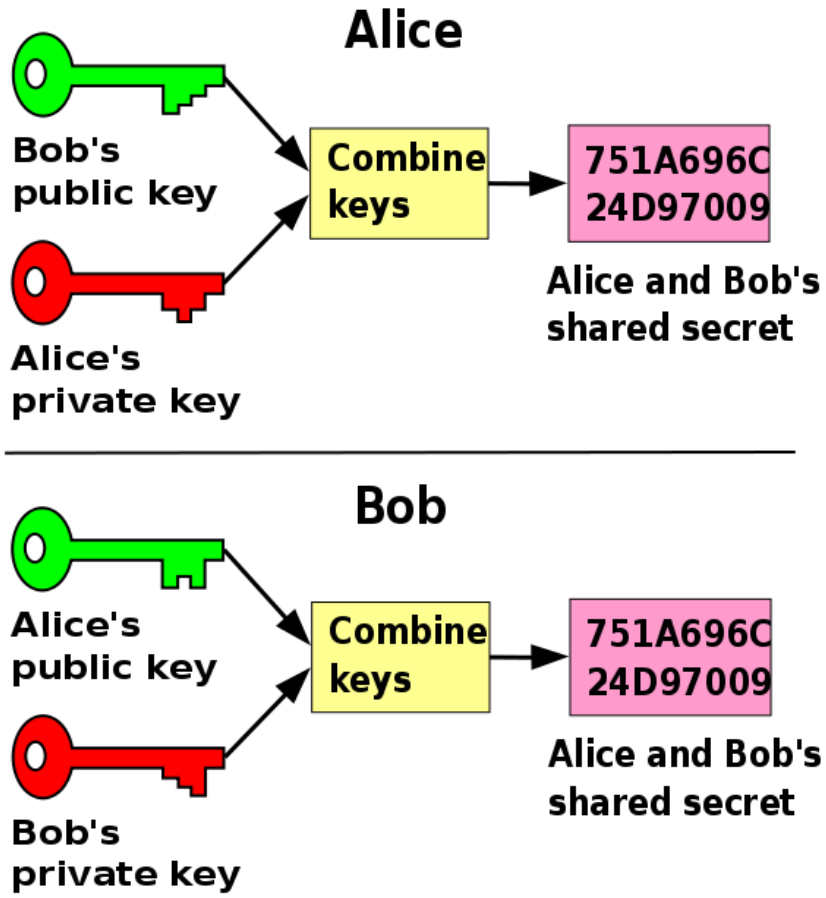
ALICE

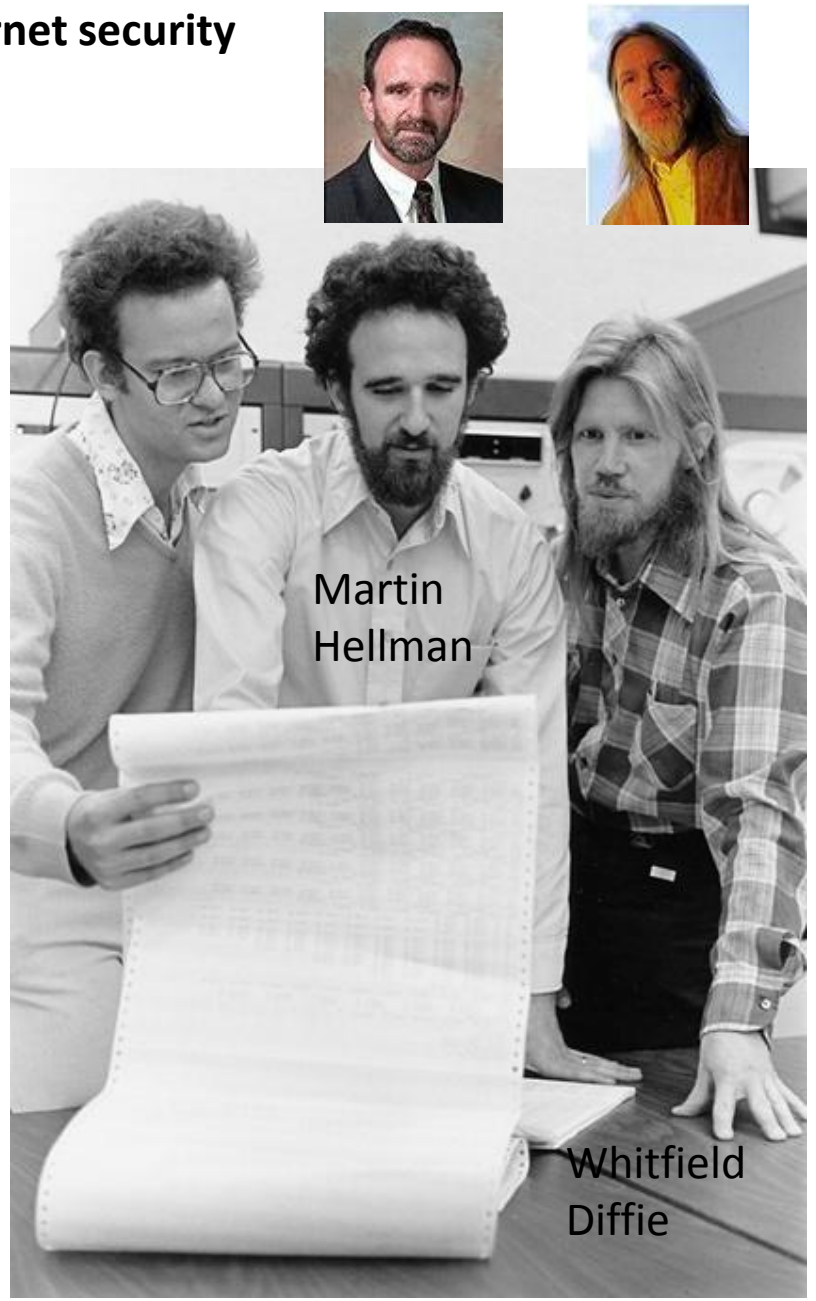
EVE

BOB

Case study #6: Modern encryption & internet security

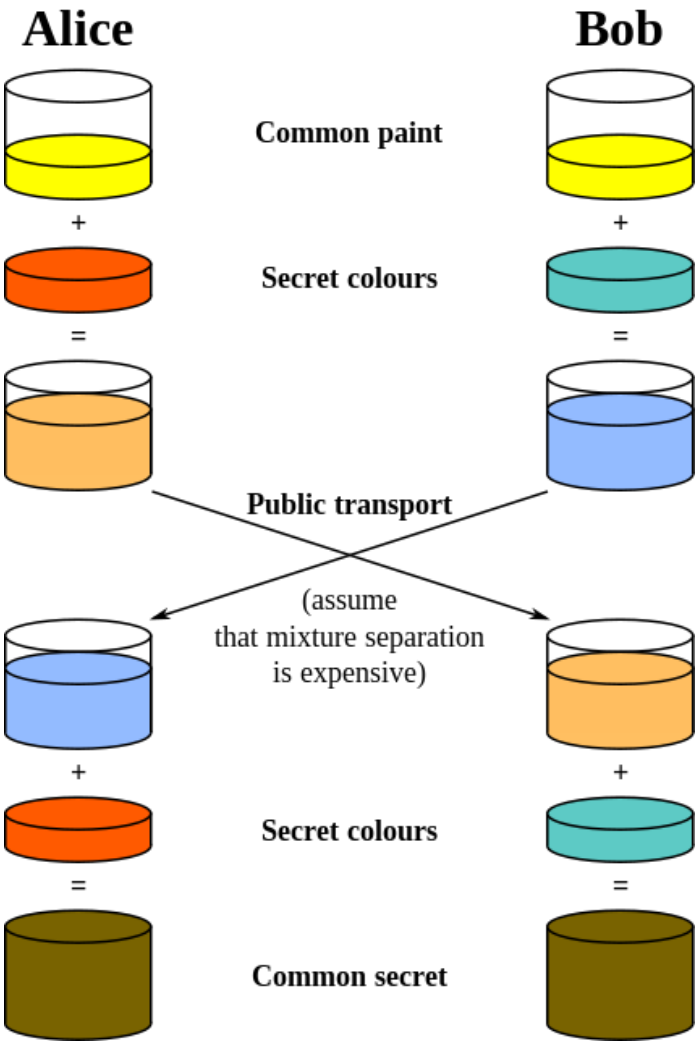
A solution, via the **Diffie-Hellman key exchange protocol** (1976) is to use an *algorithm* which generates the same key, but from *different secret parts* which are not communicated on their own.





Case study #6: Modern encryption & internet security

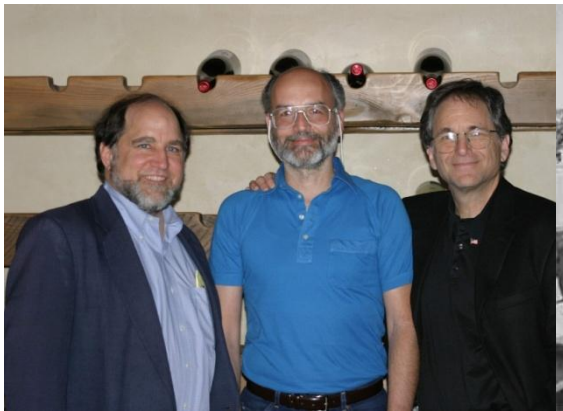
Ron Rivest, Adi Shamir, and Leonard Adleman proposed the **RSA algorithm** for performing the **Diffie-Hellman key exchange** in 1977

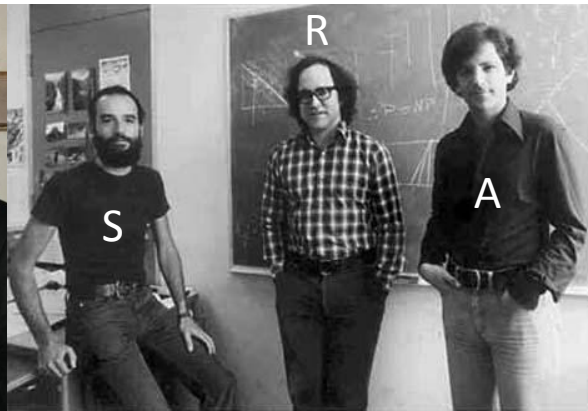


A paint-mixing analogy of the **Diffie-Hellman key exchange**

Clifford Cocks discovered the RSA algorithm *three years earlier* .... but he worked for GCHQ so he had to keep it secret till 1997!

RSA : Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman





Alice chooses two *secret* prime numbers *p, q* e.g. $p=17, q=11$

Alice's **Public Key**

Publish $N = pq$ and another prime number e

e.g. $N = 17 \times 11 = 187$

$e = 7$

Bigger primes mean *much more security* as *N* will be harder to factorize

N, e

Bob encodes a message into a number *M*
e.g. the decimal ASCII code for the letter X is

$M = 88$

Enciphered message **to Alice** is:

$C = M^e \pmod N$

e.g. $88^7 \pmod{187} = 11$

C

Alice computes *M* using

$M = C^d \pmod N$

s.t. $ed = 1 \pmod{(p-1)(q-1)}$

e.g. $7 \times 23 = 1 \pmod{16 \times 10}$

$\therefore d = 23$

$\therefore 11^{23} \pmod{187} = 88$

Only Alice can decrypt Bob's message because only she knows *p,q* whereas Bob only needs to know *N*

