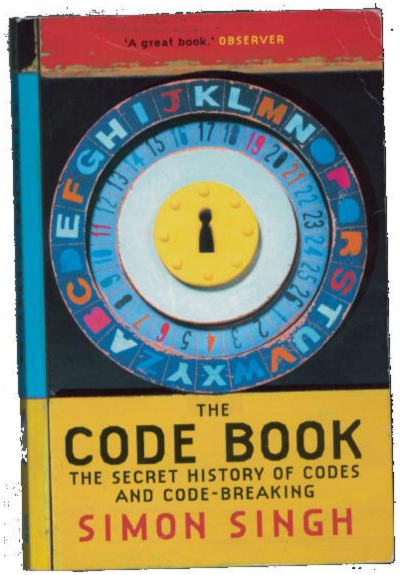
The University Of Sheffield.



# COM1008: Web and Internet Technology

## Lecture 19. Information Security Part 3

**Dr. Steve Maddock**
s.maddock@sheffield.ac.uk

(with thanks to Dr Mike Stannett
who shared his lecture slides)

# 1. Introduction

- *Last two lectures*: Information; security; risk – vulnerabilities, threats, attacks; Three classical goals of information security: Confidentiality, Integrity, Availability; legal frameworks; computer and network security: some practicalities
- *Today*: cryptography

- *Example*: What does the following encrypted message say?

```
ALPCS'Z RZ YSLH EZ ZPKSE O UMRSH SMRSH
VR L WWNLE YWNLE WWRI EZBPKSE,
TVV L YWNLE WWNLE'D PBX L DZPKSE ZPKSE
CU E WTUOX YTUOX WTYL XZYWNLE.
```

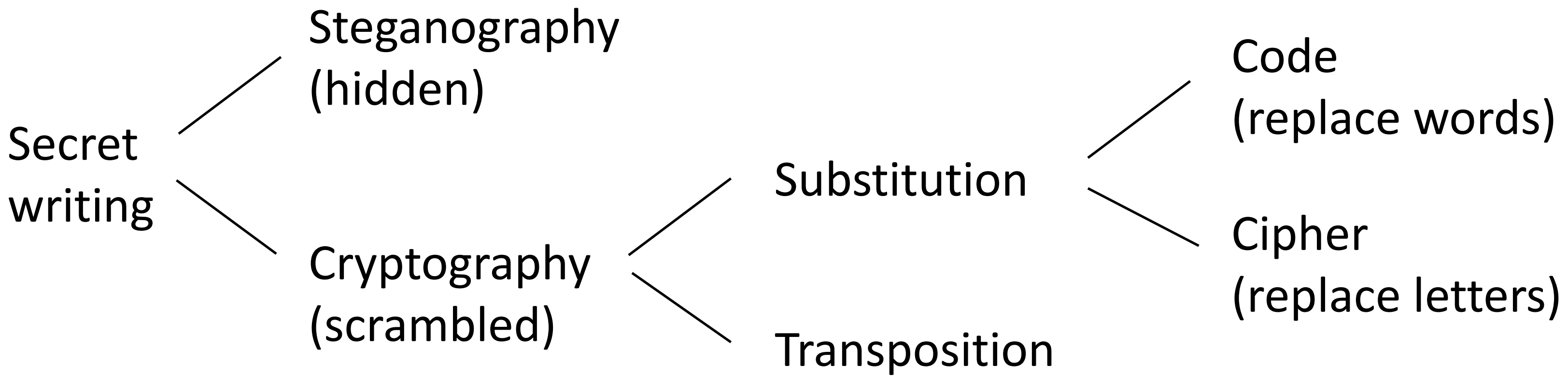
## 2. Relevance

- Who sent that email?
- Who downloaded that torrent?
- Who vandalised that Wikipedia entry?
- Is the virus checker I just downloaded safe to install?
- Is it safe to pay for this book online using my credit card?
- Is this iPlayer programme being watched in the UK?
- How do I prove I submitted my online tax return?
- How do I prove it wasn't me that uploaded the file?
- Is this the same customer we saw yesterday?
- Can I show him the account details he's asked for?
- How do I know this person has access rights to this folder?
- Is this guy allowed to erase my database?

# 3. Secret writing

Steganography in use in 5th century BC, Greeks against Persians

STEGANOGRAPHY: hide existence of message



Secret writing

Steganography (hidden)

Cryptography (scrambled)

Substitution

Transposition

Code (replace words)

Cipher (replace letters)

Abū Yūsuf Yaʻqūb ibn Isḥāq al-Kindī (801-873 CE) wrote the earliest known book on cryptanalysis

CRYPTOGRAPHY: hide meaning of message, not existence, using a process called encryption

Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000, p.30

## 3.1 Terminology

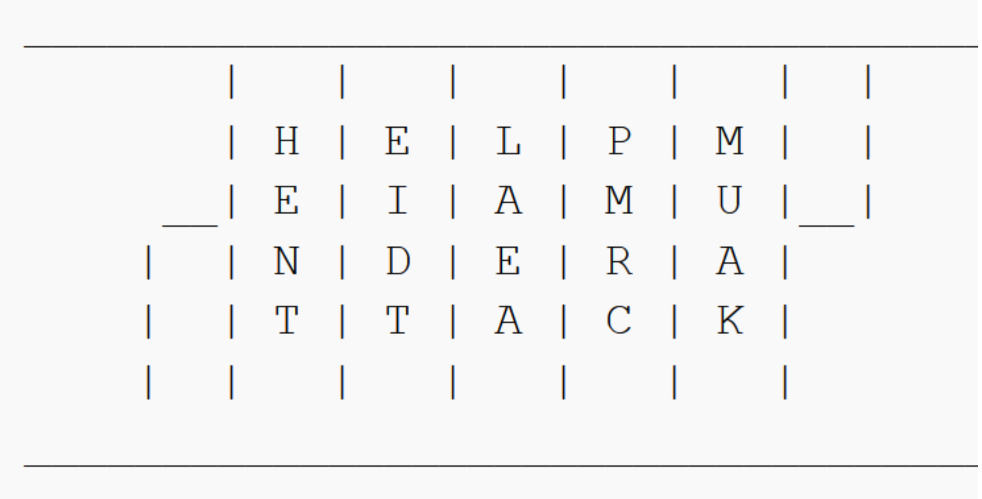
- ENCRYPTION: Converting an intelligible message (plaintext) into something that can't be directly interpreted correctly (ciphertext)
- DECRYPTION: Converting the ciphertext back into the plaintext
- CRYPTOSYSTEM: The underlying algorithms used to encrypt and decrypt messages
- KEY: Information required by the cryptosystem at run-time, in addition to the plaintext or ciphertext

# 4. Transposition

- Rail fence transposition
- Example
  - Plaintext: `attack at dawn`
  - Ciphertext: `ATCADWTAKTAN`

```
A   T   C   A   D   W
  T   A   K   T   A   N
```

