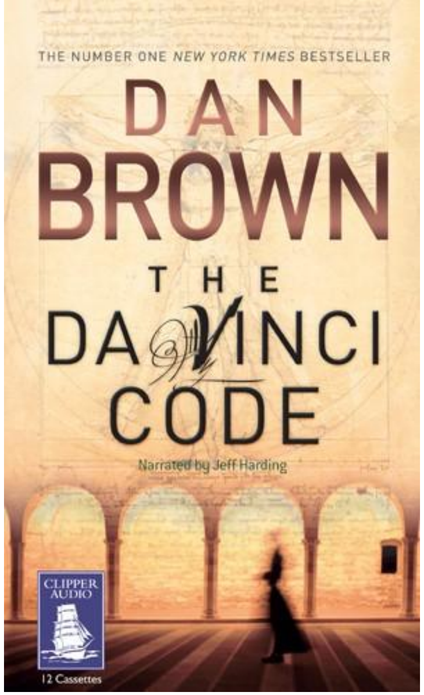
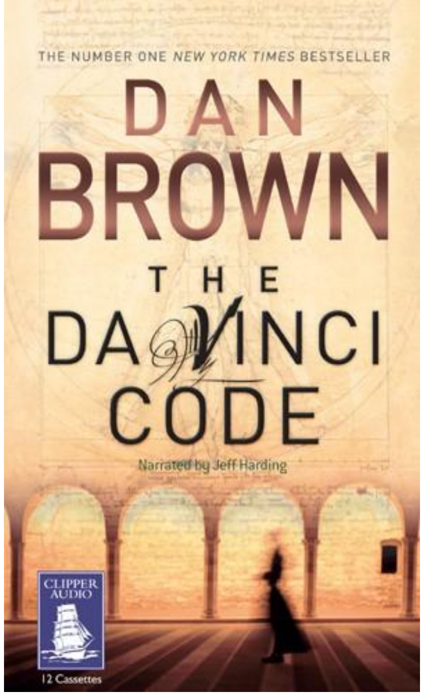
Cryptography and The Da Vinci Code



Prof. Keith Martin

Information Security Group
Royal Holloway
University of London

(OR… what Sophie Neveu did NOT seem to learn when she studied at Royal Holloway)



"**There's an easier way**," Sophie said, taking the pen from Teabing.

"**It works for all reflectional substitution ciphers, including the Atbash. A little trick I learned at the Royal Holloway**."

Sophie wrote the first half of the alphabet from left to right and then, beneath it, wrote the second half, right to left.

"**Cryptanalysts call it the fold-over. Half as complicated. Twice as clean**."

Teabing eyed her handiwork and chuckled.: "**Right you are. Glad to see those boys at the Holloway are doing their job**."

What is cryptography ?

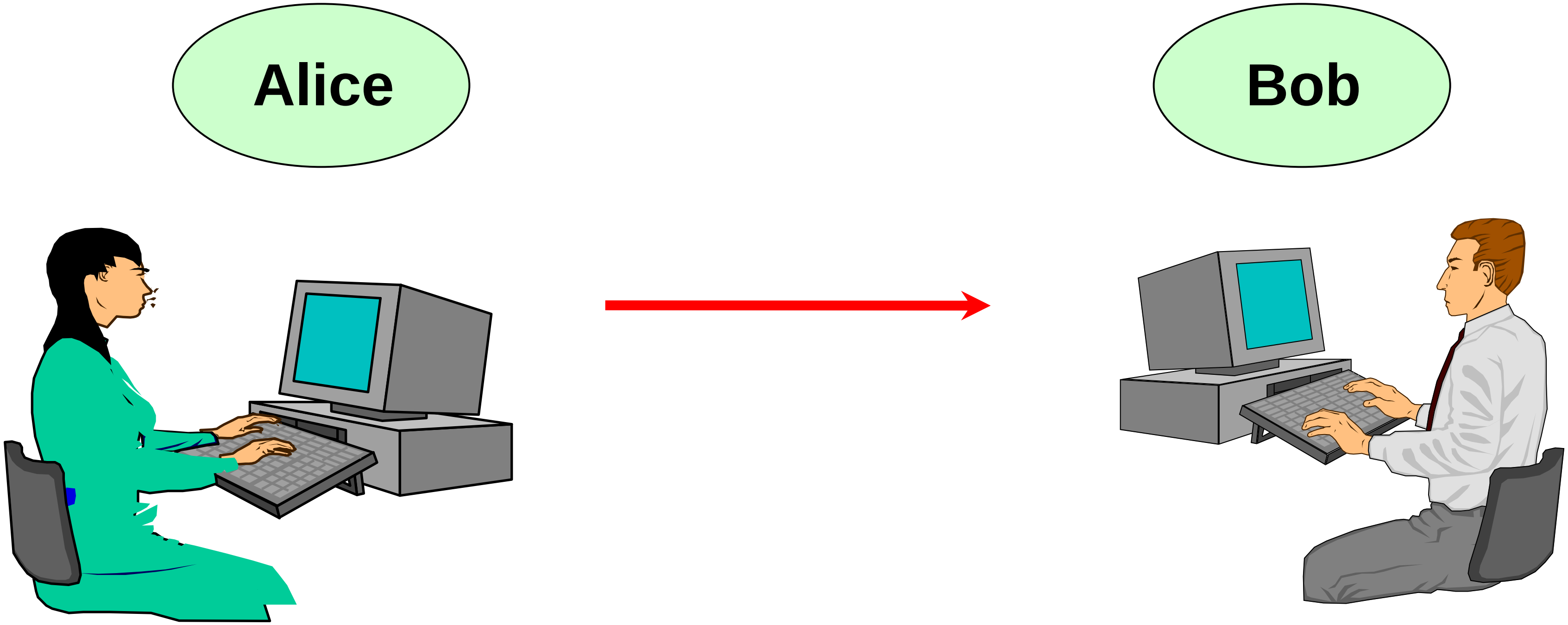
Have you used cryptography:

on a daily basis?

on a weekly basis?

occasionally?

A simple scenario



Alice

Bob

Risks to information

- Passive attacks
  - unauthorised access to information
- Active attacks
  - Unauthorised alteration
  - Unauthorised deletion
  - Unauthorised transmission
  - Falsification of origin of information
  - Unauthorised prevention of access to information

Cryptography: the toolkit

Cryptography provides a mathematical toolkit of techniques that can be called upon in order to implement the security services required for any application.