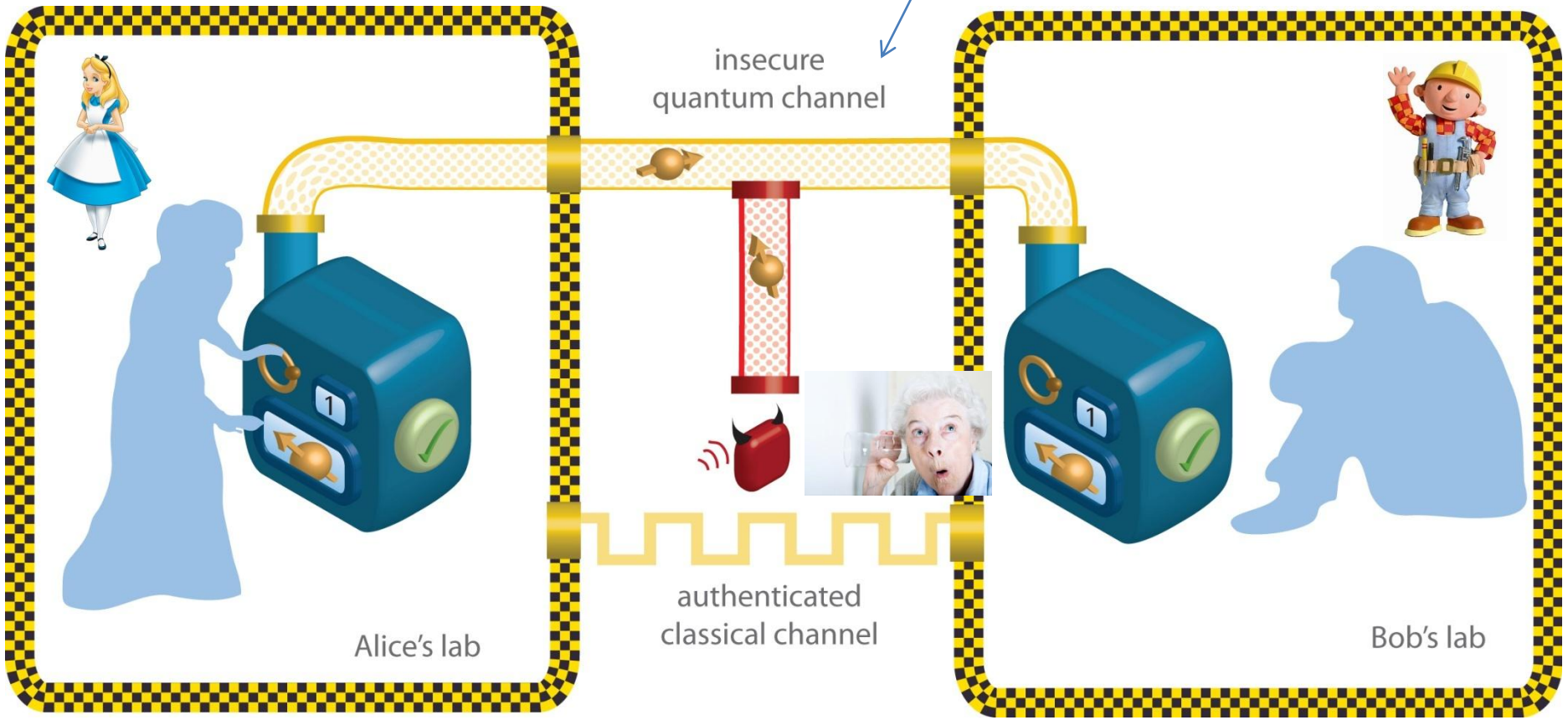
This works because exponentials in modular arithmetic are *one-way functions*
i.e. it is very hard to find *M* from *C* without *p,q*

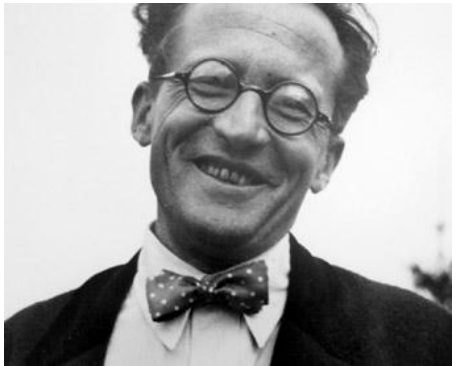
RSA uses **modular arithmetic**
x mod *y* = *x* – *ny* where *n* is an integer
e.g 32 mod **5** = **2** since **2** = 32 - 6 x **5**

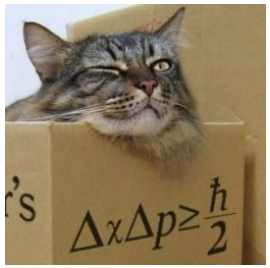
(Adapted from *The Code Book* by Simon Singh pp379)

The Quantum future of cryptography

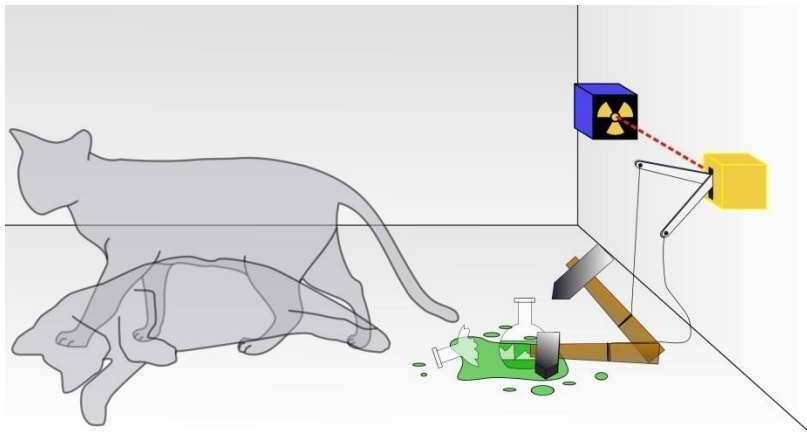
Here you can tell whether Eve has been listening!







