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

by

Simon Singh

Synopsis

In 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.

Sort review

Praise for Fermat's Enigma by Simon Singh:"Vividly recounted...I strongly recommend this book to anyone wishing to catch a glimpse of what is one of the most important and ill-understood, but oldest, cultural activities of humanity...an excellent and very worthwhile account of one of the most dramatic and moving events of the century."--Roger Penrose, The New York Times Book Review"How great a riddle was Fermat's 'last theorem'? The exploration of space, the splitting of the atom, the discovery of DNA--unthinkable in Fermat's time--all were achieved while his Pythagorean proof still remained elusive...Though [Singh] may not ask us to bring too much algebra to the table, he does expect us to appreciate a good detective story."--The Boston Sunday Globe"It is hard to imagine a more informative or gripping account of...this centuries-long drama of ingenious failures, crushed hopes, fatal duels, and suicides."--The Wall Street Journal"[Singh] writes with graceful knowledgeability of the esoteric and esthetic appeal of mathematics through the ages, and especially of the mystifying behavior of numbers."--The New York Times"[Singh] has done an admirable job with an extremely difficult subject. He has also done mathematics a great service by conveying the passion and drama that have carried Fermat's Last Theorem aloft as the most celebrated mathematics problem of the last four centuries."--American Mathematical Society"The amazing achievement of Singh's book is that it actually makes the logic of the modern proof understandable to the nonspecialist...More important, Singh shows why it is significant that this problem should have been solved."--The Christian Science MonitorPeople 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 Littleton--This text refers to an out of print or unavailable edition of this title.From the Inside FlapCodes have decided the fates of empires, countries, and monarchies throughout recorded history. Mary, Queen of Scots was put to death by her cousin, Queen Elizabeth, for the high crime of treason after spymaster Sir Francis Walsingham cracked the secret code she used to communicate with her conspirators. And thus the course of British history was altered by a few sheets of cryptic prose. This is just one link in humankind's evolutionary chain of secret communication, and just one of the fascinating incidents recounted in The Code Book, written by bestselling author Simon Singh.Combining a superb storyteller's sense of drama and a scientist's appreciation for technical perfection, Singh traces the evolution of secret writing from ancient Greek military espionage to the frontiers of computer science. The result is an epic tale of human ingenuity, with examples that range from the poignant to the peculiar to the world-historical.There is the case of the Beale ciphers, which involves Wild West escapades, a cowboy who amassed a vast fortune, a buried treasure worth $20 million, and a mysterious set of encrypted papers describing its whereabouts--papers that have baffled generations of cryptanalysts and captivated hundreds of treasure hunters.A speedier end to a bloody war was the only reward that could be promised to the Allied code breakers of World Wars I and II, whose selfless contributions altered the course of history; but few of them lived to receive any credit for their top-secret accomplishments. Among the most moving of these stories is that of the World War II British code breaker Alan Turing, who gave up a brilliant career in mathematics to devote himself to the Allied cause, only to end his years punished by the state for his homosexuality, while his heroism was ignored. No less heroic were the Navajo code talkers, who volunteered without hesitation to risk their lives for the Allied forces in the Japanese theater, where they were routinely mistaken for the enemy.Interspersed with these gripping stories are clear mathematical, linguistic, and technological demonstrations of codes, as well as illustrations of the remarkable personalities--many courageous, some villainous, and all

