The Codebreakers The Comprehensive History Of Secret Communication From Ancient Times To The Internet

The CodebreakersThe Comprehensive History of Secret Communication from Ancient Times to the InternetSimon and Schuster

During the 1920s Herbert O. Yardley was chief of the first peacetime cryptanalytic organization in the United States, the ancestor of today's National Security Agency. Funded by the U.S. Army and the Department of State and working out of New York, his small and highly secret unit succeeded in breaking the diplomatic codes of several nations, including Japan. The decrypts played a critical role in U.S. diplomacy. Despite its extraordinary successes, the Black Chamber, as it came to known, was disbanded in 1929. President Hoover's new Secretary of State Henry L. Stimson refused to continue its funding with the now-famous comment, "Gentlemen do not read other people's mail." In 1931 a disappointed Yardley caused a sensation when he published this book and revealed to the world exactly what his agency had done with the secret and illegal cooperation of nearly the entire American cable industry. These revelations and Yardley's right to publish them set into motion a conflict that continues to this day: the right to freedom of expression versus national security. In addition to offering an expose on post-World War I cryptology, the book is filled with exciting stories and personalities.

Cipher and decipher codes: transposition and polyalphabetical ciphers, famous codes, typewriter and telephone codes, codes that use playing cards, knots, and swizzle sticks . . . even invisible writing and sending messages through space. 45 diagrams.

During and after the English civil wars, between 1640 and 1690, an unprecedented number of manuals teaching cryptography were published, almost all for the general public. While there are many surveys of cryptography, none pay any attention to the volume of manuals that appeared during the seventeenth century, or provide any cultural context for the appearance, design, or significance of the genre during the period. On the contrary, when the period’s cryptography writings are mentioned, they are dismissed as esoteric, impractical, and useless. Yet, as this book demonstrates, seventeenth-century cryptography manuals show us one clear beginning of the capitalization of information. In their pages, intelligence—as private message and as mental ability—becomes a central commodity in the emergence of England’s capitalist media state. Publications boasting the disclosure of secrets had long been popular, particularly for English readers with interests in the occult, but it was during these particular decades of the seventeenth century that cryptography emerged as a permanent bureaucratic function for the English government, a fashionable activity for the stylish English reader, and a respected discipline worthy of its own genre. These manuals

established cryptography as a primer for intelligence, a craft able to identify and test particular mental abilities deemed "smart" and useful for England's financial future. Through close readings of five specific primary texts that have been ignored not only in cryptography scholarship but also in early modern literary, scientific, and historical studies, this book allows us to see one origin of disciplinary division in the popular imagination and in the university, when particular broad fields—the sciences, the mechanical arts, and the liberal arts—came to be viewed as more or less profitable.

A collection of articles and monographs on cryptography ranges from a technical study of the spy cipher used by Reino Hayhanen to an argument against a government-sponsored computer cryptosystem

Spies, secret messages, and military intelligence have fascinated readers for centuries but never more than today, when terrorists threaten America and society depends so heavily on communications. Much of what was known about communications intelligence came first from David Kahn's pathbreaking book, The Codebreakers. Kahn, considered the dean of intelligence historians, is also the author of Hitler's Spies: German Military Intelligence in World War II and Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943, among other books and articles. Kahn's latest book, How I Discovered World War II's Greatest Spy and Other Stories of Intelligence and Code, provides insights into the dark realm of intelligence and code that will fascinate cryptologists, intelligence personnel, and the millions interested in military history, espionage, and global affairs. It opens with Kahn telling how he discovered the identity of the man who sold key information about Germany's Enigma machine during World War II that enabled Polish and then British codebreakers to read secret messages. Next Kahn addresses the question often asked about Pearl Harbor: since we were breaking Japan's codes, did President Roosevelt know that Japan was going to attack and let it happen to bring a reluctant nation into the war? Kahn looks into why Nazi Germany's totalitarian intelligence was so poor, offers a theory of intelligence, explicates what Clausewitz said about intelligence, tells—on the basis of an interview with a head of Soviet codebreaking—something about Soviet Comint in the Cold War, and reveals how the Allies suppressed the second greatest secret of WWII. Providing an inside look into the efforts to gather and exploit intelligence during the past century, this book presents powerful ideas that can help guide present and future intelligence efforts. Though stories of WWII spying and codebreaking may seem worlds apart from social media security, computer viruses, and Internet surveillance, this book offers timeless lessons that may help today's leaders avoid making the same mistakes that have helped bring at least one global power to its knees. The book includes a Foreword written by Bruce Schneier.