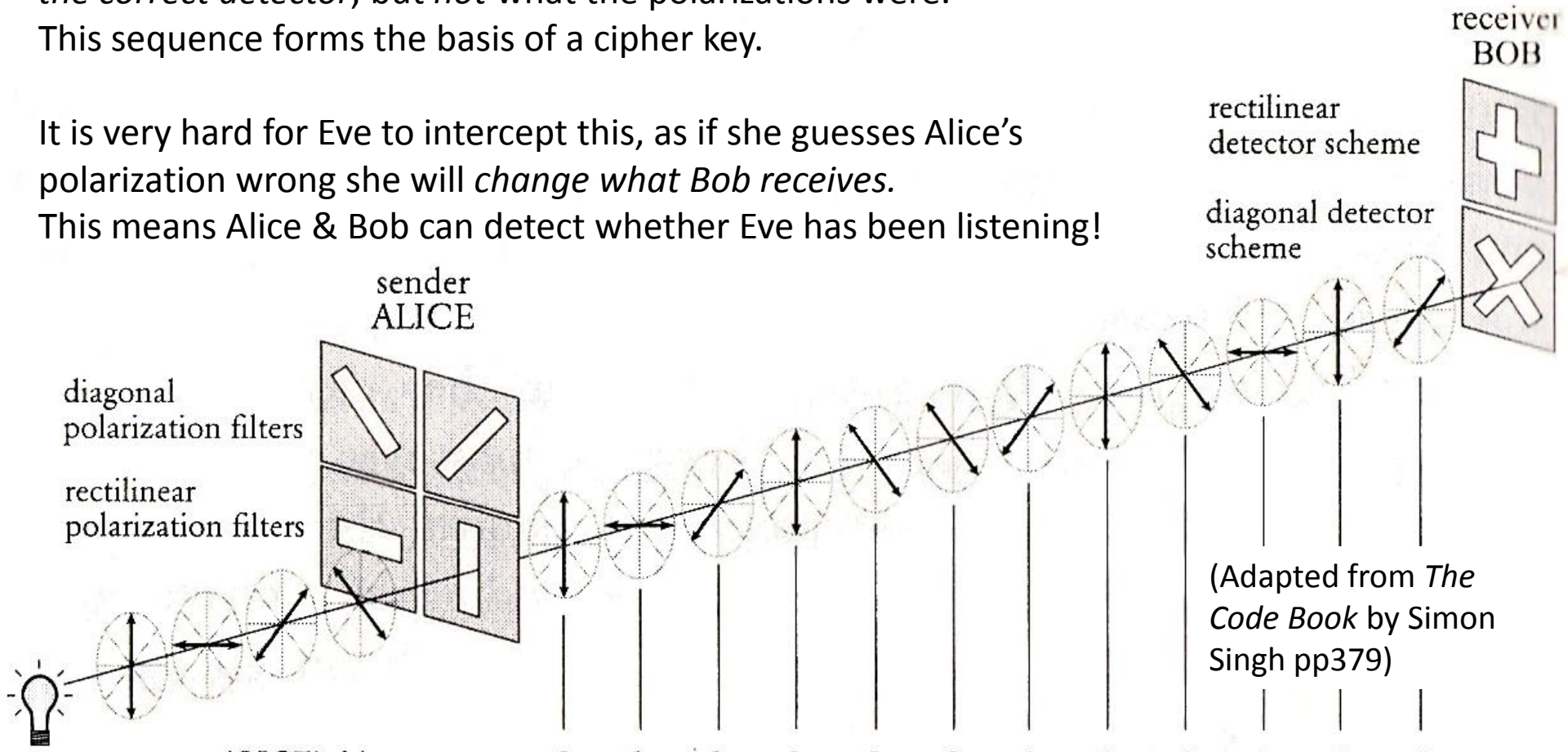
Erwin Schrödinger (1887-1961)



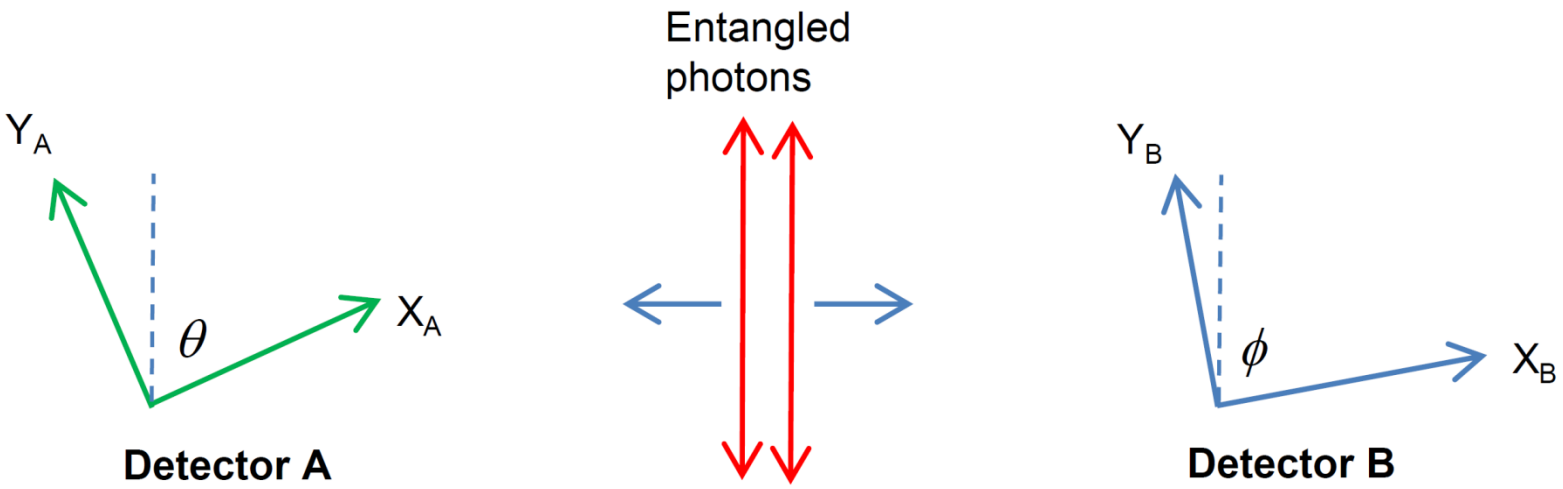
If you intercept a photon, you will force its polarization to be that of the detector.
In Quantum Mechanics your *act of measurement collapses the wavefunction.*