- Scytale, use by Spartans in 5th century BC



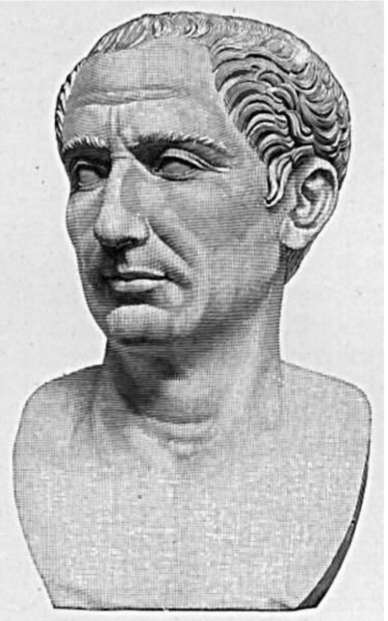
```
____________________________________________________
          |      |      |      |      |      |    |
          |  H   |  E   |  L   |  P   |  M   |    |
      ____|  E   |  I   |  A   |  M   |  U   |____|
     |    |  N   |  D   |  E   |  R   |  A   |
     |    |  T   |  T   |  A   |  C   |  K   |
     |    |      |      |      |      |      |
____________________________________________________
```

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

"Skytale". Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Skytale.png#/media/File:Skytale.png

# 5. Substitution

- Caesar cipher
- Vigenère cipher



"Gaius Julius Caesar (100-44 BC)" by H. F. Helmolt (ed.): History of the World. New York, 1902 (University of Texas Library Portrait Gallery). Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:Gaius_Julius_Caesar_(100-44_BC).JPG#/media/File:Gaius_Julius_Caesar_(100-44_BC).JPG

"Vigenere" by Thomas de Leu - Woodcut Photograph. No date found.. Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:Vigenere.jpg#/media/File:Vigenere.jpg

## 5.1 Caesar cipher (shift cipher)

- Replace each letter with the letter a fixed number of characters further on in the alphabet
  - Plaintext : `once upon a time`
  - Ciphertext : `RQFH XSRQ D WLPH`
- The key is the number of places in the alphabet that we need to move sideways
  - Given A = 0, B =1, … Z=25, then
  - $E_n(x) = (x+n) \bmod 26$
  - $D_n(x) = (x-n) \bmod 26$
- We always substitute the same ciphertext character for the same plaintext character
- This makes the system crackable using frequency analysis

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

## 5.2 Frequency analysis

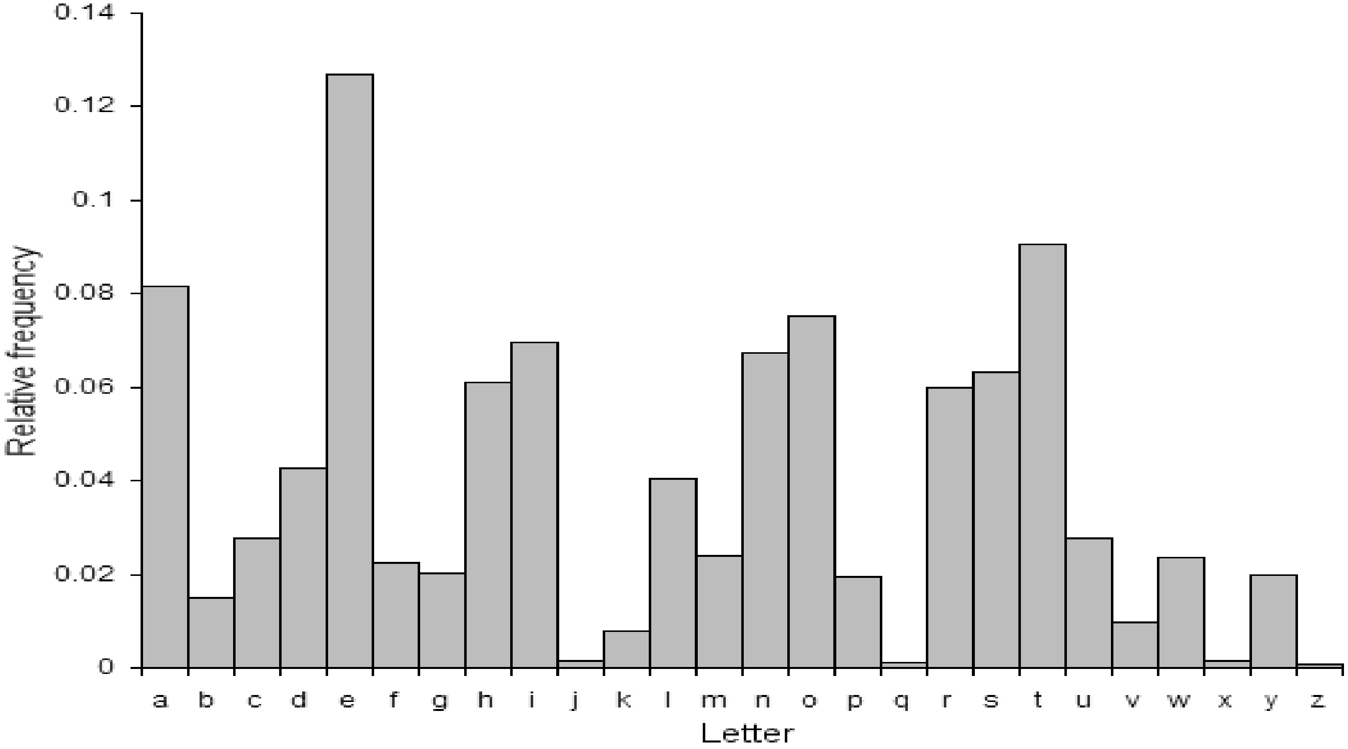
- Plain  : `when does the plane leave?`
- Cipher: `ZKHQ GRHV WKH SODQH OHDYH?`

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **P** | 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 |
| | 2 | - | - | 1 | 6 | - | - | 2 | - | - | - | 2 | - | 2 | 1 | 1 | - | - | 1 | 1 | - | 1 | 1 | - | - | - |
| **C** | - | - | - | 2 | - | - | 1 | 6 | - | - | 2 | - | - | - | 2 | - | 2 | 1 | 1 | - | - | 1 | 1 | - | 1 | 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 |

