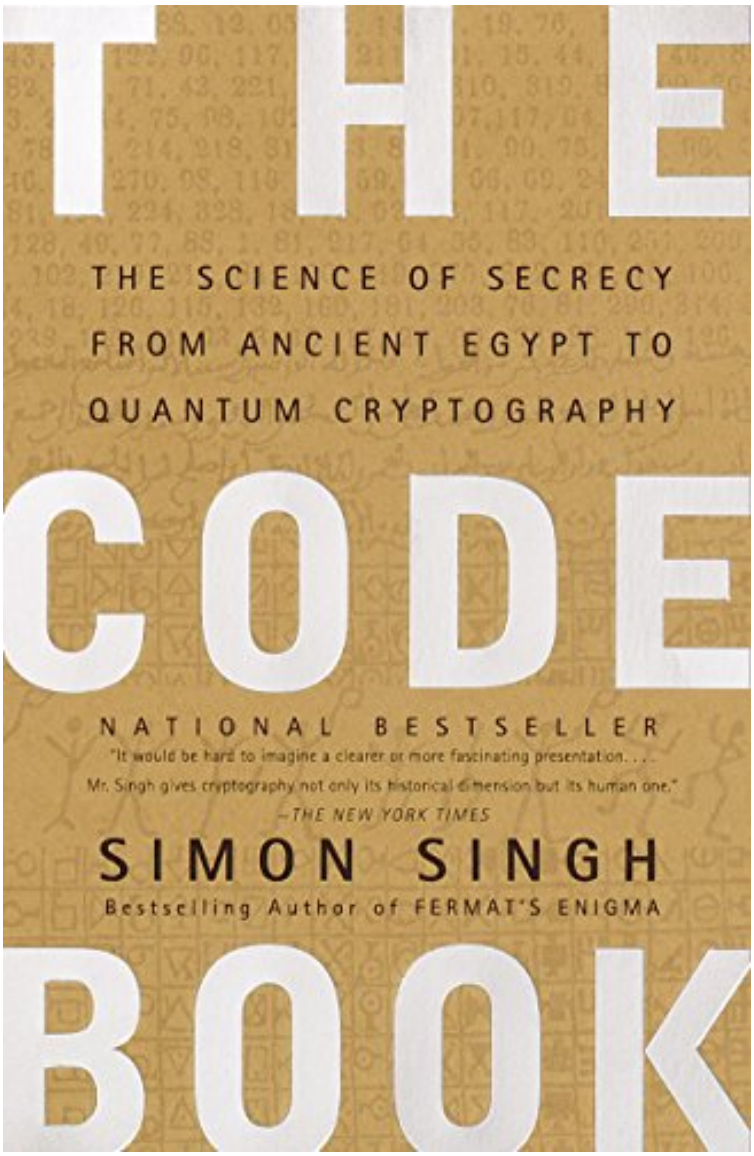
[PDF] File size: 69.Mb

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography



Download Read Online

Par Simon Singh
*ebooks | Download PDF | *ePub | DOC | audiobook*

Dtails sur le produit Rang parmi les ventes : #46176 dans eBooksPubli le: 2011-01-26Sorti le: 2011-01-26Format: Ebook Kindle

[PDF] The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Par Simon Singh : The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography before purchasing it in order to gage whether or not it would be worth my time, and all praised The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography:

Description :

Prsentation de l'diteurIn his first book since the bestselling Fermat's Enigma, Simon Singh offers the first sweeping history of encryption, tracing its evolution and revealing the dramatic effects codes have had on wars, nations, and individual lives. From Mary, Queen of Scots, trapped by her own code, to the Navajo Code Talkers who helped the Allies win World War II, to the incredible (and incredibly simple) logisitical breakthrough that made Internet commerce secure, The Code Book tells the story of the most powerful intellectual weapon ever known: secrecy.Throughout the text are clear technical and mathematical