Cryptographic **primitives**

Identification schemes

Block ciphers

Digital signatures

Stream ciphers

Message authentication codes

Bit commitment

Hash functions

One-way functions

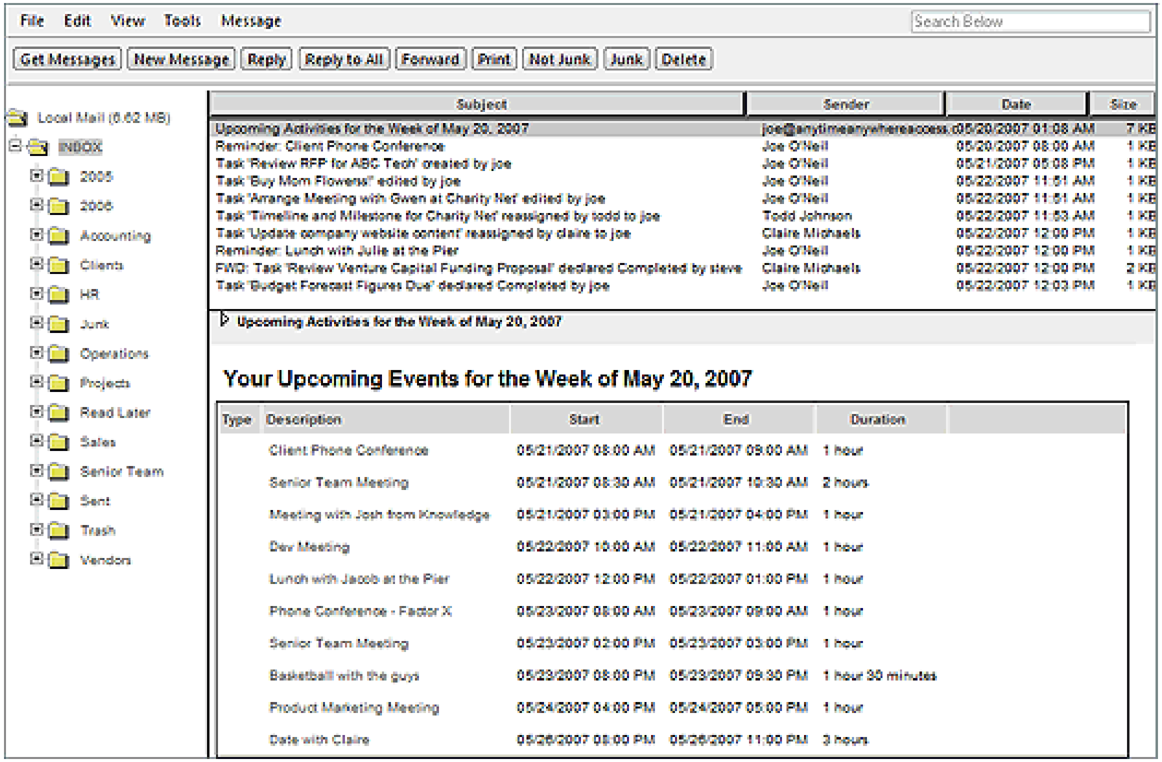
Secret sharing schemes

Zero-knowledge protocols

The need for confidentiality

Sending a letter to a friend

Sending an email to a friend



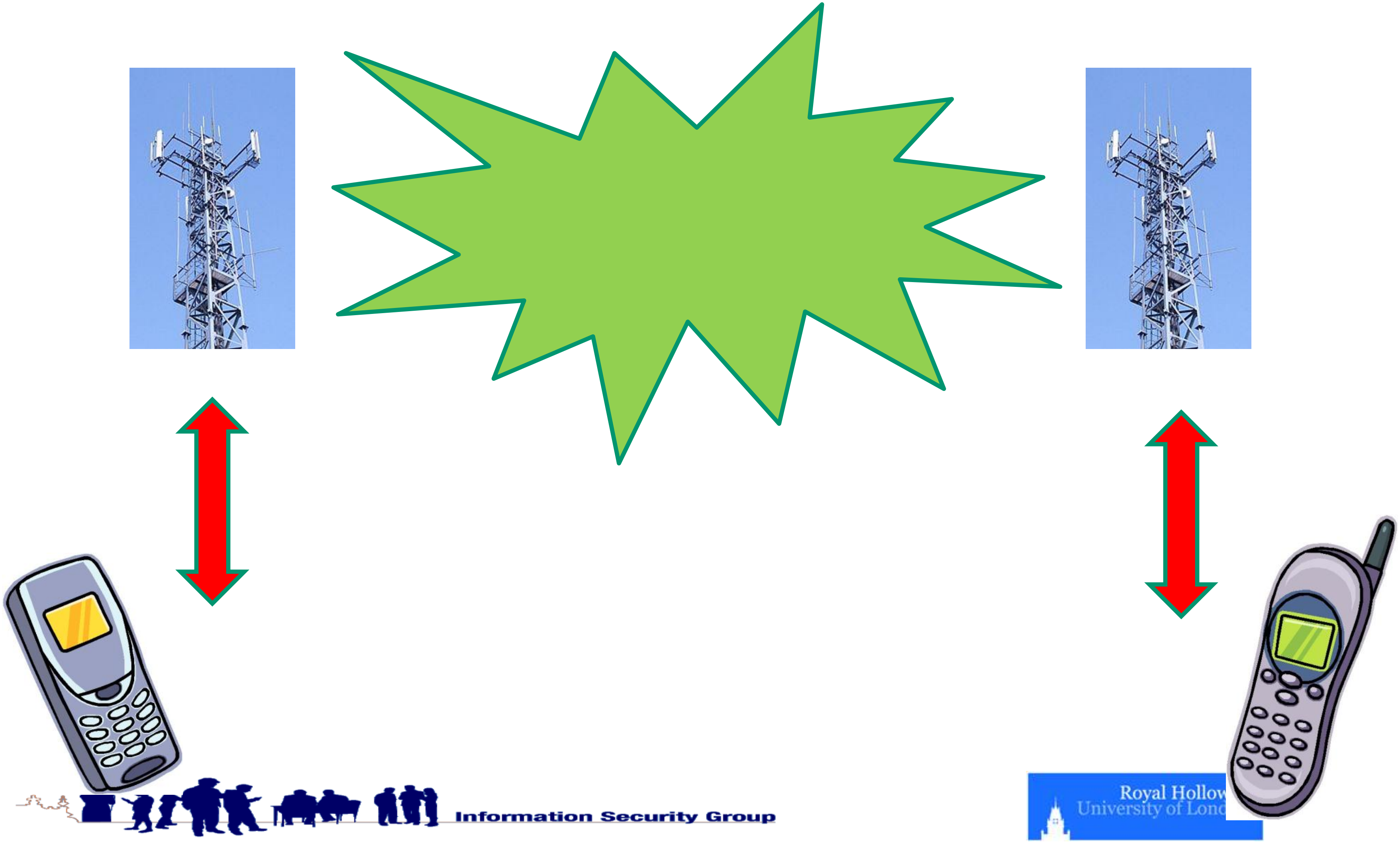
Subject	Sender	Date	Size
Upcoming Activities for the Week of May 20, 2007	joe@anytimeanywhereaccess.c	05/20/2007 01:08 AM	7 KB
Reminder: Client Phone Conference	Joe O'Neil	05/20/2007 08:00 AM	1 KB
Task 'Review RFP for ABC Tech' created by joe	Joe O'Neil	05/21/2007 05:08 PM	1 KB
Task 'Buy Mom Flowers!' edited by joe	Joe O'Neil	05/22/2007 11:51 AM	1 KB
Task 'Arrange Meeting with Gwen at Charity Net' edited by joe	Joe O'Neil	05/22/2007 11:51 AM	1 KB
Task 'Timeline and Milestone for Charity Net' reassigned by todd to joe	Todd Johnson	05/22/2007 11:53 AM	1 KB
Task 'Update company website content' reassigned by claire to joe	Claire Michaels	05/22/2007 12:00 PM	1 KB
Reminder: Lunch with Julie at the Pier	Joe O'Neil	05/22/2007 12:00 PM	1 KB
FWD: Task 'Review Venture Capital Funding Proposal' declared Completed by steve	Claire Michaels	05/22/2007 12:00 PM	2 KB
Task 'Budget Forecast Figures Due' declared Completed by joe	Joe O'Neil	05/22/2007 12:03 PM	1 KB