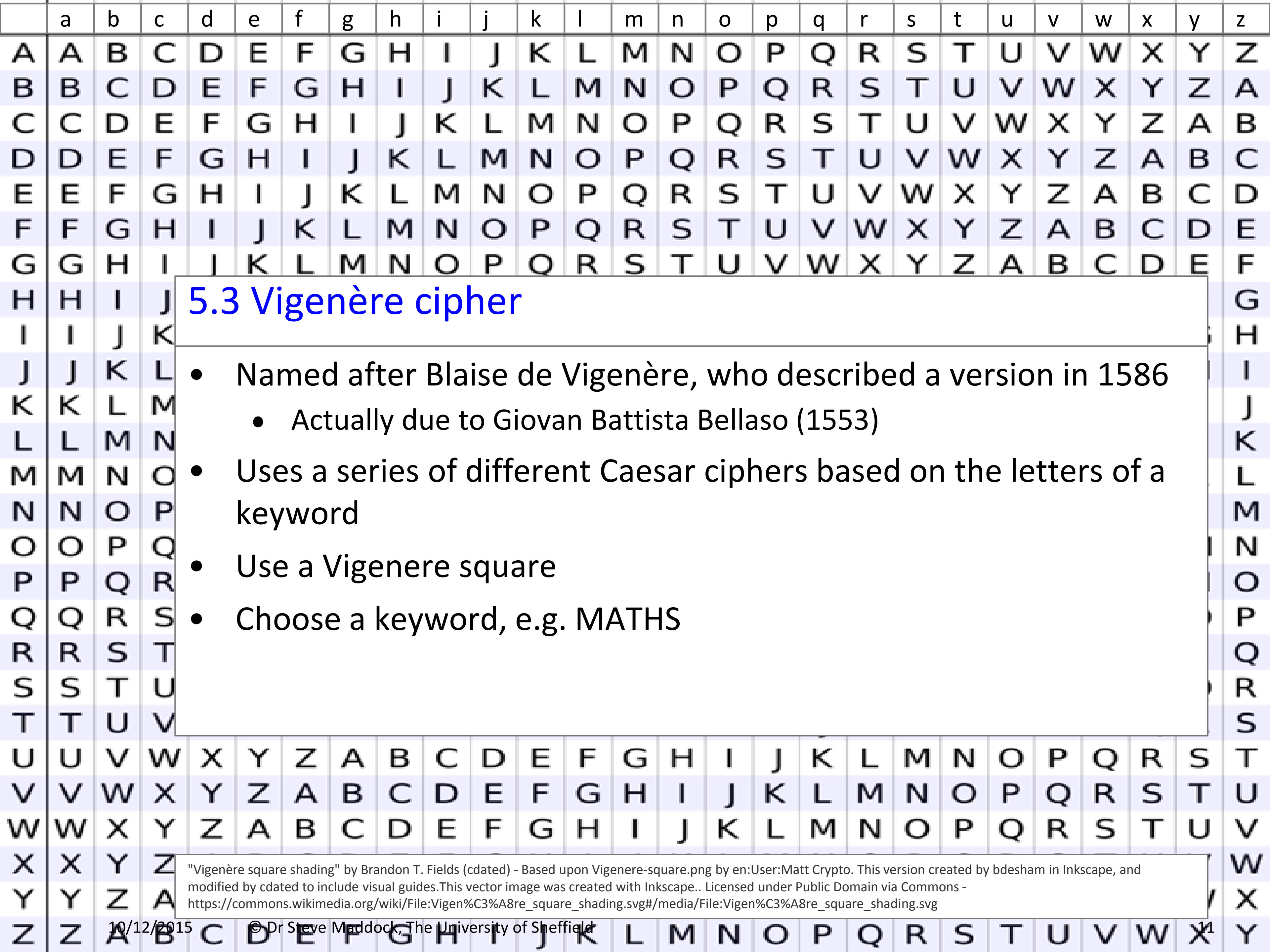
- How often does each letter occur in the plaintext and ciphertext?
- The pattern of frequencies is the same in both rows, except that those for the ciphertext have been displaced 3 characters to the right.
- So the key is 3

# 5.2 Frequency analysis (more generally)

- How often does each letter occur in standard English? The distribution is different for different languages.



https://en.wikipedia.org/wiki/Frequency_analysis. "English letter frequency (alphabetic)" by Nandhp - Own work; en:Letter frequency.. Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:English_letter_frequency_(alphabetic).svg#/media/File:English_letter_frequency_(alphabetic).svg



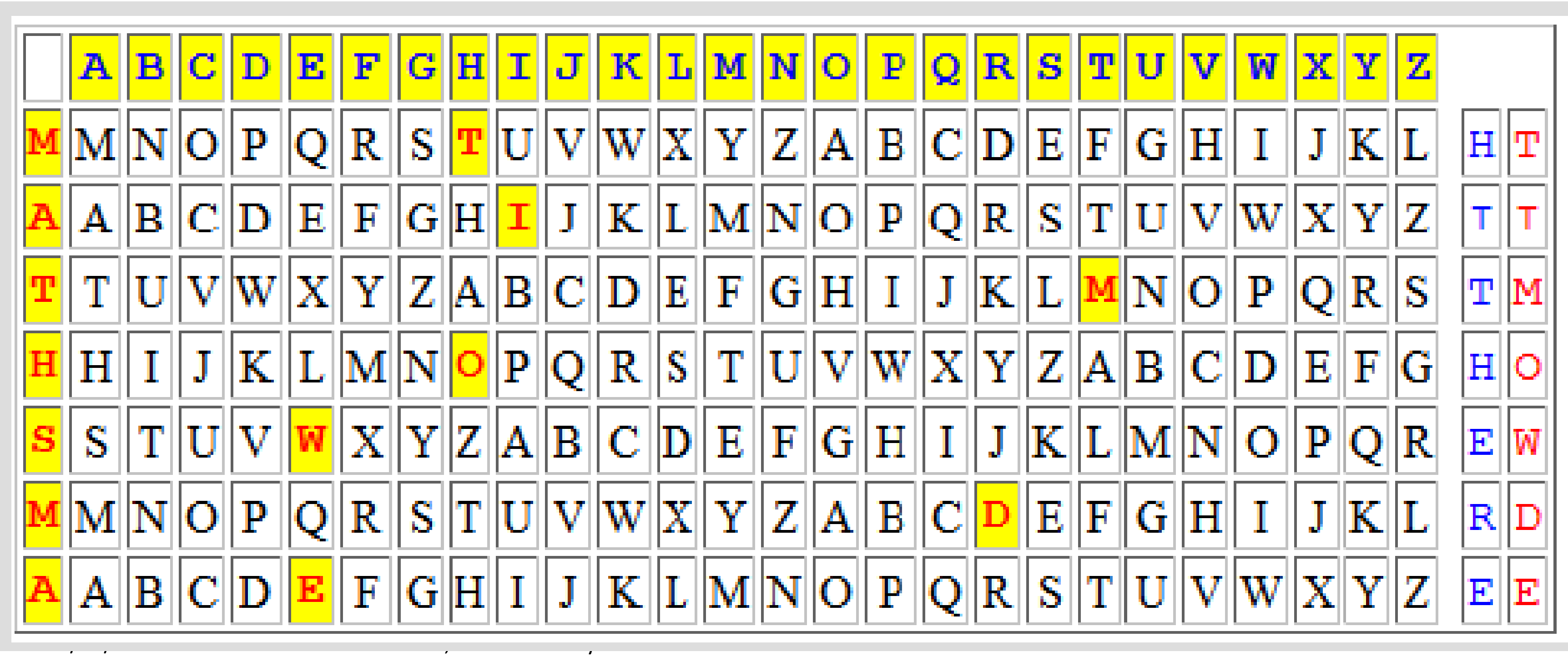
## 5.3 Vigenère cipher

- Named after Blaise de Vigenère, who described a version in 1586
  - Actually due to Giovan Battista Bellaso (1553)
- Uses a series of different Caesar ciphers based on the letters of a keyword
- Use a Vigenere square
- Choose a keyword, e.g. MATHS

"Vigenère square shading" by Brandon T. Fields (cdated) - Based upon Vigenere-square.png by en:User:Matt Crypto. This version created by bdesham in Inkscape, and modified by cdated to include visual guides.This vector image was created with Inkscape.. Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:Vigen%C3%A8re_square_shading.svg#/media/File:Vigen%C3%A8re_square_shading.svg