Alice sends Bob a message based upon photons of different polarizations.
Alice & Bob communicate to agree *which photons were intercepted with the correct detector*, but *not* what the polarizations were.
This sequence forms the basis of a cipher key.

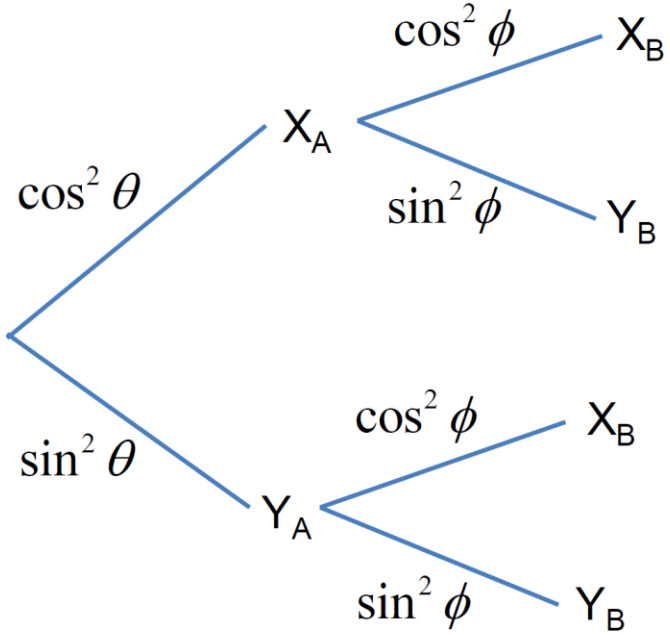
It is very hard for Eve to intercept this, as if she guesses Alice's polarization wrong she will *change what Bob receives.*
This means Alice & Bob can detect whether Eve has been listening!



(Adapted from *The Code Book* by Simon Singh pp379)



We shall assign probabilities for each detector's eigenstate to be based upon the statistics of the **classical limit** i.e. billions and billions of photons! In this case we expect Malus' Law to hold i.e. the square of the projection of the polarization yields transmitted power.



Classical scenario

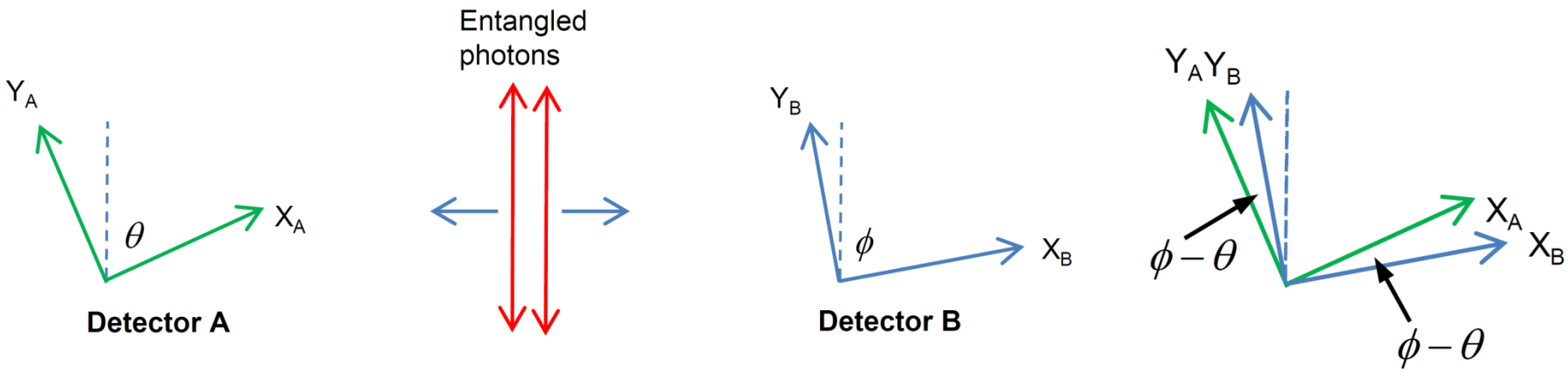
$$P(\text{match}) = P(X_A, X_B) + P(Y_A, Y_B)$$

$$P(\text{match}) = \cos^2\theta\cos^2\phi + \sin^2\theta\sin^2\phi$$

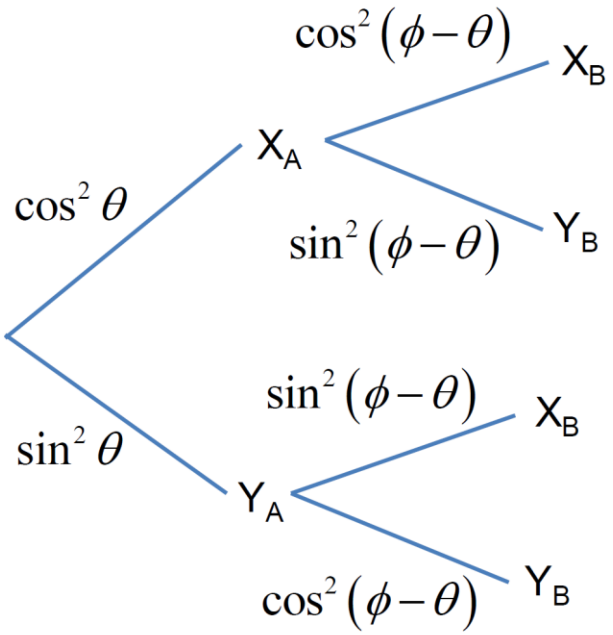
$$P(\text{mismatch}) = 1 - \cos^2\theta\cos^2\phi - \sin^2\theta\sin^2\phi$$