▷ **Upcoming Activities for the Week of May 20, 2007**

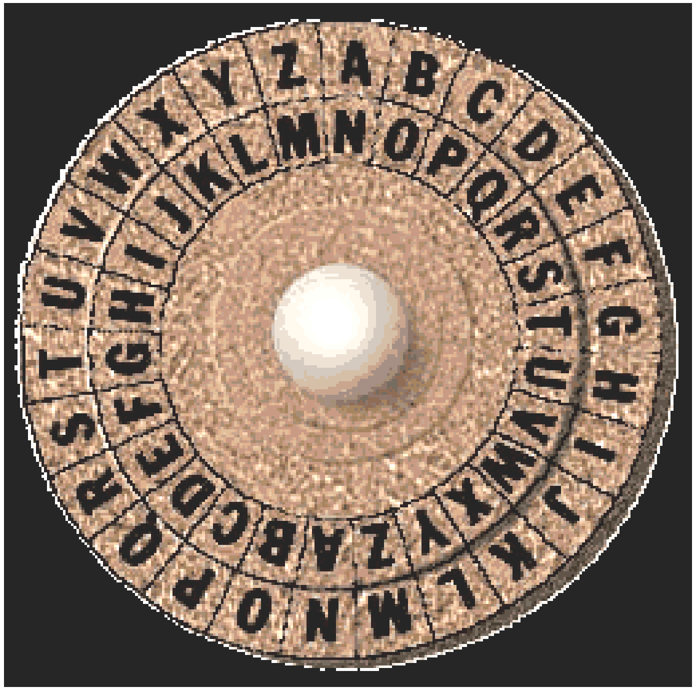
Your Upcoming Events for the Week of May 20, 2007

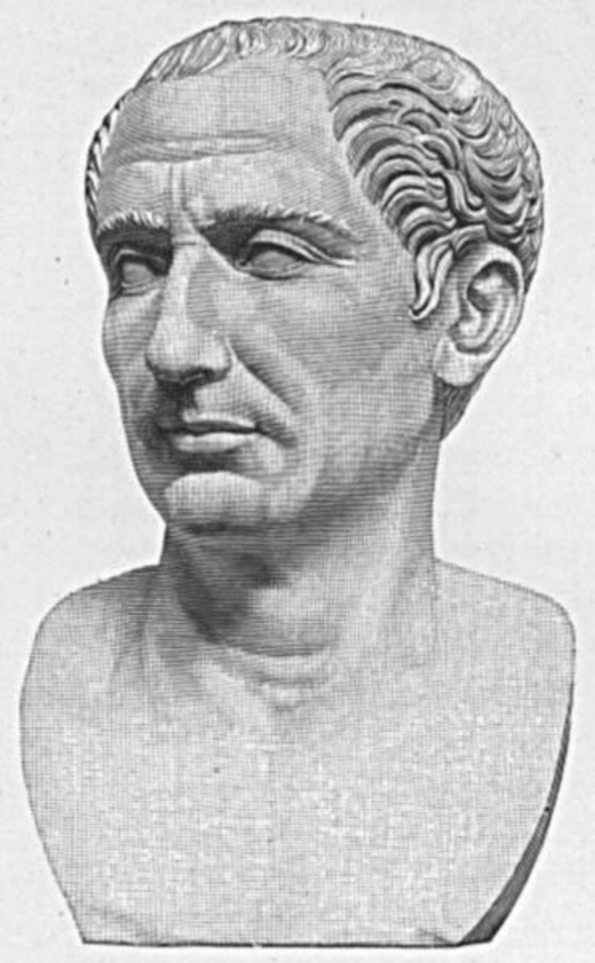
Type	Description	Start	End	Duration
	Client Phone Conference	05/21/2007 08:00 AM	05/21/2007 09:00 AM	1 hour
	Senior Team Meeting	05/21/2007 08:30 AM	05/21/2007 10:30 AM	2 hours
	Meeting with Josh from Knowledge	05/21/2007 03:00 PM	05/21/2007 04:00 PM	1 hour
	Dev Meeting	05/22/2007 10:00 AM	05/22/2007 11:00 AM	1 hour
	Lunch with Jacob at the Pier	05/22/2007 12:00 PM	05/22/2007 01:00 PM	1 hour
	Phone Conference - Factor X	05/23/2007 08:00 AM	05/23/2007 09:00 AM	1 hour
	Senior Team Meeting	05/23/2007 02:00 PM	05/23/2007 03:00 PM	1 hour
	Basketball with the guys	05/23/2007 08:00 PM	05/23/2007 09:30 PM	1 hour 30 minutes
	Product Marketing Meeting	05/24/2007 04:00 PM	05/24/2007 05:00 PM	1 hour
	Date with Claire	05/26/2007 08:00 PM	05/26/2007 11:00 PM	3 hours

Calling a friend on a mobile

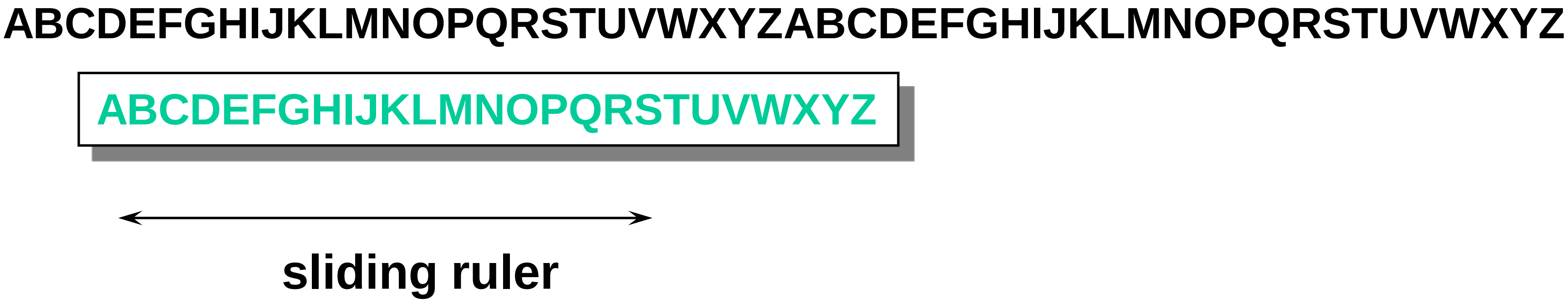


The Caesar Cipher


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
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



The Caesar Cipher



ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

sliding ruler

Caesar Cipher Example

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C													

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E

A	X	E

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C		

A	X	E

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C	E	

A	X	E

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C	E	G

A	X	E

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C	E	G

A	X	E
C		

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C	E	G

A	X	E
C	Z	

Caesar Cipher Example

Key shift C

A	B	C	D	E	F	G	H	I	J	…	X	Y	Z
C	D	E	F	G	H	I	J	K	L	…	Z	A	B

A	C	E
C	E	G

A	X	E
C	Z	G

Caesar Cipher Challenges

What creature hops about and explodes near a naked flame?

MX MW E KEWLSTTIV (key shift E)

Which creature says “baa” and fights at sea?

ZNOY OY G HGZZRKYNKKV (key shift G)

Which animal runs very fast and keeps you warm?

AL AK S OAFVUZWWLSZ (key shift S)

Simple Substitution Cipher

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

Keyspace of the Substitution Cipher

The key space of the Simple Substitution Cipher is approximately 4 x 10^{26}, that is:

400 000 000 000 000 000 000 000 000

Just how big is that?

There are an estimated 10 sextillion (that's 10^{22}) stars in our universe. That means that the Simple Substitution Cipher has about 40 000 **times** the number of keys than there are stars in our universe.

The key space of DES is somewhere between 10^{16} and 10^{17}. That's a much smaller number – it's only about 100 000 times the number of stars in our galaxy!