## 5.3 Vigenère cipher. Example: Hi there

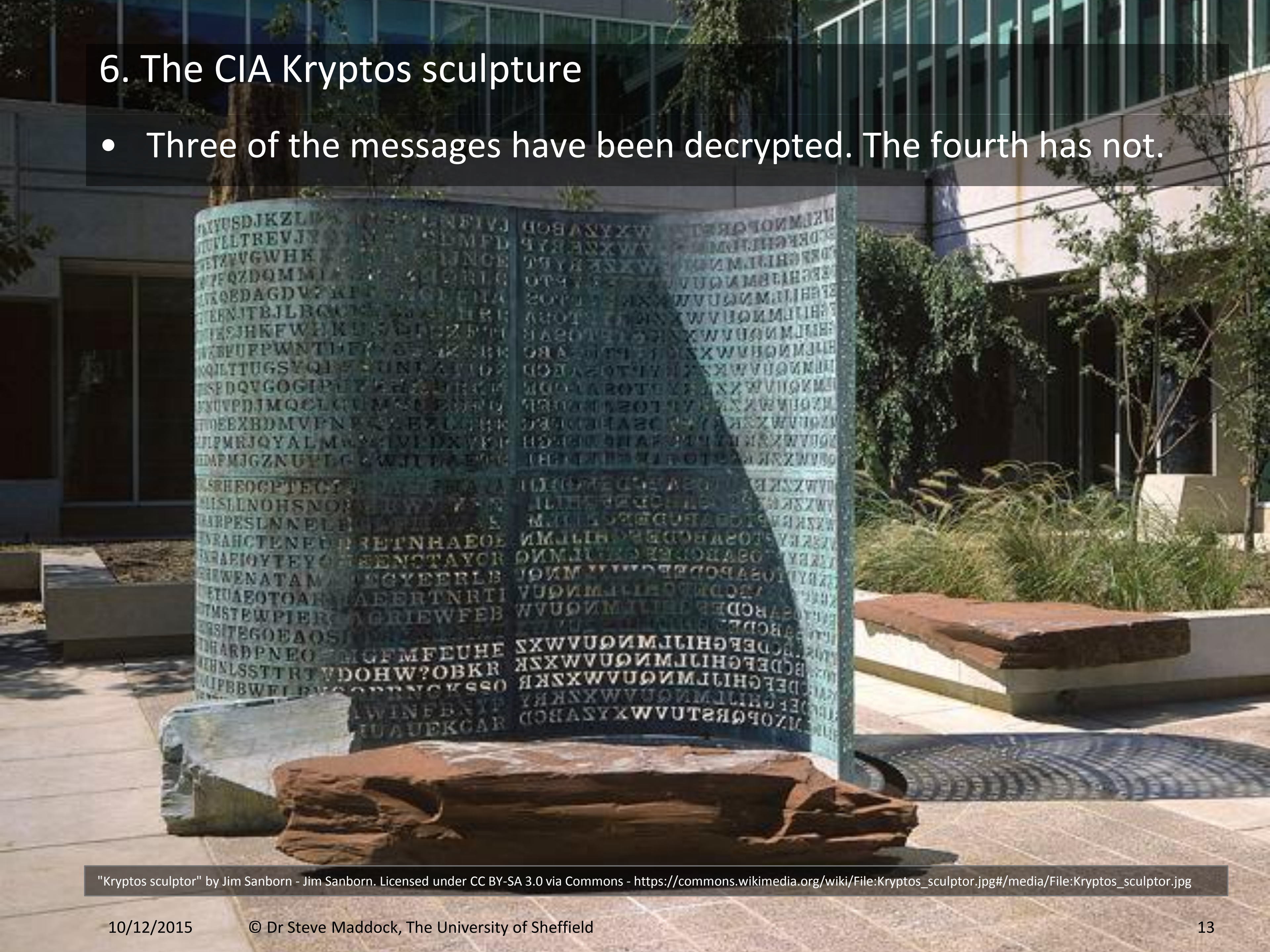
- Keyword: MATHSMA
- Plain : hithere
- Cipher : TTMOWDE
- The first e becomes W, but the second becomes E. This stops the system being cracked by simple frequency analysis.



| | 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 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | H | T |
| 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 | T | T |
| 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 | T | M |
| 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 | H | O |
| 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 | E | W |
| 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 | R | D |
| 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 | E | E |

# 6. The CIA Kryptos sculpture

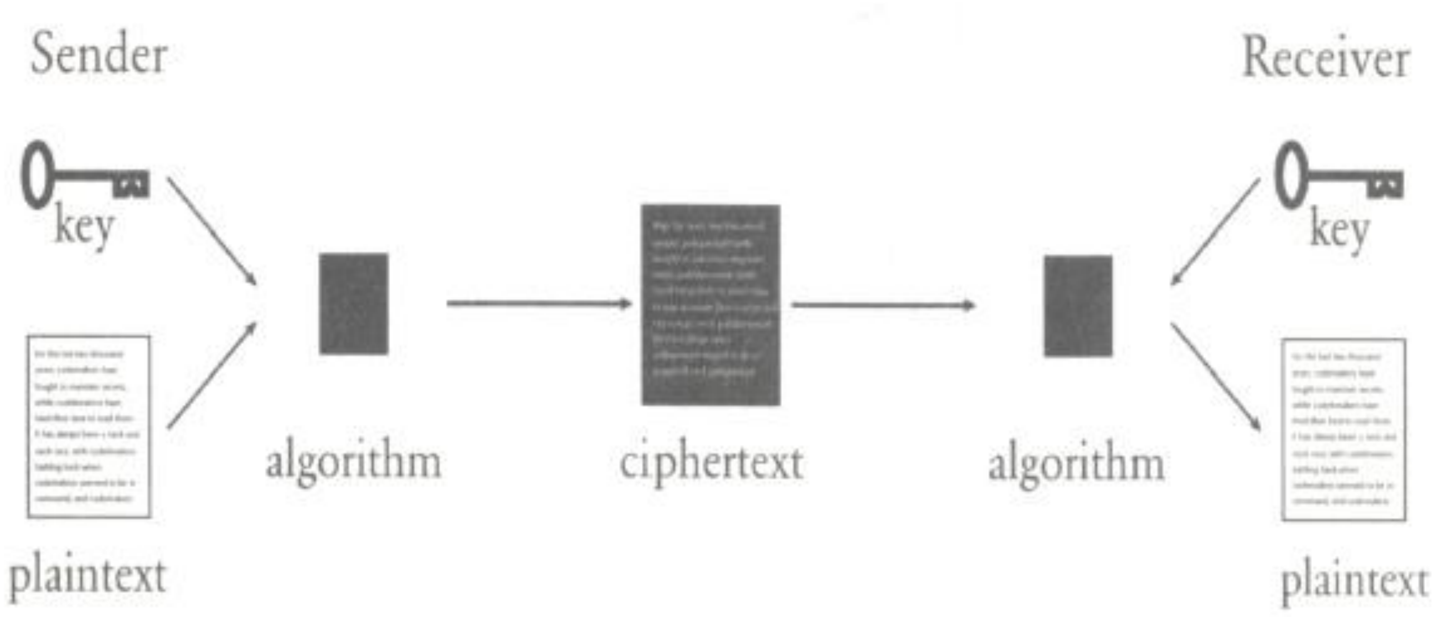
- Three of the messages have been decrypted. The fourth has not.