obsessive--who wrote and broke them.All roads lead to the present day, in which the possibility of a truly unbreakable code looms large. Singh explores this possibility, and the ramifications of our increasing need for privacy, even as it begins to chafe against the stated mission of the powerful and deeply secretive National Security Agency. Entertaining, compelling, and remarkably far-reaching, this is a book that will forever alter your view of history, what drives it, and how private that e-mail you just sent really is.Included in the book is a worldwide Cipher Challenge--a $15,000 award will be given by the author to the first reader who cracks the code successfully. Progress toward the solution will be tracked on The Code Book website. --This text refers to an out of print or unavailable edition of this title.From Scientific AmericanThe ancient battle between people who want to preserve secrets and people who want to discover them proceeds as a form of evolution. Codemakers devise a better means of encryption; codebreakers solve it, forcing the encoders to find another improvement. Singh, trained in physics but now an author of works on science, spins an absorbing tale of codemaking and codebreaking over the centuries. Does the simple monoalphabetic substitution cipher, which replaces each letter of a message with a letter from a cipher alphabet, no longer suffice? Replace it with a code using two or more cipher alphabets. When that no longer outwits the cryptanalysts, encode with a Vigenère square, in which a plaintext alphabet is followed by 26 cipher alphabets. And so on through one-time pad ciphers, cryptographic machines and public-key cryptography.Singh explains them all deftly. Looking to the future, he sees "one idea in particular that might enable cryptanalysts to break all today's ciphers." It is the quantum computer. If it can be built, "it would be able to perform calculations with such enormous speed that it would make a modern supercomputer look like a broken abacus." Or perhaps the cryptographers will triumph with quantum cryptography. "If quantum cryptography systems can be engineered to operate over long distances, the evolution of ciphers will stop. The quest for privacy will have come to an end."--This text refers to an out of print or unavailable edition of this title.From the Back CoverPraise for Fermat's Enigma by Simon Singh:"Vividly recounted...I strongly recommend this book to anyone wishingto catch a glimpse of what is one of the most important andill-understood, but oldest, cultural activities of humanity...anexcellent and very worthwhile account of one of the most dramatic andmoving events of the century."--Roger Penrose, The New York Times Book Review"How great a riddle was Fermat's 'last theorem'? The exploration ofspace, the splitting of the atom, the discovery of DNA--unthinkable inFermat's time--all were achieved while his Pythagorean proof stillremained elusive...Though [Singh] may not ask us to bring too muchalgebra to the table, he does expect us to appreciate a good detectivestory."--The Boston Sunday Globe"It is hard to imagine a more informative or gripping accountof...this centuries-long drama of ingenious failures, crushed hopes,fatal duels, and suicides." --The Wall Street Journal"[Singh] writes with graceful knowledgeability of the esoteric andesthetic appeal of mathematics through the ages, and especially of themystifying behavior of numbers." --The New York Times"[Singh] has done an admirable job with an extremely difficultsubject. He has also done mathematics a great service by conveying thepassion and

drama that have carried Fermat's Last Theorem aloft as themost celebrated mathematics problem of the last four centuries."--American Mathematical Society"The amazing achievement of Singh's book is that it actually makes thelogic of the modern proof understandable to the nonspecialist...Moreimportant, Singh shows why it is significant that this problem shouldhave been solved." --The Christian Science Monitor--This text refers to an out of print or unavailable edition of this title.From BooklistFor millennia, secret writing was the domain of spies, diplomats, and generals; with the advent of the Internet, it has become the concern of the public and businesses. One cyber-libertarian responded with the freeware encryption program Pretty Good Privacy (PGP), and Singh similarly meets a sharpening public curiosity about how codes work. His first popular foray into a mathematical topic, Fermat's Last Theorem (1997), nicely balanced technical detail with vibrant storytelling, a quality happily present again here. Although the quantum-mechanical encryption with which Singh culminates his narrative is challengingly arcane to most except for the math spooks at the National Security Agency, Singh successfully conveys its essential principles, as he does those of all major ciphering schemes. Beginning with such simple ideas as monoalphabetic substitution, which can protect the communications of a boy's treehouse club but not much more, Singh underscores with stories how codemakers and codebreakers have battled each other throughout history. A tool called frequency analysis easily defeats the monoalphabetic cipher, and encryptors over time have added the Vigenere square, cipher disks, one-time pads, and public-key cryptography that underlies PGP. But each security strategy, Singh explains, contains some vulnerability that the clever code cracker can exploit, an opaque process the author splendidly illuminates. Instances of successful decipherment, as of Egyptian hieroglyphics or the German Enigma cipher system in World War II, combine with Singh's sketches of the mathematicians who have advanced the art of secrecy, from Julius Caesar to Alan Turing to contemporary mathematicians, resulting in a wonderfully understandable survey. Gilbert Taylor --This text refers to an out of print or unavailable edition of this title.About the AuthorSimon Singh received his Ph.D. in physics from the University of Cambridge. A former BBC producer, he directed an award-winning documentary film on Fermat's Last Theorem that aired on PBS's "Nova" series, and wrote the bestselling book Fermat's Enigma. He lives in London, England. --This text refers to an out of print or unavailable edition of this title.From Publishers WeeklyIn an enthralling tour de force of popular explication, Singh, author of the bestselling Fermat's Enigma, explores the impact of cryptographyAthe creation and cracking of coded messagesAon history and society. Some of his examples are familiar, notably the Allies' decryption of the Nazis' Enigma machine during WWII; less well-known is the crucial role of Queen Elizabeth's code breakers in deciphering Mary, Queen of Scots' incriminating missives to her fellow conspirators plotting to assassinate Elizabeth, which led to Mary's beheading in 1587. Singh celebrates a group of unsung heroes of WWII, the Navajo "code talkers," Native American Marine radio operators who, using a coded version of their native language, played a vital role in defeating the Japanese in the Pacific. He also elucidates the intimate links between codes or ciphers and the development of the telegraph,

