The Code Book

- Simon Singh

  Other Books:
  Fermat's Enigma
  The Big Bang

The Code Book

- The Science of Secrecy from Ancient Egypt to Quantum Cryptography

- Cypher of Mary Queenof Scotts
- Le Chiffre Indechiffrable
- Mechanization of Secrecy
- Cracking the Enigma
- Language Barrier (Rosetta Stone)
- Digital -- Keys Alice & Bob go ‘Public’.

The Code Book (Contents cont'd)

- The Science of Secrecy from Ancient Egypt to Quantum Cryptography
- Zimmerman –Keys for the 'People'
- Deutsch-Quantum Computing

The Code Book

- Summary—
- Many schemes of Code are possible & have been employed-- ALL HAVE BEEN BROKEN!!
- Core issue is ‘Will the Code be broken (or conversely, safe) within the time required to be relevant ??’
- If an order is transmitted, can it be intercepted and decoded in sufficient time to prevent it from being carried out ??

The Code Book

- Code Makers (Encryption-Cipher) and Code Breakers (Decipherment-Cryptanalysis) continue in a never ending intellectual arms race. It is an evolutionary struggle with implications in essentially all aspects of life –personal, religious, political, military, and business.
- The Code Book reviews many of these issues, essentially from the earliest time of the history of man to the present.
- While there are many books on Codes, Singh has a historical presentation covering the entire field with sufficient depth to be considered SCIENCE.

Mary Queen of Scots

- Mary's supporters employed a 'nomenclator' for the alphabetic letters ('j', 'v' and 'w' not used), and 35 symbols representing words or phrases. Also 4 'nulls' and a 'doublith'.
- The Code was broken, and the carrier of the message to start an uprising was intercepted and Mary later 'beheaded'.

Code Development (Language Based-MonoAlphabetic)

- Code –Word/Symbol replaced by Word/Symbol: Attack at Dawn>>Jupiter
- Cipher --More fundamental level-replacing letter by letter).
  Example --Each letter in a phrase
  is replace by the next letter.
- A>>B, B>>C, etc.
- A t t a c k a t D a w n
  B u u b d l b u E b x o

Code Development

- Frequency Analysis
  Based upon the statistical distribution of letters in the English language:
- Letter Percentage
- ‘a’ >>>> 8.2%
- ‘b’ >>>> 1.5%
- ‘e’ >>>> 12.7%
- ‘t’ >>>> 9.1%
- ‘y’ >>>> 2.0%
- ‘z’ >>>> 0.1%

Code Development (PolyAlphabetic)

- Switching Cipher Alphabets (2)
- Plain Text
  abcde fghij klmno pqsrt uvwxyz
- Cipher Alphabet No. 1
  FZBVK IXAYM EPLSD HJORG NQCUTW
- Cipher Alphabet No. 2
  GOXBF WTHQI LAPZJ DESVY CRKUHN
- Plain Text: ‘hello’
- A(1) F(2) P(1) A(2) D(1) >>AFPAD
- Same plaintext letter not encoded identically within message.

Code Development (Vigenere Square)

- Plain: a b c d e…… x y z
- 1 B C D E F……Y Z A
- 2 C D E F G ……Z A B
- 3 D E F G H…… A B C
- 4 E F G H I…… ..B C D
- ……
- ……
- 25 Z A B C D……W X Y
- 26 A B C D E……X Y Z

Code Development (Vigenere Square)

- Vigenere's strength is that it has 26 distinct cipher alphabets to encrypt the message.
- Row 1 is a 'Ceasar shift' of 1.
- Row 2 is a 'Ceasar shift' of 2, etc.
- 'a' ROW 2 becomes C
- 'a' ROW 4 becomes E
- KEYWORD—To unscramble, it is necessary for the intended receiver of the message to know which ROW of 'V' Square enciphers each letter.
- Let 'WHITE' be the KEYWORD.
- Let plaintext message be 'divert troops to east ridge'.

‘V’ Square (cont’d)

- KEYWORD: WHITE (5 letters)
  WHITEW HITEWHI TE WHIT EWHIT
- plaintext:
  divert troops to east ridge
- Ciphertext
  ZPDXVP AZHSLZ BH IWZB KMZNM
- ‘V’ is impregnable to Frequency Analysis—it was neglected for 200 years.

‘Lost’ Languages

- Singh includes an interesting chapter on ‘Lost’ Languages.
- While these are not actually considered part of Cryptology, the same techniques for Decoding are employed. The ‘Lost’ Languages include:
  The Rosetta Stone –Hieroglyphics.
  Linear ‘a’ & ‘b’.
  The Navajo Indian Code Talkers.

‘Capturing’ The Enigma

- Enigma is an electrical/ mechanical device for converting plaintext messages into code for transmission over Military radio or telegraph channels, and invented in Germany in 1918 (Scherbius).
- The Polish purchased a commerical version but determined the German Navy & Army had upgraded devices that were different and could not be decoded.
- The French purchased a unit & code from a German officer, but could not break the code. They approached the Polish & British for help. Marian Rejewski recreated rotors and the patch board, and in three months broke code. They turned over their machine, simulator and all code info British.
- The British obtained a Navy unit from sinking sub & all material was sent to Turing at Bettchley Park. He developed a multiple channel version called the ‘bombe’ to speed the decoding process.

Enigma Photographs

- Photos—Top Open, Closed, Rotors & Patch Board.
- The Rotors moved 1/26 of a revolution each Keystroke. A complete rotation of first Rotor caused the second to move 1/26 of a revolution, likewise third. Additionally, the patch board plugs could be could rearranged.
- The number of staring positions was between 2 & 3 billion. It would take 100 machines 5.8 years to exhaust all possibilities.
- Turing built the ‘Bombe’ to facilitate faster decoding.

Alice & Bob go Public

- Alice wants to send message to Bob employing a secure Assymetric Code (similar to Lucifer) over the Internet, but Eve can 'Eve's drop'. While the actual message is Secure, it was necessary that the Key be agreed to usually, requiring a conversation prior to the Internet transmission. The Key is a digital number and it would be desirable to simply combine it with the message. This problem was envisioned by Duffy at SUN Microsystems, and later solved by Rives, Shamir and Adleman (known as 'RSA') at MIT in 1977.
- Alice develops her Public code which is produced using a One –way Modular mathematical code and the Product (N) -175,828,273 of two Prime Numbers, (p) -17,159 & (q) -10,247. This is called the Public Encription Key. These numbers are agreed to by Bob & Alice, and permit them to safely communicate.
- Eve can try to determine 'p' & 'q' by 'Factoring' N, but for a 56 bit Key implementation, N approaches 10^308, taking one hundred million PCs, 1000 years to be broken.

Quantum Computing

- While the RSA Cipher is presently impenetrable, attempts for to break it continue. Using machines based upon classical physics requires Factoring each possible prime number to be inputted and processed sequentially, requiring billions of times more speed than presently available. Using the Quantum machine the numbers are entered and processed simultaneously. ‘Superposition’ of possible inputs reduces the time dramatically by performing the input and processing functions simultaneously. A 250 ’cubit’ machine can perform calculations 10^75 times faster than a conventional computer!
- When will one be built ?