"Kryptos sculptor" by Jim Sanborn - Jim Sanborn. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Kryptos_sculptor.jpg#/media/File:Kryptos_sculptor.jpg

# Summarising

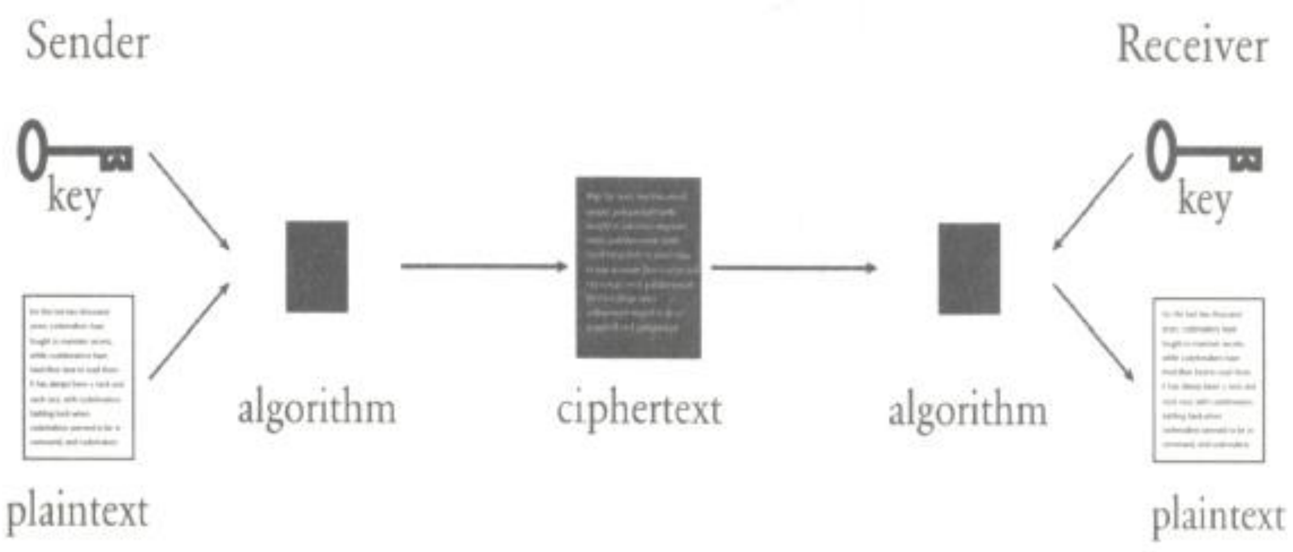
- In the process depicted below, the key must be kept secret
- The Caesar cipher is weak because there are only 25 keys



Picture from: Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000, p.11

# 7. Enter the computer

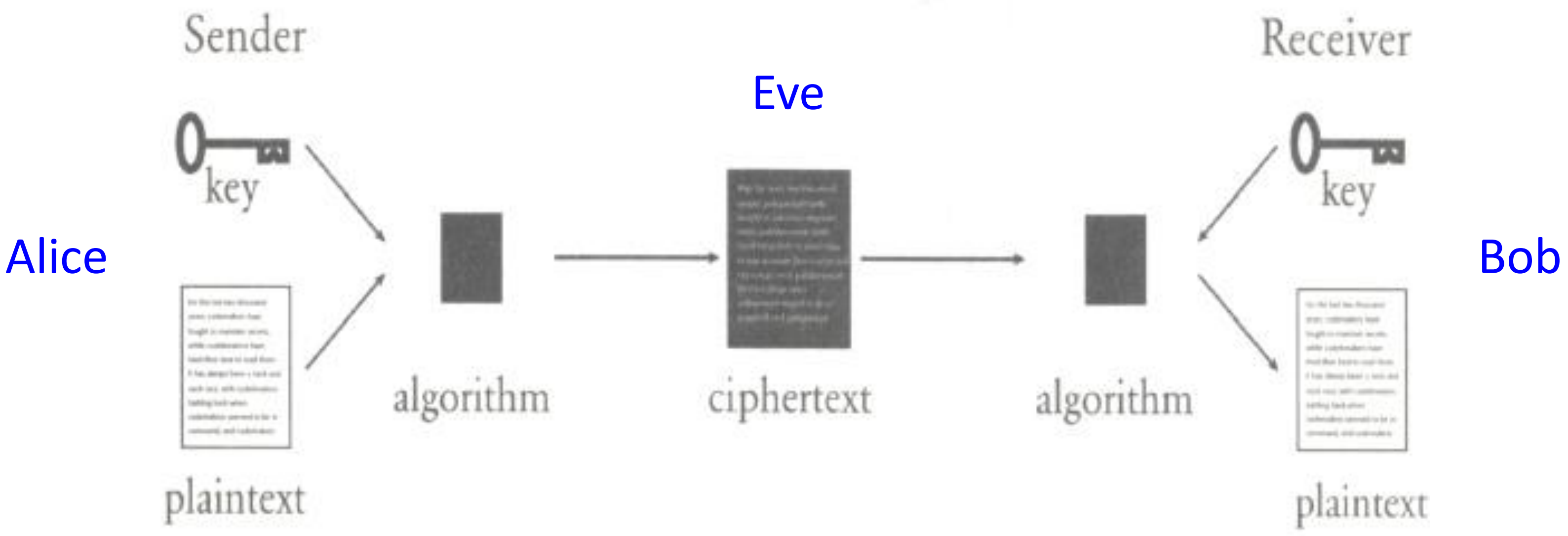
- When using a computer the message string is converted into binary before being communicated
- Companies communicating required standard
- 1976: DES – Data Encryption Standard. Complex algorithm.