$$P(X_A) = \cos^2\theta, \quad P(Y_A) = \sin^2\theta$$

$$P(X_B) = \cos^2\phi, \quad P(Y_B) = \sin^2\phi$$



Alternatively, if we measure using detector A first, then QM says that the polarization will now be the measured eigenstate of detector A. This will *change the statistics of measurement of B*. This if course requires 'spooky action at a distance' between A and B....



Quantum scenario

$$P(\text{match}) = P(X_A, X_B) + P(Y_A, Y_B)$$

$$P(\text{match}) = \cos^2\theta\cos^2(\phi-\theta) + \sin^2\theta\cos^2(\phi-\theta)$$

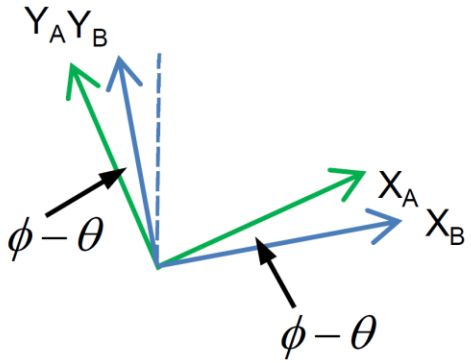
$$P(\text{match}) = (\cos^2\theta + \sin^2\theta)\cos^2(\phi-\theta)$$

$$\boxed{P(\text{match}) = \cos^2(\phi-\theta)}$$

$$P(\text{mismatch}) = 1 - \cos^2(\phi-\theta)$$

$$\boxed{P(\text{mismatch}) = \sin^2(\phi-\theta)}$$

Note we get the same match and mismatch probabilities if we measure B first. However, what happens if A and B detections are simultaneous?



Example:
Classical

$$\theta=-30^\circ,\ \phi=30^\circ$$

$$P(\text{mismatch})=1-\cos^2\theta\cos^2\phi-\sin^2\theta\sin^2\phi$$

$$P(\text{mismatch})=1-\left(\tfrac{\sqrt{3}}{2}\right)^2\left(\tfrac{\sqrt{3}}{2}\right)^2-\left(-\tfrac{1}{2}\right)^2\left(\tfrac{1}{2}\right)^2$$

$$P(\text{mismatch})=1-\tfrac{9}{16}-\tfrac{1}{16}=\frac{16-10}{16}=\boxed{\tfrac{3}{8}}$$

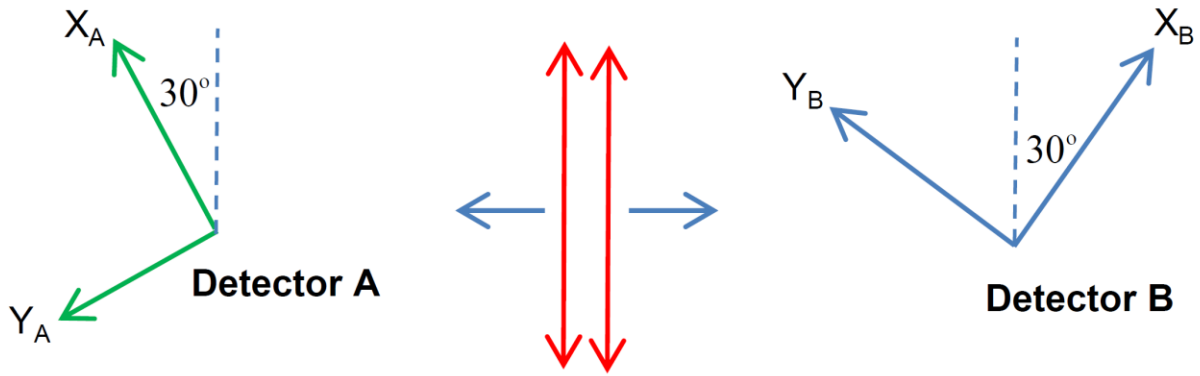
Example:
QM

$$\theta=-30^\circ,\ \phi=30^\circ$$

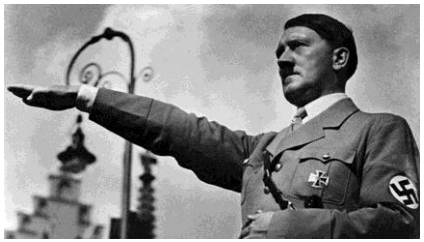
$$P(\text{mismatch})=\sin^2(\phi-\theta)$$