explanations, and portraits of the remarkable personalities who wrote and broke the world's most difficult codes. Accessible, compelling, and remarkably far-reaching, this book will forever alter your view of history and what drives it.It will also make you wonder how private that e-mail you just sent really is..comPeople love secrets, and ever since the first word was written, humans have written coded messages to each other. In The Code Book, Simon Singh, author of the bestselling Fermat's Enigma, offers a peek into the world of cryptography and codes, from ancient texts through computer encryption. Singh's compelling history is woven through with stories of how codes and ciphers have played a vital role in warfare, politics, and royal intrigue. The major theme of The Code Book is what Singh calls "the ongoing evolutionary battle between codemakers and codebreakers," never more clear than in the chapters devoted to World War II. Cryptography came of age during that conflict, as secret communications became critical to either side's success. Confronted with the prospect of defeat, the Allied cryptanalysts had worked night and day to penetrate German ciphers. It would appear that fear was the main driving force, and that adversity is one of the foundations of successful codebreaking. In the information age, the fear that drives cryptographic improvements is both capitalistic and libertarian--corporations need encryption to ensure that their secrets don't fall into the hands of competitors and regulators, and ordinary people need encryption to keep their everyday communications private in a free society. Similarly, the battles for greater decryption power come from said competitors and governments wary of insurrection. The Code Book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography. Singh's accessible style and clear explanations of complex algorithms cut through the arcane mathematical details without oversimplifying. Can't get enough crypto? Try solving the Cipher Challenge in the back of the book--$15,000 goes to the first person to crack the code! --Therese LittletonExtraitOn the morning of Wednesday, 15 October 1586, Queen Mary entered the crowded courtroom at Fotheringhay Castle. Years of imprisonment and the onset of rheumatism had taken their toll, yet she remained dignified, composed and indisputably regal. Assisted by her physician, she made her way past the judges, officials and spectators, and approached the throne that stood halfway along the long, narrow chamber. Mary had assumed that the throne was a gesture of respect towards her, but she was mistaken. The throne symbolised the absent Queen Elizabeth, Mary's enemy and prosecutor. Mary was gently guided away from the throne and towards the opposite side of the room, to the defendant's seat, a crimson velvet chair.Mary Queen of Scots was on trial for treason. She had been accused of plotting to assassinate Queen Elizabeth in order to take the English crown for herself. Sir Francis Walsingham, Elizabeth's Principal Secretary, had already arrested the other conspirators, extracted confessions, and executed them. Now he planned to prove that Mary was at the heart of the plot, and was therefore equally culpable and equally deserving of death.Walsingham knew that before he could have Mary executed, he would have to convince Queen Elizabeth of her guilt. Although Elizabeth despised Mary, she had several reasons for being reluctant to see her put to death. First, Mary was a Scottish queen, and many questioned whether an English court had the authority to execute a foreign head of state. Second, executing Mary might establish an awkward precedent -- if the state is allowed to kill one queen, then perhaps rebels might have fewer reservations about killing another, namely Elizabeth. Third, Elizabeth and Mary were cousins, and their blood tie made Elizabeth all the more squeamish about ordering her execution. In short, Elizabeth would sanction Mary's execution only if Walsingham could prove beyond any hint of doubt that she had been part of the assassination plot.The conspirators were a group of young English Catholic noblemen intent on removing Elizabeth, a Protestant, and replacing her with Mary, a fellow Catholic. It was apparent to the court that Mary was a figurehead for the conspirators, but it was not clear that she had actually given her blessing to the conspiracy. In fact, Mary had authorised the plot. The challenge for Walsingham was to demonstrate a palpable link between Mary and the plotters.On the morning of her trial, Mary sat alone in the dock, dressed in sorrowful black velvet. In cases of treason, the accused was forbidden counsel and was not permitted to call witnesses. Mary was not even allowed secretaries to help her prepare her case. However, her plight was not hopeless because she had been careful to ensure that all her correspondence with the conspirators had been written in cipher. The cipher turned her words into a meaningless series of symbols, and Mary believed that even if Walsingham had captured the letters, then he could have no idea of the meaning of the words within them. If their contents were a mystery, then the letters could not be used as evidence against her. However, this all depended on the assumption that her cipher had not been broken.Unfortunately for Mary, Walsingham was not merely Principal Secretary, he was also England's spymaster. He had intercepted Mary's letters to the plotters, and he knew exactly who might be capable of deciphering them. Thomas Phelippes was the nation's foremost expert on breaking codes, and for