Substitution Cipher Examples

Decrypt the following ciphertexts

1 **B TO T OTA**

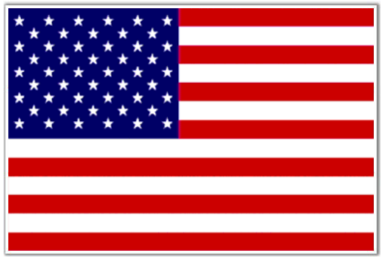
2 **XAV**

3 **VBDDQD**

4 **VBDDQD** **(given that the plaintext is the name of a country)**

5 **ABXAZ O OAZ TCYE TE F CEOE UCZXT**

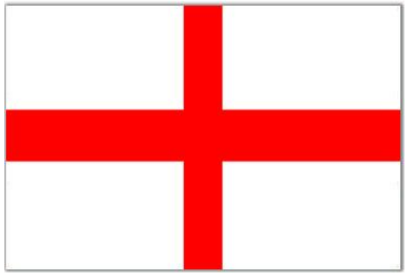
World Cup 2010 Special Examples



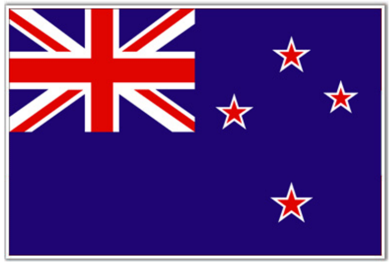