Picture from: Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000, p.11

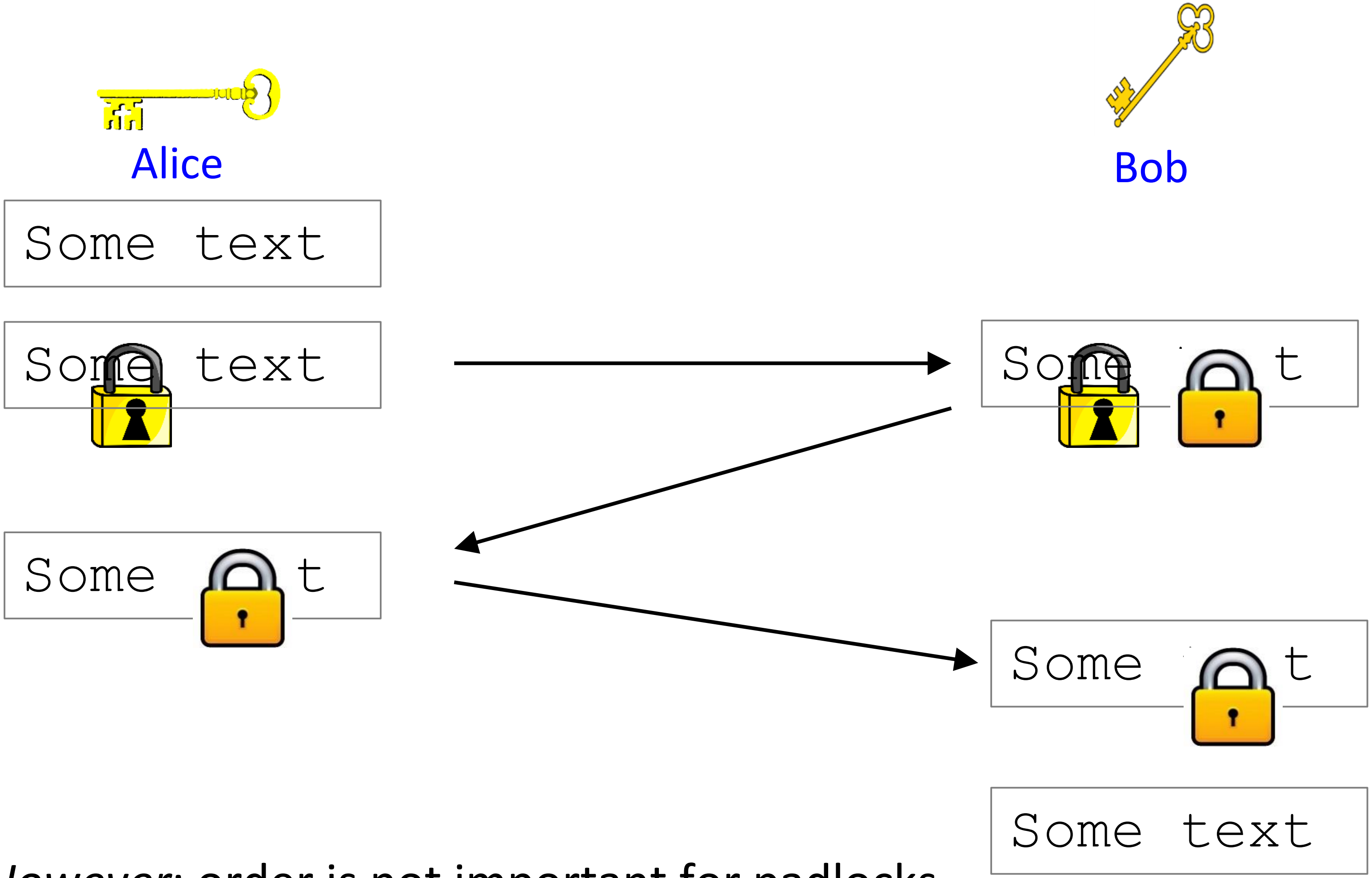
# 8. Private-key (symmetric) systems

- The key-distribution problem: The sender and receiver both know and use the same key. But how do they share the key in the first place? (If they have a secure channel for sending the key, why not use it for the message as well?)



Picture from: Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000, p.11

# 8.1 Solving the problem of key distribution?



Alice

Bob

Some text

Some text

Some t

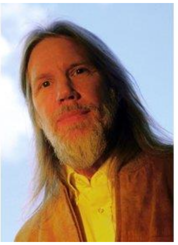
Some t

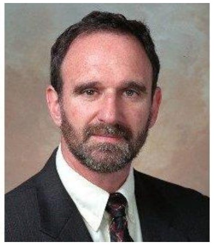
Some t

Some text

- *However*: order is not important for padlocks, but it is for computer algorithms

# 8.2 Whitfield Diffie and Martin Helman





- Instead of two-way function, e.g. doubling and halving
- Focus: one-way function
- Modular arithmetic (clock arithmetic)
- 2 + 3 = 5 (mod 7)
- 2 + 6 = 1 (mod 7)
- 6 * 5 = 2 (mod 7)
- $3^x = 81$. What is x?
- $3^x$ (mod 7) = 1. What is x?

"Whitfield Diffie" by The original uploader was Matt Crypto at English Wikipedia - Transferred from en.wikipedia to Commons. Licensed under CC BY 2.0 via Commons - https://commons.wikimedia.org/wiki/File:Whitfield_Diffie.png#/media/File:Whitfield_Diffie.png

"Martin-Hellman" by User .:Ajvol:. on en.wikipedia - Originally from en.wikipedia; description page is (was) here07:35, 21 October 2004 .:Ajvol:. 240x280 (13,237 bytes) (Martin Hellman). Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Martin-Hellman.jpg#/media/File:Martin-Hellman.jpg

# 8.2 Diffie and Helman (1976)

- $Y^x$ (mod P)
- Alice and Bob agree on Y=7 and P=11 and contact each other with these details

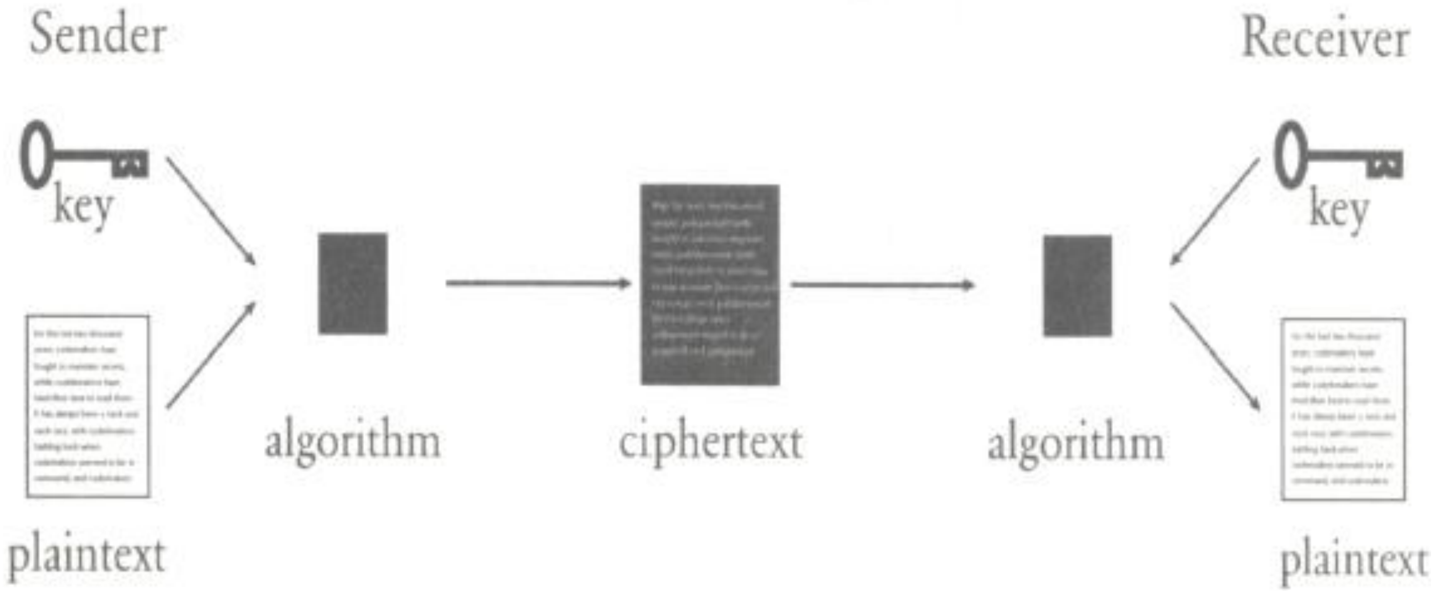
| | |
|---|---|
| Alice chooses A=3 (secret) | Bob choose B=6 (secret) |
| $\alpha = 7^A$ (mod 11) = 2 | $\beta = 7^B$ (mod 11) = 4 |
| Send $\alpha$ to Bob | Send $\beta$ to Alice |
| Doesn’t matter if Eve intercepts the numbers | |
| Alice calculates key<br>$\beta^A$ (mod 11) = 9 | Bob calculates key<br>$\alpha^B$ (mod 11) = 9 |

- The process (which would use much larger numbers) produces a key that can be used in, say, a DES process.

