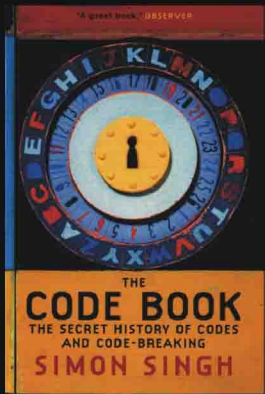


The Code Book on CD-ROM

The Code Book on CD-ROM is an interactive version of Simon Singh's best-selling book *The Code Book*. It includes a wealth of material including video clips from Simon Singh's channel 4 television series 'The Science of Secrecy' plus other clips filmed specifically for the CD-ROM. Text from the book is presented in easily digested chunks that are illustrated with video clips, computer generated animations and interactive tools and demonstrations. The interactive tools enable messages to be encrypted using all the ciphers discussed in the book.

Most impressive of all is the full Enigma Machine emulator. Other tools assist with the cracking of encrypted messages using techniques such as frequency analysis. There are also numerous puzzles and encrypted messages to be cracked. The CD-ROM presents a fascinating subject in a very hands-on format, so that anyone can try out the encryption and cracking methods described in the text, but with the computer doing any tedious analysis that might be necessary. The CD-ROM makes full use of the potential of multimedia to communicate technical ideas.



- Welcome Page
- Introduction Page
- Index
- Highlights
- The Code Book
- Book Reviews
- Simon Singh
- Teachers Section
- Junior Codebreakers
- Code Competition
- Crypto Corner and Links
- How to obtain further CD-ROMs
- Made by Virtual Image
- Bletchley Park
- Feedback and Newsletter
- Main Menu

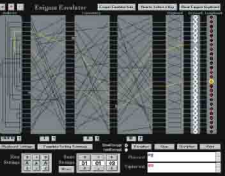
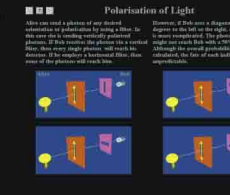
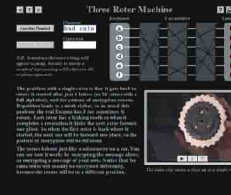
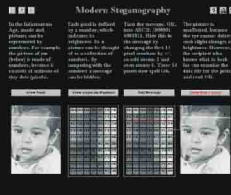
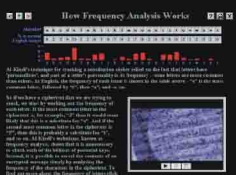
- The Birth of Cryptography
- Transposition
- The Railfence Cipher
- Latin Square
- Scytale
- Substitution
- Caesar Shift Cipher
- How to make a Caesar Wheel
- Kama-Sutra Cipher
- Pigpen Cipher
- Pigpen Gravestone
- Atbash Cipher
- Affine Cipher
- Affine Cipher Tool
- General Monoalphabetic Cipher
- Cracking the Substitution Cipher
- Invention in Baghdad
- How Frequency Analysis Works
- Finer Points
- Frequency Analysis Tool
- Frequency Analysis Puzzle
- Statistics
- Key Secrets
- Number of Keys for Various Ciphers
- Kerckhoffs' Principle
- The Tragedy of Mary Queen of Scots
- The Babington Plot
- Cracking the Babington Cipher
- The Execution of Mary Queen of Scots

- The Uncrackable Code
- Vigenère Cipher
- Swapping Cipher Alphabets
- The Vigenère Square
- How Vigenère Works
- The Vigenère Tool
- Why is Vigenère so strong?
- Alternative Ciphers
- Digraph Substitution
- Oldest Digraph Cipher
- Dancing Men Cipher
- Homophonic Ciphers
- Book Ciphers
- The Beale Ciphers
- Encryption for the Masses
- Morse Code
- Dancing Men Cipher
- Agony Columns
- Pinprick Cipher
- Cracking the Vigenère Cipher
- Charles Babbage
- Babbage's Computers
- Babbage the Codebreaker
- The Cracking Principle
- A Cracking Example
- Vigenère Cracking Tool
- Forgotten Genius

- Mechanisation of Secrecy
- World War I
- Codes
- The Zimmermann Telegram
- Cracking Zimmermann
- The Weakness of Codes
- ADFGVX Cipher
- Building Enigma
- Meet the Machine
- Basic Principle
- Three Rotor Machine
- Reflector
- Plugboard
- Complete Overview of Enigma
- Using the Enigma
- Who Used Enigma?
- What is the Key?
- How Many Keys?
- Agreeing a Key
- Enigma Emulator
- Enigma Emulator Info
- How to Select a Key
- Cracking the Enigma
- Polish Codebreakers
- Bletchley Park
- Cribs
- Turing's Bombe
- Bombe Demo
- Flaws in the Enigma
- By Hook or by Crook
- Enigma's Impact on World War II
- Secret Success
- Other World War II Ciphers
- CodeTalkers

- The Age of the Internet
- Computer Cryptography
- Substitution
- Transposition
- Data Encryption Standard
- How DES Works
- Other Modern Ciphers
- Key Distribution Problem
- Alice, Bob and Eve
- God Rewards Fools
- Apparent Solution
- Padlocks commute, but ...
- Public Key Cryptography
- Asymmetric Cipher
- Alice and Bob Explain
- Mathematical Padlock
- Rivest, Shamir and Adelman
- Modular Arithmetic
- A One-way Function
- Broad Argument
- RSA Algorithm
- How do you calculate d?
- RSA Encryption Tool
- Prime Number Questions
- Eratosthenes Sieve
- RSA in Practice
- Is RSA Secure?
- Not Just Secrets
- The Secret History
- James Ellis and Clifford Cocks
- Malcolm Williamson
- 25 Year Secret

- Future of Cryptography
- Politics of Encryption
- Pro Encryption
- Anti Encryption
- Steganography
- Modern Steganography
- Quantum Cryptography
- One Time Pad
- Polarisation of Light
- Quantum Crypto Protocol
- The End?



The Code Book on CD-ROM is available FREE with any software ordered from Virtual Image



Virtual Image, 184 Reddish Road, South Reddish, Stockport SK5 7HS, U.K.

Tel: (+44) (0)161 480 1915 Fax: (+44) (0)161 612 2965