TBZ

GYZICEBCG

HPSNRPV

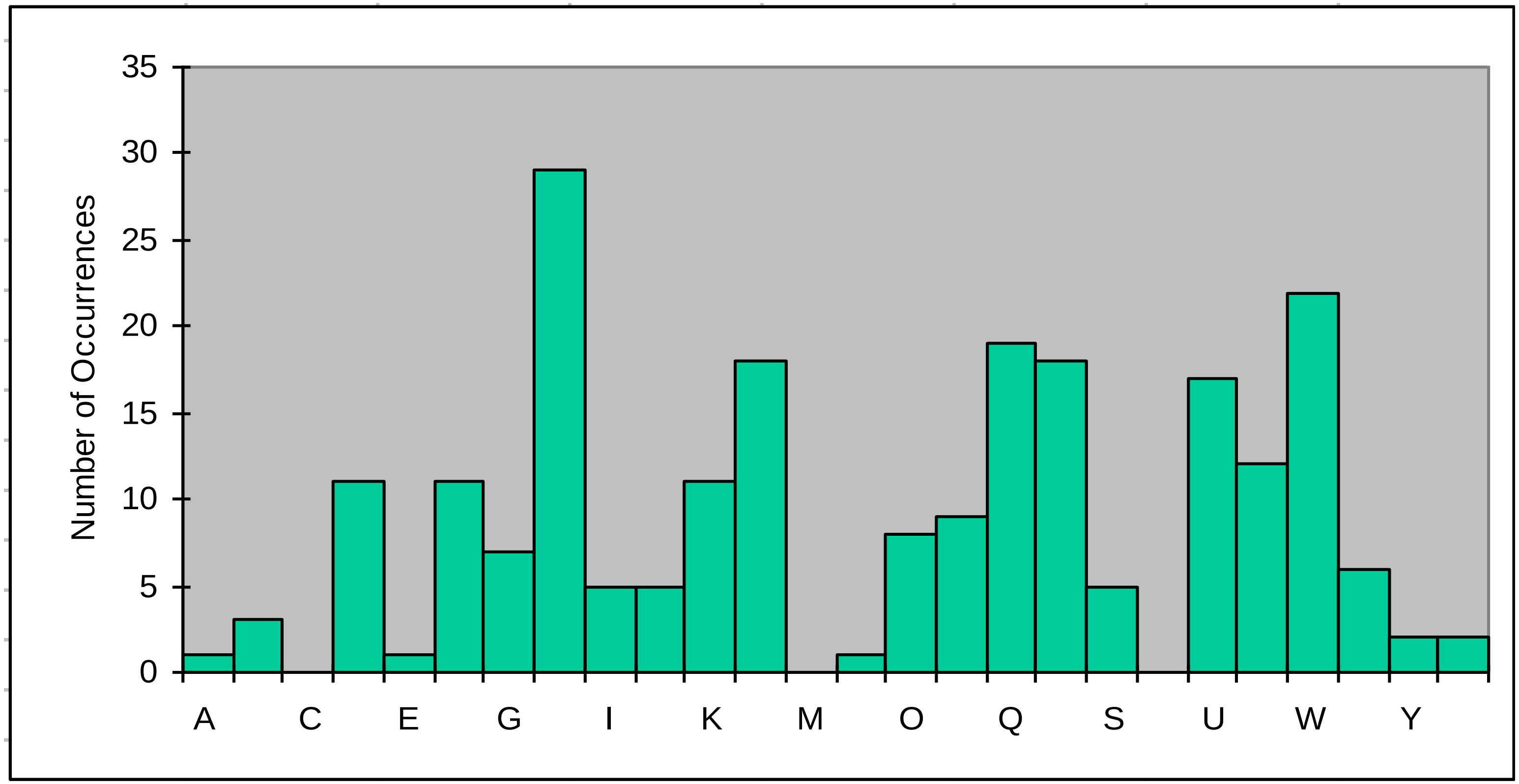


OQC UQFKFOX



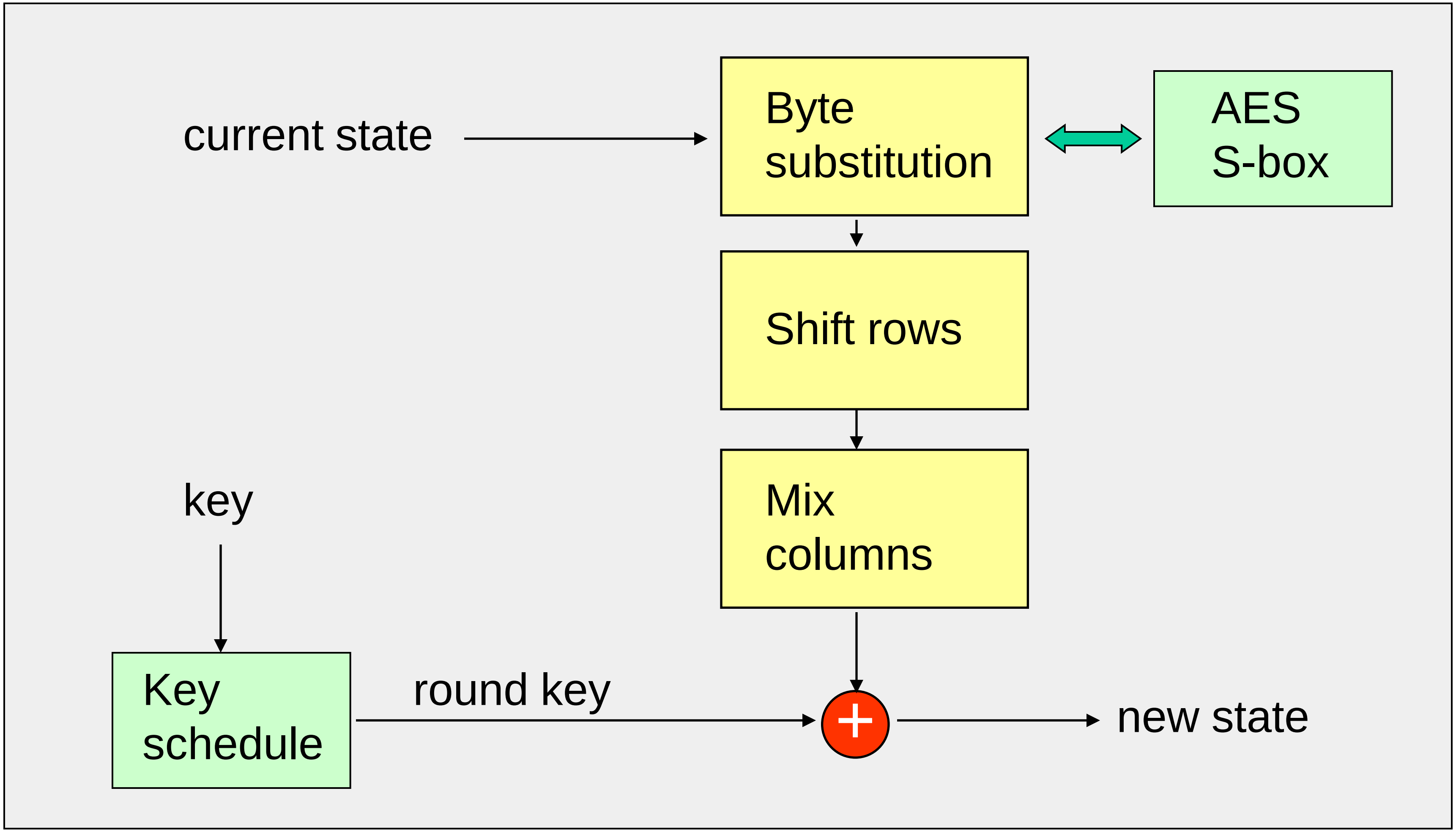
YEVENLEM

Substitution Cipher Histogram

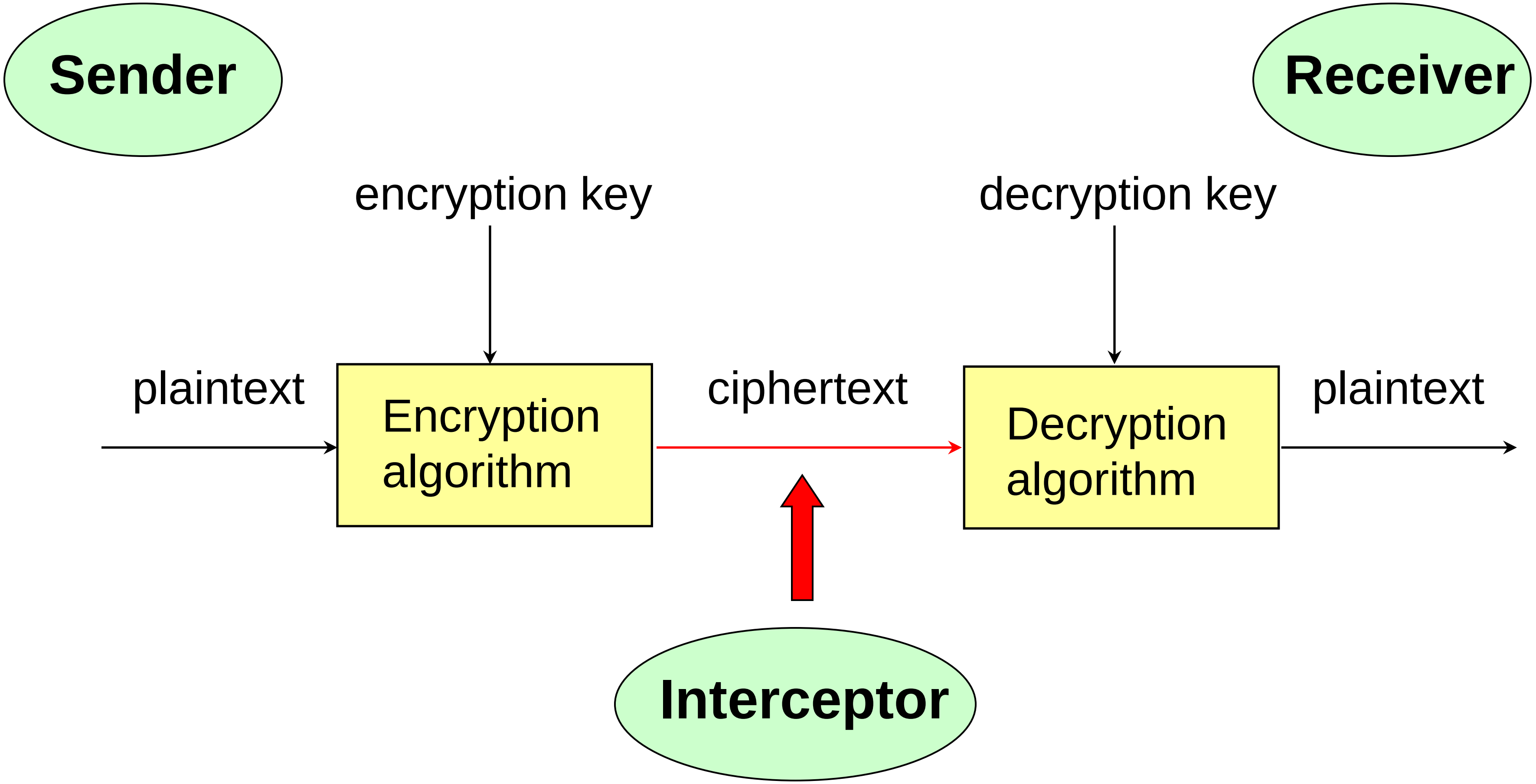


A histogram showing the relative frequencies of the letters in a cryptogram that was obtained by using a simple substitution cipher.