years he had been deciphering the messages of those who plotted against Queen Elizabeth, thereby providing the evidence needed to condemn them. If he could decipher the incriminating letters between Mary and the conspirators, then her death would be inevitable. On the other hand, if Mary's cipher was strong enough to conceal her secrets, then there was a chance that she might survive. Not for the first time, a life hung on the strength of a cipher.The Evolution of Secret WritingSome of the earliest accounts of secret writing date back to Herodotus, 'the father of history' according to the Roman philosopher and statesman Cicero. In The Histories, Herodotus chronicled the conflicts between Greece and Persia in the fifth century bc, which he viewed as a confrontation between freedom and slavery, between the independent Greek states and the oppressive Persians. According to Herodotus, it was the art of secret writing that saved Greece from being conquered by Xerxes, King of Kings, the despotic leader of the Persians.The long-running feud between Greece and Persia reached a crisis soon after Xerxes began constructing a city at Persepolis, the new capital for his kingdom. Tributes and gifts arrived from all over the empire and neighbouring states, with the notable exceptions of Athens and Sparta. Determined to avenge this insolence, Xerxes began mobilising a force, declaring that 'we shall extend the empire of Persia such that its boundaries will be God's own sky, so the sun will not look down upon any land beyond the boundaries of what is our own'. He spent the next five years secretly assembling the greatest fighting force in history, and then, in 480 bc, he was ready to launch a surprise attack.However, the Persian military build-up had been witnessed by Demaratus, a Greek who had been expelled from his homeland and who lived in the Persian city of Susa. Despite being exiled he still felt some loyalty to Greece, so he decided to send a message to warn the Spartans of Xerxes' invasion plan. The challenge was how to dispatch the message without it being intercepted by the Persian guards. Herodotus wrote:As the danger of discovery was great, there was only one way in which he could contrive to get the message through: this was by scraping the wax off a pair of wooden folding tablets, writing on the wood underneath what Xerxes intended to do, and then covering the message over with wax again. In this way the tablets, being apparently blank, would cause no trouble with the guards along the road. When the message reached its destination, no one was able to guess the secret, until, as I understand, Cleomenes' daughter Gorgo, who was the wife of Leonides, divined and told the others that if they scraped the wax off, they would find something written on the wood underneath. This was done; the message was revealed and read, and afterwards passed on to the other Greeks.As a result of this warning, the hitherto defenceless Greeks began to arm themselves. Profits from the state-owned silver mines, which were usually shared among the citizens, were instead diverted to the navy for the construction of two hundred warships.Xerxes had lost the vital element of surprise and, on 23 September 480 bc, when the Persian fleet approached the Bay of Salamis near Athens, the Greeks were prepared. Although Xerxes believed he had trapped the Greek navy, the Greeks were deliberately enticing the Persian ships to enter the bay. The Greeks knew that their ships, smaller and fewer in number, would have been destroyed in the open sea, but they realised that within the confines of the bay they might outmanoeuvre the Persians. As the wind changed direction the Persians found themselves being blown into the bay, forced into an engagement on Greek terms. The Persian princess Artemisia became surrounded on three sides and attempted to head back out to sea, only to ram one of her own ships. Panic ensued, more Persian ships collided and the Greeks launched a full-blooded onslaught. Within a day, the formidable forces of Persia had been humbled.Demaratus' strategy for secret communication relied on simply hiding the message. Herodotus also recounted another incident in which concealment was sufficient to secure the safe passage of a message. He chronicled the story of Histaiaeus, who wanted to encourage Aristagoras of Miletus to revolt against the Persian king. To convey his instructions securely, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to regrow. This was clearly a period of history that tolerated a certain lack of urgency. The messenger, apparently carrying nothing contentious, could travel without being harassed. Upon arriving at his destination he then shaved his head and pointed it at the intended recipient.Secret communication achieved by hiding the existence of a message is known as steganography, derived from the Greek words steganos, meaning 'covered', and graphein, meaning 'to write'. In the two thousand years since Herodotus, various forms of steganography have been used throughout the world. For example, the ancient Chinese wrote messages on fine silk, which was then scrunched into a tiny ball and covered in wax. The messenger would then swallow the ball of wax. In the fifteenth century, the Italian scientist Giovanni Porta described how to conceal a message within a hard-boiled egg by making an ink from a mixture of one ounce of alum and a pint of vinegar, and then using it to write on the shell. The solution penetrates the porous shell, and leaves a message on the surface of the hardened egg albumen, which can be read only when the shell is