radio, computers and the Internet. As he ranges from Julius Caesar's secret military writing to coded diplomatic messages in feuding Renaissance Italy city-states, from the decipherment of the Rosetta Stone to the ingenuity of modern security experts battling cyber-criminals and cyber-terrorists, Singh clarifies the techniques and tricks of code makers and code breakers alike. He lightens the sometimes technical load with photos, political cartoons, charts, code grids and reproductions of historic documents. He closes with a fascinating look at cryptanalysts' planned and futuristic tools, including the "one-time pad," a seemingly unbreakable form of encryption. In Singh's expert hands, cryptography decodes as an awe-inspiring and mind-expanding story of scientific breakthrough and high drama. Agent, Patrick Walsh. (Oct.) FYI: The book includes a "Cipher Challenge," offering a $15,000 reward to the first person to crack that code.Copyright 1999 Reed Business Information, Inc. --This text refers to an out of print or unavailable edition of this title.Excerpt. © Reprinted by permission. All rights reserved.On 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... --This text refers to an out of print or unavailable edition of this title.From Library JournalSingh, Cambridge-educated physicist, has written a provocative study of code, the way in which humans hide the inherent meanings of messages by substituting words and or characters in a text. Author of the popular Fermat's Enigma, he broadly portrays the evolution of cryptography throughout the centuries. In essence, efforts of those wishing for secrecy and others who attempt to break it is a story of intrigue of the highest form. Employing a smooth narrative style, Singh tells of secrecy, fascinating events, and people, starting with Mary Queen of Scots and ending with recent attempts by quantum theorists to construct an unbreakable code. This is the history of technology at its best and serves as an excellent addition to David Kahn's mammoth work on cryptography, The Codebreakers (Scribner, 1996). Highly recommended for all public and academic libraries.-ADayne Sherman, Southeastern Louisiana Univ., Hammond Copyright 1999 Reed Business Information, Inc. --This text refers to an out of print or unavailable edition of this title.Read more

What people say about this book

George, “For people that enjoy the history and science genres. For people that enjoy the history and science genres, this is the perfect book. You get a balance of the history of ciphers and encryption over the course of human history while also learning about the technical details of how ciphers and encryption work (and how they are broken). The Code Book is extremely well written and after finishing it you really do feel like you learned something.Some other great aspects of this book are a Cipher Challenge at the end which allows you to test your codebreaking skills as well as multiple appendices for those who want to go even deeper into the technical areas of ciphers and encryption.My only complaint about this book is that it's aging. It was written in 1999, and the world of computing has changed a lot from 1999-2018. But don't let this fact deter you from reading The Code Book. The historical cipher/encryption knowledge that you learn about in the World Wars and the dawn of computing are very interesting. Even if you only want to focus on the modern aspects of encryption, I still recommend reading this book and then picking up something more modern after.”