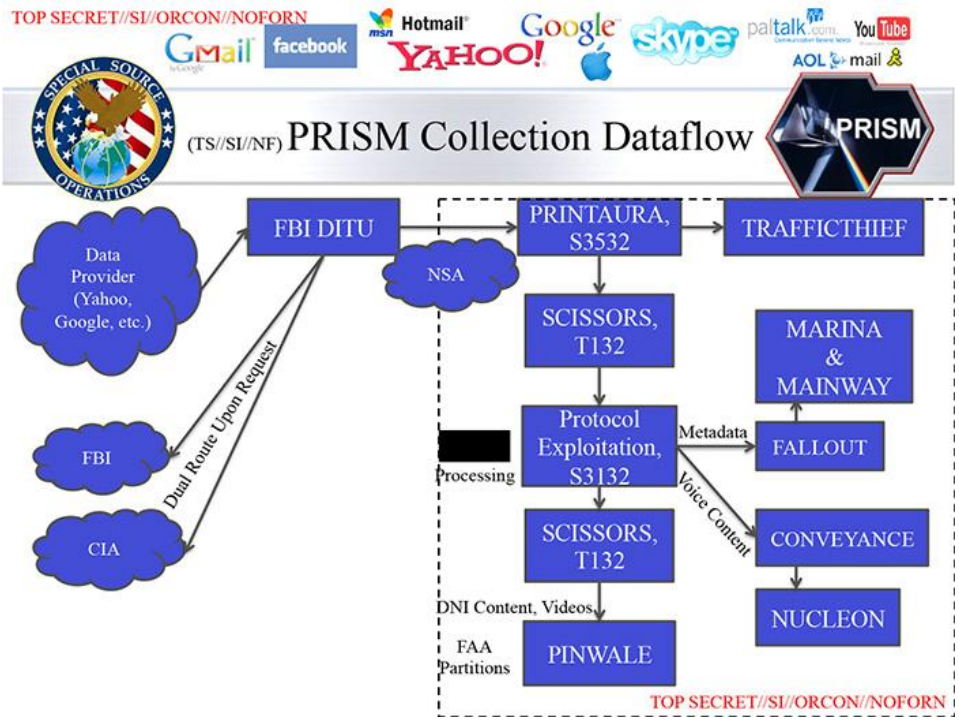
$$P(\text{mismatch})=\sin^2(60^\circ)=\tfrac{3}{4}=\boxed{\tfrac{6}{8}}$$

The difference between the probabilities is significant, and therefore readily measurable. For this scenario the QM prediction is that the fraction of mismatches between the detector strings XXXYYXXYXYYX... is *double* the classical prediction.



Ethical issues: Personal privacy vs national security?





Quis custodiet ipsos custodes?
"Who will guard the guards themselves?"
Juvenal, Satire VI, lines 347–8

Ethical issues: Current UK privacy law

Ian Hislop. Private Eye Editor

Article 8 of the **UK Human Rights Act 1998**
(from the **European Convention of Human Rights**)

Right to respect for private and family life:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

\+ **UK Data Protection Act 1998**
(Has National Security exemptions)

Need a **warrant** granted by the Home Secretary for a wiretap etc.
But monitoring of internet usage within the workplace *is legal* as a ***Lawful Business Practice.***


Sara Cox (Radio 1 DJ)

http://www.legislation.gov.uk/ukpga/1998/29/contents
http://findlaw.co.uk/law/z_articles-for-carousel/500284.html https://www.lawontheweb.co.uk/legal-help/right-to-privacy

"I concluded that however awful it may be, it's better to have a press which can expose MPs' private lives because it means we have a free press… It means we can expose corruption. Max Mosley has argued for the further advancement of the law whereas the editor of the *Daily Mail* newspaper Paul Dacre has accused Mr Justice Eady, the judge in the Mosley case, of bringing in a privacy law by the back door."

The Sun (2011)

Mark Oaten
Liberal Democrat Home Affairs Spokesman 2003-2006
MP for Winchester 1997-2010
Resigned from Liberal front bench due to a sex scandal published in the *News of the World* in 2006

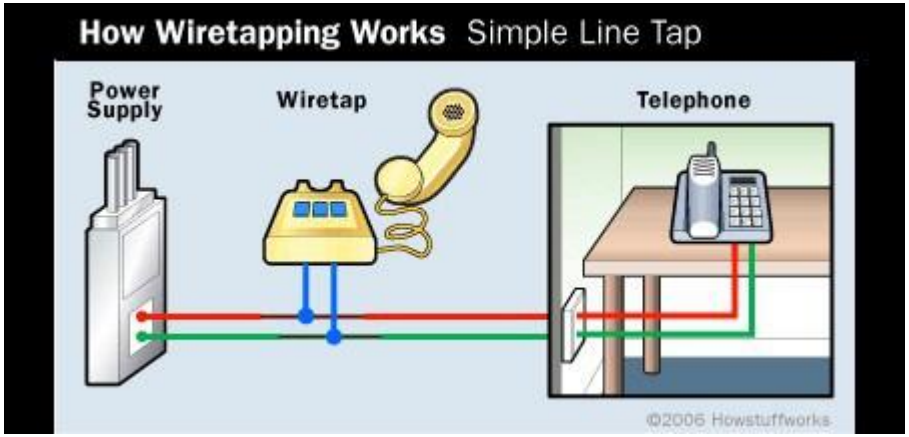
https://en.wikipedia.org/wiki/Privacy_in_English_law