Advanced Encryption Standard



A cryptosystem



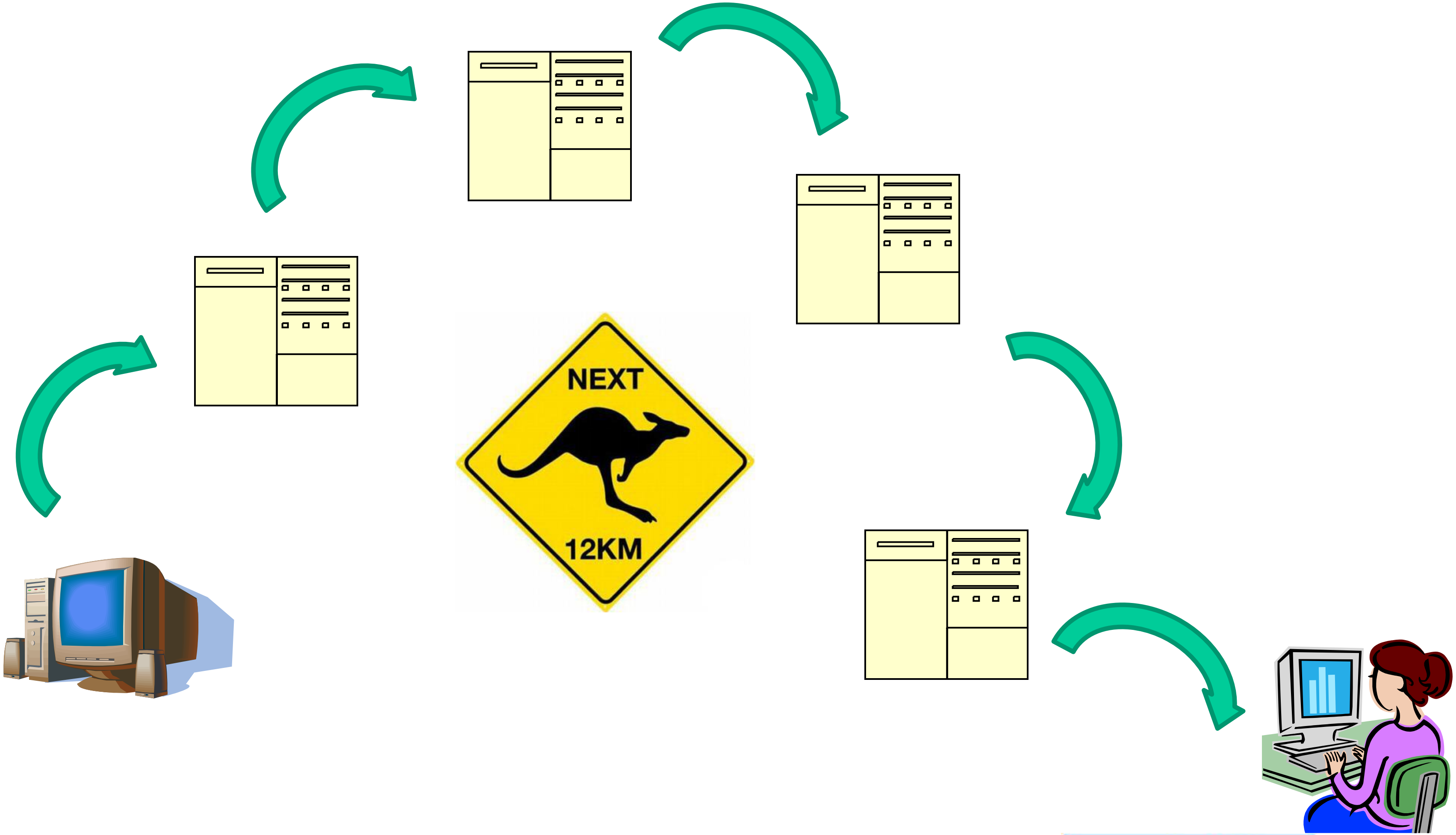
The need for data integrity

Two things that can go wrong...

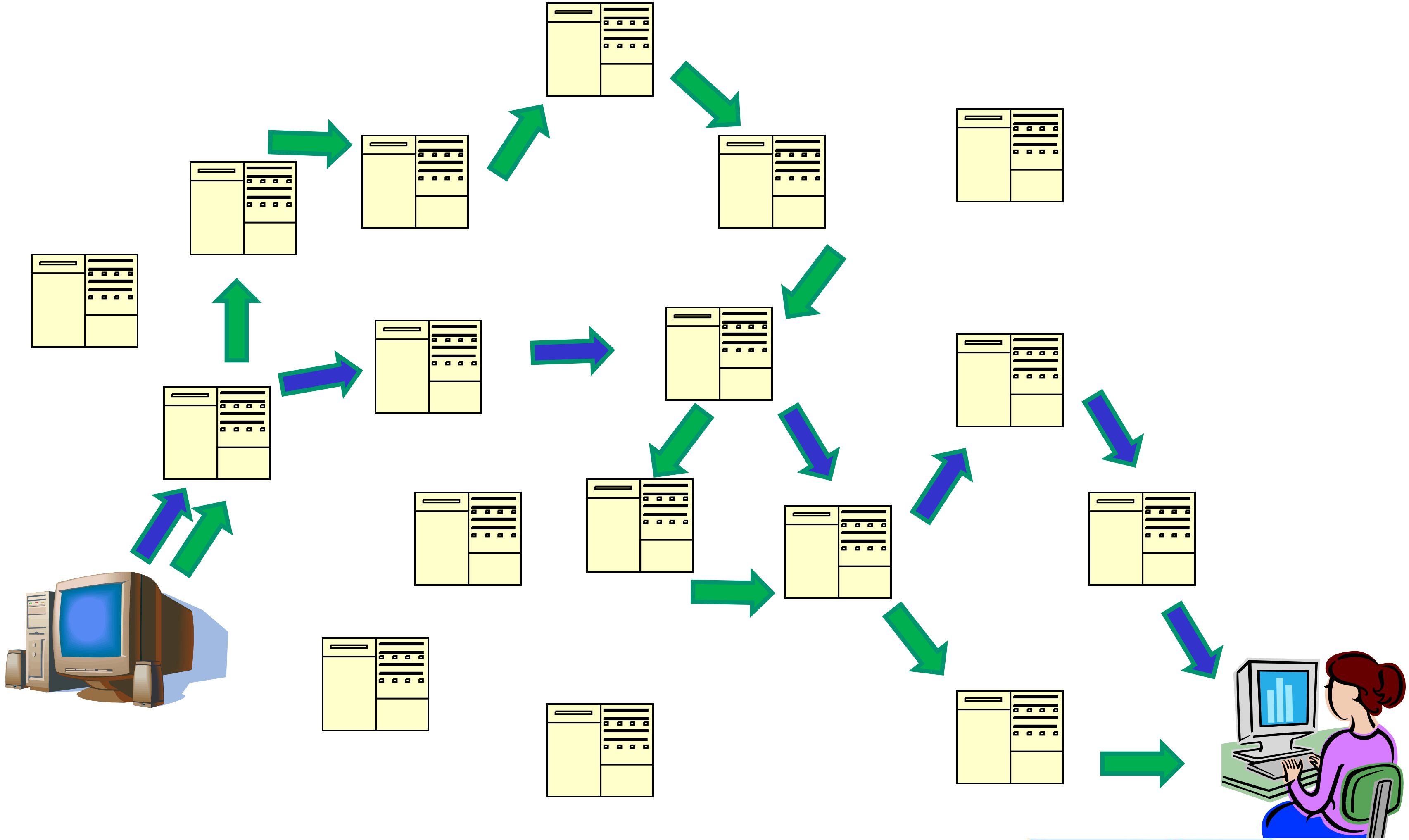
Accidental errors

Deliberate errors

How the Internet works (part 1)



How the Internet works (part 2)



International Morse Code

- 1 dash = 3 dots.
- The space between parts of the same letter = 1 dot.
- The space between letters = 3 dots.
- The space between words = 7 dots.

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	▬ ▬ ● ●
.	● ▬ ● ▬ ● ▬
,	▬ ▬ ● ● ▬ ▬
?	● ● ▬ ▬ ● ●
/	▬ ● ● ▬ ●
@	● ▬ ▬ ● ▬ ●
1	● ▬ ▬ ▬ ▬
2	● ● ▬ ▬ ▬
3	● ● ● ▬ ▬
4	● ● ● ● ▬
5	● ● ● ● ●
6	▬ ● ● ● ●
7	▬ ▬ ● ● ●
8	▬ ▬ ▬ ● ●
9	▬ ▬ ▬ ▬ ●
0	▬ ▬ ▬ ▬ ▬