D. Engel, “Best Book I've Ever Read. I am only half-way through this book but I find this book absolutely fascinating! Not only can you learn about cryptography but you get some very interesting history lessons. Of course these lessons apply to cryptography, which is one of the fascinating parts of this book. History as we know it, was hugely impacted by cryptography.This book doesn't read like most text books we find boring and mundane. I read it as if I was reading a fiction novel, which really helps with the comprehension of the topics presented. Ciphers and Codes presented in the book are explained very clearly, I'd almost dare say near perfectly. There are appendices mentioned where you can study items in further detail (in the back of the book).This book, in my opinion, offers a rock solid foundation for those new to cryptology and can reinforce concepts for those that are well experienced.I highly recommend this book, if you interested in cryptography, history, or science.”

frogman, “The Code Book--Masterpiece of Historical Significance & Present Secure Communications Quandaries.. From describing very descriptive ancient codes to the fascinating world of quantum computing this author touches on it all with very well illustrated examples to help clarify a very difficult and highly complex subject of cryptanalysis--- with its modern employment of linguists, mathematicians, and computer engineers. It's an ongoing quest to keep our PRIVACY from intrusions of all sources such as governments, business competitors, or prying eyes. There are many privacy issues that both governments and private citizens alike must face in today's technological world. These questions are posed and answered in many ways within the book. One caveat---recalling what our esteemed Statesman Benjamin Franklin once expressed---"Any one who will trade freedom for security deserves neither" The quandary is how government protects its citizens from acts of terror or how citizens may be protected by a

tyrannical government--read this bookSimon Singh has produced a manuscript that not only gives one a deeper insight into the world of cryptanalysis from a historical prospective but also the men and women involved in this complex field of science through out the ages,----the brilliant people from various and varied walks of life who have contributed immensely to this science past and present . It covers the humanist aspect from those involved with their various idiosyncrasies of behavior from the selling of data to foreign powers as well as personal behavior that could cause one to be blackmailed by enemies. This book is a can of worms in many respects since it opens up to the reader a world fraught with possible invasion of privacy -one of the most fundamental rights we should all hold dear--especially in America--and what avenues we have at our disposal to solve these dilemmas.The writing style Simon uses to explain the complex theories and problems that code breakers or code makers must use is exemplary and easily understood for the average layman--although he helps to have some advanced understanding of the sciences ---but it is not necessary in comprehending what the author conveys in this book.I found the Appendix in the rear especially helpful in my study of the very basic science of cryptanalysis as well as his simple examples on how it all pieces together to form the whole picture.Even though this book was written in 1999--- for those of us who are concerned about CURRENT EVENTS in this science the last chapter offers deeper insights and may be used as a springboard to investigate further developments of cryptanalysis and how we may apply it to our everyday life of sending emails, buying merchandize or researching various subjects. While the wide world of the internet has opened our vast horizons to knowledge and communications within a multitude of domains ---rest assure there is an army of cryptanalyst struggling to keep our messages and correspondence secure daily---or at least we HOPE THERE IS--or we may involve ourselves with political action to ensure our freedom of privacy?"

Petra Bryce, "A remarkable achievement. Simon Singh provides the reader with an overview of the history of cryptology and brings to the reader's attention events in history that would probably have had different outcomes had it not been for the achievements of some historical figures - mostly unknown to us today - like Thomas Phelippes who deciphered and forged an encrypted message to Mary, Queen of Scots, thereby forcing her to effectively sign her own death warrant, and Marian Rejewski who provided the groundwork on deciphering the Enigma machine before handing his research over to the British; his enthusiasm for the subject shines through at every page. He also aims to set the record straight for a few unsung heroes, mainly from recent history who, due to the secrecy act, were forbidden from publicly claiming credit for their work in cryptology at the time. Most notably amongst them is Alan Turing who helped crack the Enigma cipher, but also Tommy Flowers who single-handedly built Colossus, the precursor to the modern digital computer but who had to destroy the blueprints after the war, as well as Clifford Cocks and Malcolm Williamson who invented the asymmetric cipher and public-key cryptography four years before the Americans but were sworn to secrecy. I also enjoyed his brief foray into the decipherment of ancient texts like the Egyptian hieroglyphics and the Minoan