removed. Steganography also includes the practice of writing in invisible ink. As far back as the first century ad, Pliny the Elder explained how the 'milk' of the thithymallus plant could be used as an invisible ink. Although transparent after drying, gentle heating chars the ink and turns it brown. Many organic fluids behave in a similar way, because they are rich in carbon and therefore char easily. Indeed, it is not unknown for modern spies who have run out of standard-issue invisible ink to improvise by using their own urine. The longevity of steganography illustrates that it certainly offers a modicum of security, but it suffers from a fundamental weakness. If the messenger is searched and the message is discovered, then the contents of the secret communication are revealed at once. Interception of the message immediately compromises all security. A thorough guard might routinely search any person crossing a border, scraping any wax tablets, heating blank sheets of paper, shelling boiled eggs, shaving people's heads, and so on, and inevitably there will be occasions when the message is uncovered. Hence, in parallel with the development of steganography, there was the evolution of cryptography, derived from the Greek word kryptos, meaning 'hidden'. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, a process known as encryption. To render a message unintelligible, it is scrambled according to a particular protocol which is agreed beforehand between the sender and the intended recipient. Thus the recipient can reverse the scrambling protocol and make the message comprehensible. The advantage of cryptography is that if the enemy intercepts an encrypted message, then the message is unreadable. Without knowing the scrambling protocol, the enemy should find it difficult, if not impossible, to recreate the original message from the encrypted text.Although cryptography and steganography are independent, it is possible to both scramble and hide a message to maximise security. For example, the microdot is a form of steganography that became popular during the Second World War. German agents in Latin America would photographically shrink a page of text down to a dot less than 1 millimetre in diameter, and then hide this microdot on top of a full stop in an apparently innocuous letter. The first microdot to be spotted by the FBI was in 1941, following a tip-off that the Americans should look for a tiny gleam from the surface of a letter, indicative of smooth film. Thereafter, the Americans could read the contents of most intercepted microdots, except when the German agents had taken the extra precaution of scrambling their message before reducing it. In such cases of cryptography combined with steganography, the Americans were sometimes able to intercept and block communications, but they were prevented from gaining any new information about German spying activity. Of the two branches of secret communication, cryptography is the more powerful because of this ability to prevent information from falling into enemy hands.In turn, cryptography itself can be divided into two branches, known as transposition and substitution. In transposition, the letters of the message are simply rearranged, effectively generating an anagram. For very short messages, such as a single word, this method is relatively insecure because there are only a limited number of ways of rearranging a handful of letters. For example, three letters can be arranged in only six different ways, e.g. cow, cwo, ocw, owc, wco, woc. However, as the number of letters gradually increases, the number of possible arrangements rapidly explodes, making it impossible to get back to the original message unless the exact scrambling process is known. For example, consider this short sentence. It contains just 35 letters, and yet there are more than 50,000,000,000,000,000,000,000,000,000,000 distinct arrangements of them. If one person could check one arrangement per second, and if all the people in the world worked night and day, it would still take more than a thousand times the lifetime of the universe to check all the arrangements.