Morse Code Example

0010	01	1000	00	111

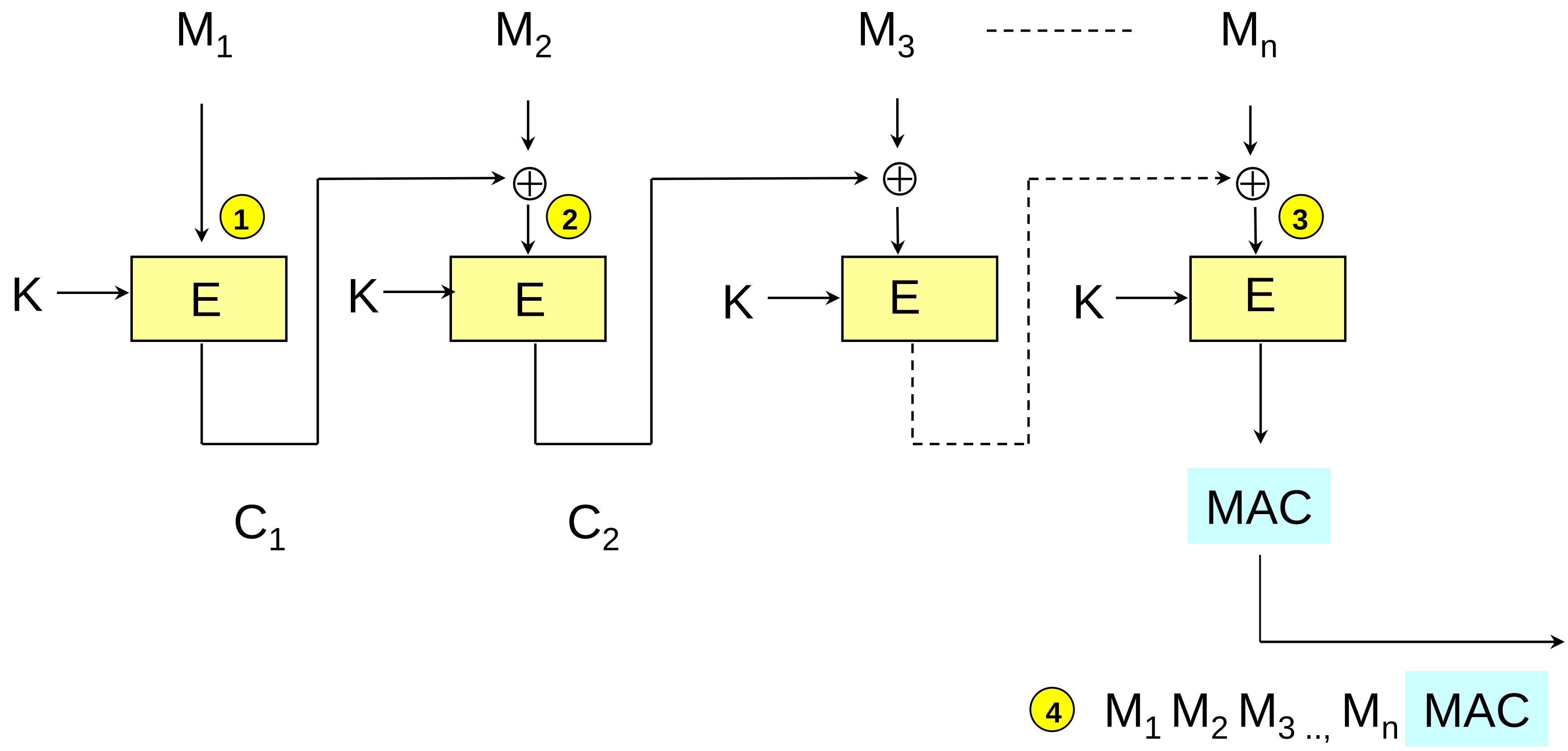
The ISBN number

$$x_{10} \equiv 11 - (10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9) \bmod 11$$

Deliberate errors

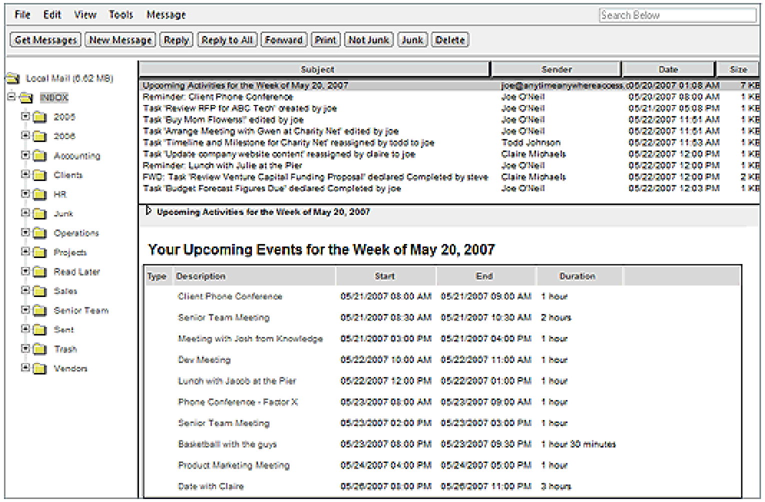
CBC-MAC

(Padded) message divided into blocks



The need for authentication

A problem with email



Subject	Sender	Date	Size
Upcoming Activities for the Week of May 20, 2007	joe@anytimeanywhereaccess.c	05/20/2007 01:08 AM	7 KB
Reminder: Client Phone Conference	Joe O'Neil	05/20/2007 08:00 AM	1 KB
Task 'Review RFP for ABC Tech' created by joe	Joe O'Neil	05/21/2007 05:08 PM	1 KB
Task 'Buy Mom Flowers!' edited by joe	Joe O'Neil	05/22/2007 11:51 AM	1 KB
Task 'Arrange Meeting with Gwen at Charity Net' edited by joe	Joe O'Neil	05/22/2007 11:51 AM	1 KB
Task 'Timeline and Milestone for Charity Net' reassigned by todd to joe	Todd Johnson	05/22/2007 11:53 AM	1 KB
Task 'Update company website content' reassigned by claire to joe	Claire Michaels	05/22/2007 12:00 PM	1 KB
Reminder: Lunch with Julie at the Pier	Joe O'Neil	05/22/2007 12:00 PM	1 KB
FWD: Task 'Review Venture Capital Funding Proposal' declared Completed by steve	Claire Michaels	05/22/2007 12:00 PM	2 KB
Task 'Budget Forecast Figures Due' declared Completed by joe	Joe O'Neil	05/22/2007 12:03 PM	1 KB

Upcoming Activities for the Week of May 20, 2007

Your Upcoming Events for the Week of May 20, 2007

Type	Description	Start	End	Duration
	Client Phone Conference	05/21/2007 08:00 AM	05/21/2007 09:00 AM	1 hour
	Senior Team Meeting	05/21/2007 08:30 AM	05/21/2007 10:30 AM	2 hours
	Meeting with Josh from Knowledge	05/21/2007 03:00 PM	05/21/2007 04:00 PM	1 hour
	Dev Meeting	05/22/2007 10:00 AM	05/22/2007 11:00 AM	1 hour
	Lunch with Jacob at the Pier	05/22/2007 12:00 PM	05/22/2007 01:00 PM	1 hour
	Phone Conference - Factor X	05/23/2007 08:00 AM	05/23/2007 09:00 AM	1 hour
	Senior Team Meeting	05/23/2007 02:00 PM	05/23/2007 03:00 PM	1 hour
	Basketball with the guys	05/23/2007 08:00 PM	05/23/2007 09:30 PM	1 hour 30 minutes
	Product Marketing Meeting	05/24/2007 04:00 PM	05/24/2007 05:00 PM	1 hour
	Date with Claire	05/26/2007 08:00 PM	05/26/2007 11:00 PM	3 hours

Can you be sure that an email from a friend is really from your friend?

A need for authentication!