Picture from: Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000, p.265

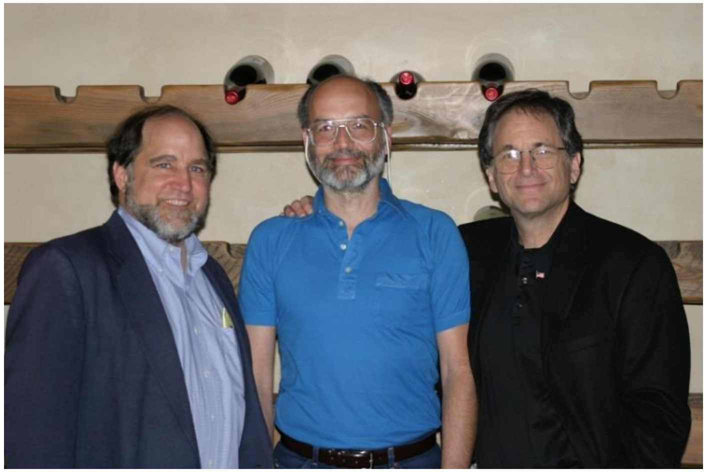
# 9. Public-key (asymmetric systems)

- The sender and receiver use different keys.
- Having one key doesn't provide enough information to deduce the other.



Picture from: Simon Singh. The Code Book – The Secret History of Codes and Codebreaking, Fourth Estate, 2000

## 9.1 The RSA cryptosystem (1977)



- Ron Rivest, Adi Shamir, Len Adleman
- The encryption key is public
- The decryption key is secret

- Alice uses Bob’s public key to encrypt the message
- Alice sends encrypted message to Bob
- Bob uses his private key to decrypt the message

- Involves choosing two large prime numbers p and q and computing n=p*q. The larger the primes, the better.
- A ‘one-way’ function that is reversible if p and q are known.

http://www.usc.edu/dept/molecular-science/RSA-2003.htm

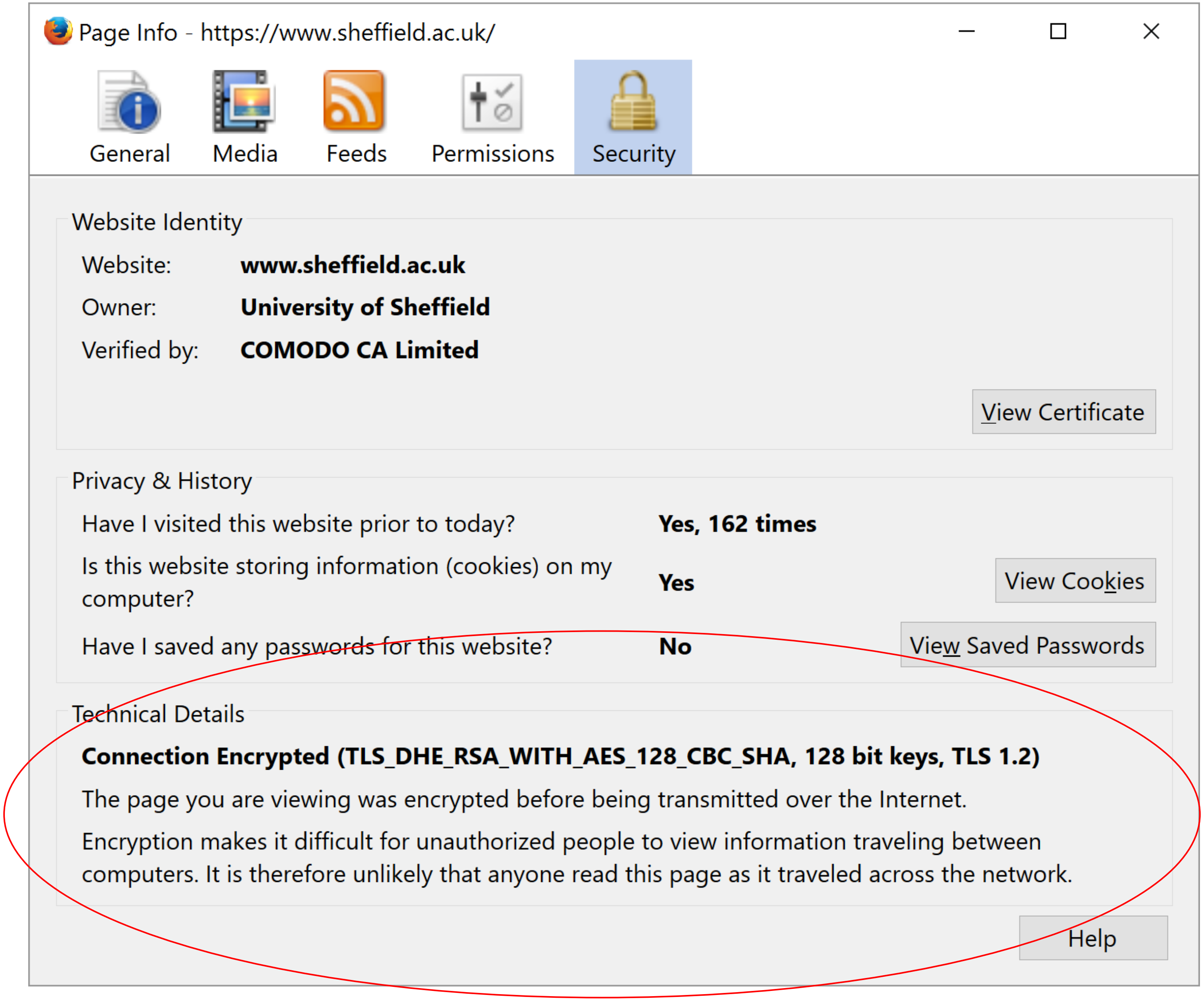
# 10. The alternative history

- GCHQ, 1969, James Ellis has similar ideas to Diffie and Hellman
- (Government Communications Headquarters)

- GCHQ, 1973, Clifford Cocks developed encryption algorithm, later independently rediscovered as RSA
- Cocks's work remained secret until 1997

Clifford Cocks in 2015

"Clifford-Cocks-FRS" by Royal Society uploader - Own work. Licensed under CC BY-SA 4.0 via Commons - https://commons.wikimedia.org/wiki/File:Clifford-Cocks-FRS.jpg#/media/File:Clifford-Cocks-FRS.jpg



Website Identity

Website: **www.sheffield.ac.uk**

Owner: **University of Sheffield**

Verified by: **COMODO CA Limited**

Privacy & History

Have I visited this website prior to today? **Yes, 162 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