Wainwright v. Home Office 2003

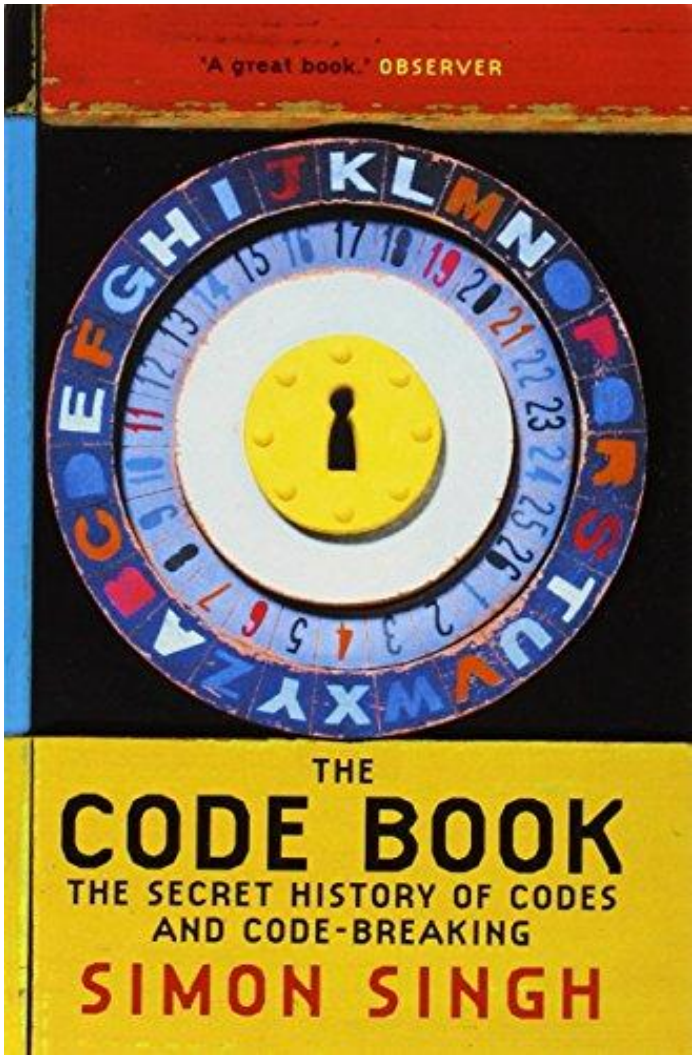
Article 8 – Privacy

- Mother and son stripped searched on prison visit for drugs
  - Breach of Prison Rules, humiliated and distressed
  - Son mentally impaired and developed PTSD
- Trespass against both persons had been committed. Son's "trespass" amounted to battery
  - Awarded £2,600 and £4,500 respectively
- Appealed trespass charges
  - No common law tort of invasion of privacy
  - Needed legislation not common law
  - Used ECHR and HRA 1998 to fill gaps

National security vs personal privacy ....



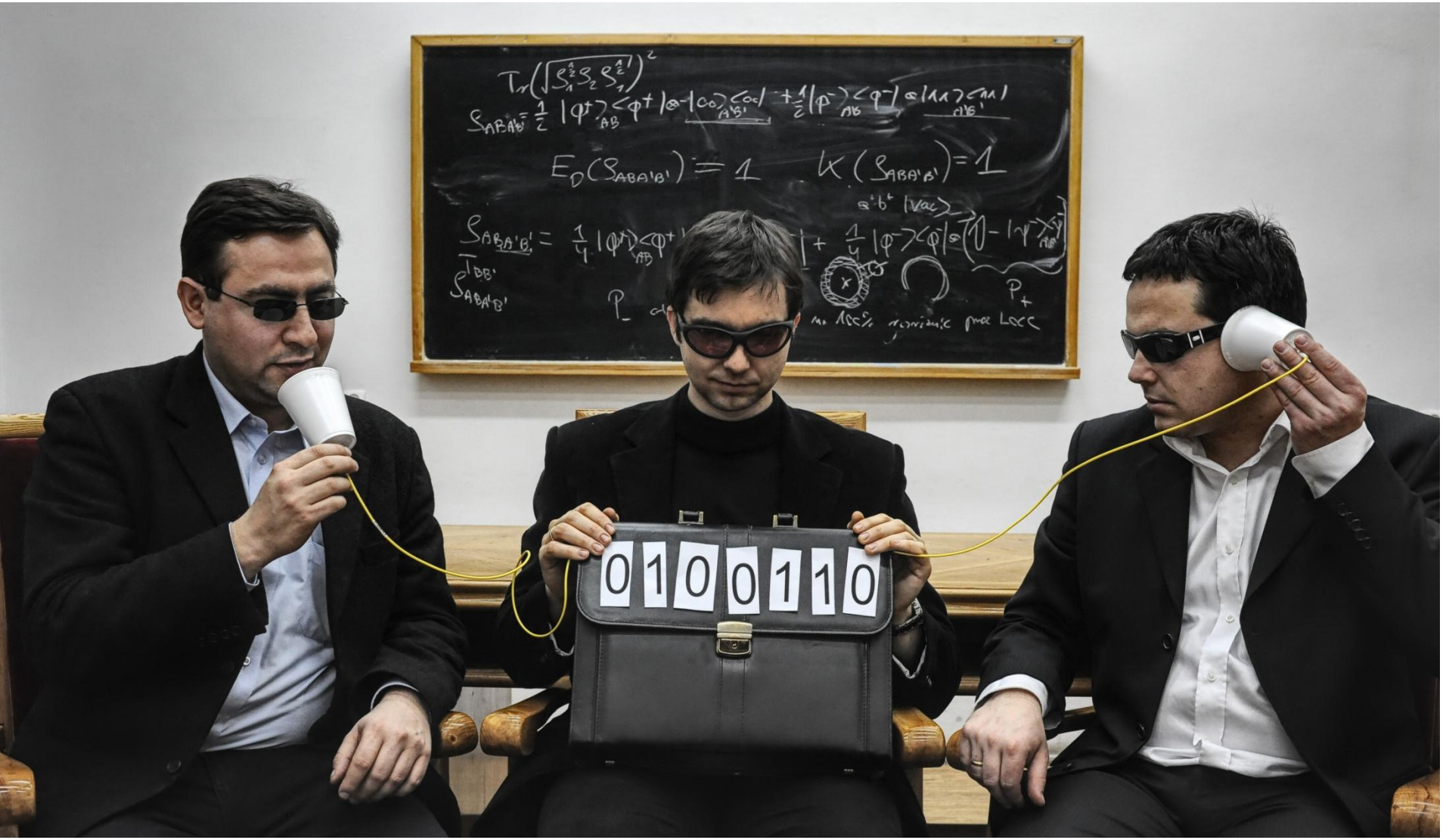
References & further reading



Bletchley Park

www.eclecticon.info

Questions



Prof. Paweł Horodecki (PG), Rafał Demkowicz-Dobrzański, PhD (FUW) and Michał Karpiński, PhD student (FUW). (Source: Grzegorz Krzyżewski, NLTK, University of Warsaw)