Types of entity authentication

The most common methods use (a combination of):

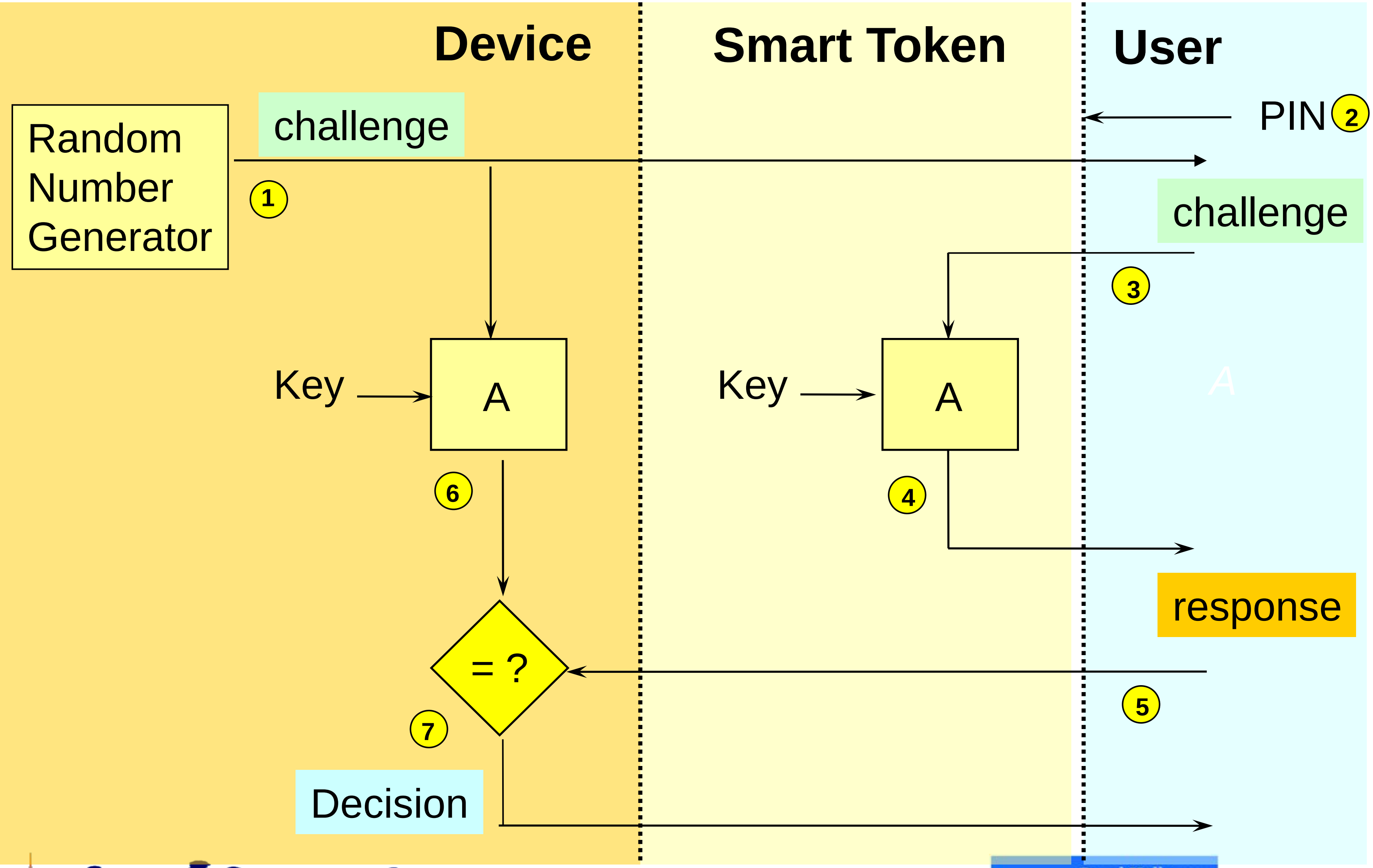
- **something that you have**
- **something that you are**
- **something that you know**

Passwords

Choose a password....

PASSWORD1
ABCDEFG
WILLIAMKATE
STATION778
MARSBAR
CV8G9Pa2**

One-time password mechanisms



Real world applications need

Confidentiality

Data Integrity

Authentication

...to varying degrees

So…
what did
Sophie Neveu learn
at Royal Holloway ?

Atbash Cipher

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

"**There's an easier way**," Sophie said, taking the pen from Teabing.

"**It works for all reflectional substitution ciphers, including the Atbash. A little trick I learned at the Royal Holloway**."

Sophie wrote the first half of the alphabet from left to right and then, beneath it, wrote the second half, right to left.

"**Cryptanalysts call it the fold-over. Half as complicated. Twice as clean**."

Teabing eyed her handiwork and chuckled.: "**Right you are. Glad to see those boys at the Holloway are doing their job**."

Highly recommended

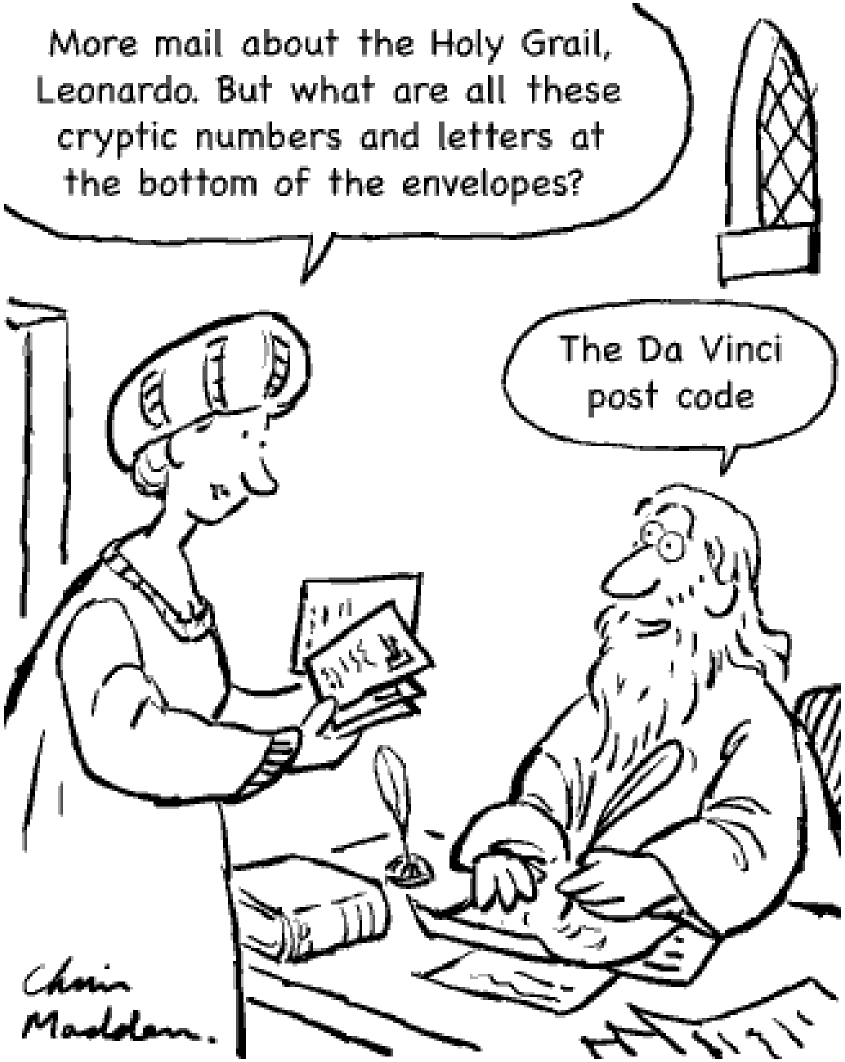
CrypTool 1.4.10

http://www.cryptool.org/

Some bed-time reading

- F. Piper and S. Murphy, **Cryptography: A Very Short Introduction**, Oxford University Press (2002).
- H.X. Mel and D. Baker, **Cryptography Decrypted**, Addison-Wesley (2001).
- D.R. Stinson, **Cryptography: Theory and Practice**, 3rd Edition, Chapman & Hall/CRC Press (2006).
- S. Levy, **Crypto**, Penguin Books (2000).
- S. Singh, **The Code Book**, Fourth Estate (1999).
- N. Ferguson and B. Schneier **Practical Cryptography**, Wiley (2003).

Thank You


More mail about the Holy Grail, Leonardo. But what are all these cryptic numbers and letters at the bottom of the envelopes?
The Da Vinci post code
Chris Madden.