script of Linear B, but Simon Singh's main achievement lies in his ability to bring across such tricky issues like key distribution, public-key cryptography and quantum cryptography in a simple and lucid manner to a mainly non-technically minded person like me. My only criticism and one that has got nothing to do with the author, is the fact that this book was written more than ten years ago when e-commerce was still in its infancy; since then the world has seen a massive leap in terms of financial transactions being conducted over the internet and even seen the arrival of internet banking and with it the need for ever better security for the individual and companies trading over the internet. I would be most interested to read a topical update in which he covers the last ten years and the impact this has had on cryptography."

dtanderson, "Don't miss this book! Totally incredible how encryption has evolved over the centuries - millenium, even. I was reading about cryptography somewhere and it recommended this book, which I subsequently purchased. Absolutely unputdownable! Cryptography and codes have been around for thousands of years, and you can follow the progression from the simplest, to a brief introduction of the totally unbreakable quantum encryption. Mary Queen of Scots plotted to kill Queen Elizabeth by sending coded messages to her accomplices. However, the Queen's code breakers could decipher everything she wrote and condemned Mary to death. Just one of the Amazon facts you will read in this book."

Lobotomised and despised, "Almost perfect.. Almost perfect for a layman's introductory book on cryptography/ cryptanalysis. 5 stars for all the historical introduction from Ceasar Shift, substitution/transposition, frequency analysis and linguistics, monoalphabets, polyalphabets, Vigenere and Babbage, Turing and the naval Enigma, but minus 0.5-1 stars because modern encryption/decryption techniques were a little rushed relative to the earlier historical half of the book and some applications were hardly mentioned. Interesting that Linear A and Etruscan had not been deciphered at the time this book was written.Although I bought this book late, and technology has advanced since it was written, I was hoping to better understand encryption in the fields of computer science and technology (authentication and certificates on the internet, hashing of passwords, credit card technology...). There was a good intro on RSA and PGP, and I enjoyed the ending on photon traps and quantum computing. I wish there had been a little more on number theory (primes), a comparison of the many modern standards, the use of analysis in digital forensics, ...something a little more technical but maybe there are other books for that.There are some dubious claims in the book that GCHQ invented asymetric public-key encryption 'before' Diffie-Hellman-Merkle and Rivest-Shamir-Aldeman. The claim being made is that GCHQ invented it shortly before (whatever they say, right?), but could not disclose their invention for reasons of national security. I realise that this story was put out in 1997 by GCHQ and not Simon Singh, but where is the evidence?What is more likely is that there were reasons of national security for not disclosing that, despite the huge budgets, the shadowy cold-war era monoliths GCHQ (and NSA) were totally outwitted by a handful of freedom loving academics like

Whitfield Diffie, who saw this technology as a means of protecting free speech and, therefore, democracy.Kudos to Simon Singh for stating his suppor for the use of Zimmermann's PGP in the book.The book concludes with a multiple stages code cracking challenge, which starts very easy and gets harder (there was a cash prize at the time)."

C.L, "Great book if you have any interest in encryption.. Great book if you have any interest in encryption. Covers from the early days of hiding messages by writing them on someones bald head before allowing the hair to grow all the way to the engima machine in world war 2. Book isnt too heavy for those who are not mathamaticians but explains modern encryption topics in an easily accessable way. Highly recommend it."

PeteMat, "A cracking read.... Having previously worked with encryption systems, I first read this book many years ago in order to get a better understanding of the underpinning principles of cryptography. As others have already conveyed, Simom Singh produced a very approachable book which neatly balanced the tasks of providing enough technical explanation of a very complex subject while avoiding the trap of overwhelming more 'casual' readers. Highly recommended!"

DMCA