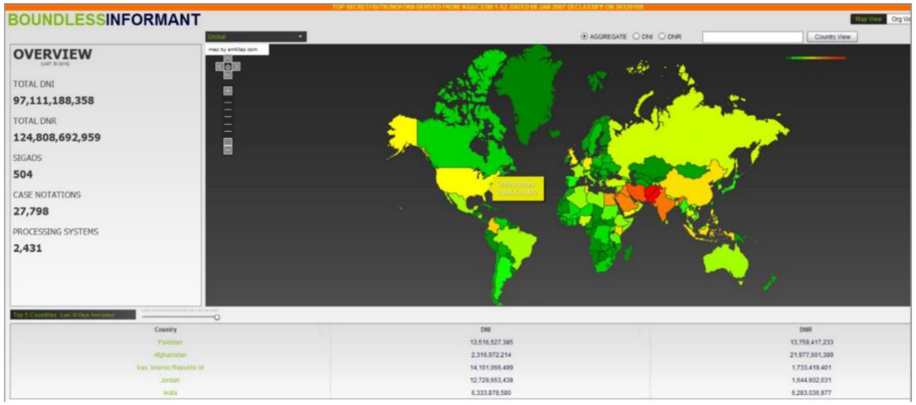
Technical Details

**Connection Encrypted (TLS_DHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

# Ongoing security discussions…



TOP SECRET//SI//TK//NOFORN DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108

BOUNDLESSINFORMANT

**OVERVIEW**
(LAST 30 DAYS)

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

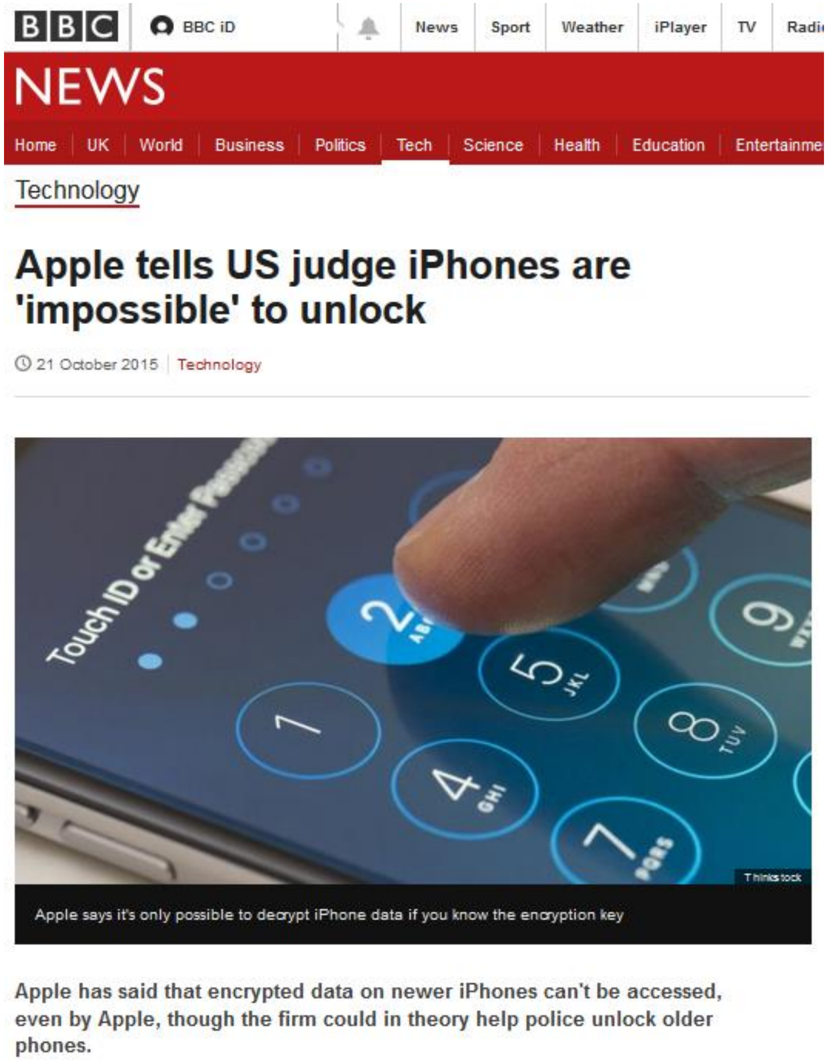
PROCESSING SYSTEMS
2,431

Top 5 Countries (Last 30 Days from today)

| Country | DNI | DNR |
|---|---|---|
| Pakistan | 13,516,527,385 | 13,759,417,233 |
| Afghanistan | 2,316,972,214 | 21,977,001,389 |
| Iran, Islamic Republic of | 14,101,066,499 | 1,733,419,401 |
| Jordan | 12,729,653,438 | 1,644,602,031 |
| India | 6,333,878,580 | 6,283,036,977 |

The worldwide heat map from the NSA's data visualisation tool BOUNDLESSINFORMANT, showing that during a 30-day period, 97 billion internet data records (DNI) and 124 billion telephony data records (DNR) were collected.

"Boundless-heatmap-large-0001" by Iamthechitt - Own work. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Boundless-heatmap-large-0001.png#/media/File:Boundless-heatmap-large-0001.png



Technology

## Apple tells US judge iPhones are 'impossible' to unlock

21 October 2015 | Technology

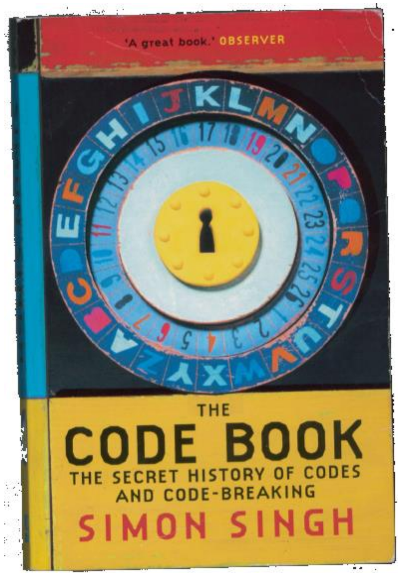
Thinkstock

Apple says it's only possible to decrypt iPhone data if you know the encryption key

Apple has said that encrypted data on newer iPhones can't be accessed, even by Apple, though the firm could in theory help police unlock older phones.

# 11. Summary

- Cryptology has a long history
- There are many systems still waiting to be cracked
- Significant changes have occurred since the 1970s
- Systems can be cracked even if they have a reputation for being secure



## Exercise: Cracking the Vigenère cipher

- How might we decrypt the following message? The original is in English, a Vigenère cipher has been used, and the punctuation has conveniently been left visible.

```
ALPCS'Z RZ YSLH EZ ZPKSE O UMRSH SMRSH
VR L WWNLE YWNLE WWRI EZBPKSE,
TVV L YWNLE WWNLE'D PBX L DZPKSE ZPKSE
CU E WTUOX YTUOX WTYL XZYWNLE.
```

# Module summary

- The ‘InterWeb’ – the Internet, the WWW
- Networks and protocols
- Web site development
  - Responsive web design, accessibility
- Front-end: HTML, CSS, JavaScript, jQuery
- Graphics on the Canvas, SVG
- Information security
  - Information, goals: CIA, practicalities, e.g. XSS, e-commerce, legal aspects, cryptography

- Hope you have enjoyed the module!!