This accessible textbook presents a fascinating review of cryptography and cryptanalysis across history. The text relates the earliest use of the monoalphabetic cipher in the ancient world, the development of the

“unbreakable” Vigenère cipher, and an account of how cryptology entered the arsenal of military intelligence during the American Revolutionary War. Moving on to the American Civil War, the book explains how the Union solved the Vigenère ciphers used by the Confederates, before investigating the development of cipher machines throughout World War I and II. This is then followed by an exploration of cryptology in the computer age, from public-key cryptography and web security, to criminal cyber-attacks and cyber-warfare. Looking to the future, the role of cryptography in the Internet of Things is also discussed, along with the potential impact of quantum computing. Topics and features: presents a history of cryptology from ancient Rome to the present day, with a focus on cryptology in the 20th and 21st centuries; reviews the different types of cryptographic algorithms used to create secret messages, and the various methods for breaking such secret messages; provides engaging examples throughout the book illustrating the use of cryptographic algorithms in different historical periods; describes the notable contributions to cryptology of Herbert Yardley, William and Elizebeth Smith Friedman, Lester Hill, Agnes Meyer Driscoll, and Claude Shannon; concludes with a review of tantalizing unsolved mysteries in cryptology, such as the Voynich Manuscript, the Beale Ciphers, and the Kryptos sculpture. This engaging work is ideal as both a primary text for courses on the history of cryptology, and as a supplementary text for advanced undergraduate courses on computer security. No prior background in mathematics is assumed, beyond what would be encountered in an introductory course on discrete mathematics. Spy on spies--uncover the secret agents of World War 2. Discover World War 2's hidden heroes and villains. Spies, Code Breakers, and Secret Agents explores the intriguing world of spycraft and shows you what goes on behind the scenes in war. From spy schools and ciphers to sneaky tools and secret armies, this guide takes you on a declassified tour of the undercover operations that helped decide the outcome of World War 2. There's also more than a dozen short spy-ographies that cover some of the most famous (and infamous!) agents that were active during the war. This World War 2 book for kids includes: Fun for aspiring historians--Dig into the causes of and what led up to World War 2 so you can better understand the important part spies played in it. A family-friendly exploration--Learn about history in a fun and accessible way that anyone can enjoy. Covert illustrations--Get an up-close look at actual spies, as well as some seriously amazing spy gear. Amaze your friends and family with all kinds of awesome facts about spies and secret agents from World War 2.

"As gripping as a good thriller." --The Washington Post Unpack the science of secrecy and discover the methods behind cryptography--the encoding and decoding of information--in this clear and easy-to-understand young adult adaptation of the national bestseller that's perfect for this age of WikiLeaks, the Sony hack, and other events that reveal the extent to which our technology is never quite as secure as we want to believe. Coders and codebreakers alike will be fascinated by history's most mesmerizing stories of intrigue and cunning--from Julius Caesar and his Caeser cipher to the Allies' use of the Enigma machine to decode German messages during World War II. Accessible, compelling, and timely, The Code Book is sure to

make readers see the past--and the future--in a whole new way. "Singh's power of explaining complex ideas is as dazzling as ever." --The Guardian

This edition surveys the entire history of codes through an eloquent narrative and an evocative range of illustrations, paying special attention to famous codes that have never been broken, such as the Beale Ciphers, the Voynich manuscript, the Easter Island code, and many more.

A million pages of new World War II codebreaking records have been released by the U.S. Army and Navy and the British government over the last five years. Now, Battle of Wits presents the history of the war that these documents reveal. From the Battle of Midway until the last German code was broken in January 1945, this is an astonishing epic of a war that was won not simply by brute strength but also by reading the enemy's intentions. The revelations of Stephen Budiansky's dramatic history include how Britain tried to manipulate the American codebreakers and monopolize German Enigma code communications; the first detailed published explanations of how the Japanese codes were broken; and how the American codebreaking machines worked to crack the Japanese, the German, and even the Russian diplomatic codes. This is the story of the Allied codebreakers puzzling through the most difficult codebreaking problems that ever existed. At the same time, the compelling narrative shows the crucial effect codebreaking had on the battle-fields by explaining the urgency of stopping the wolf pack U-boat attacks in the North Atlantic, the burning desire in the United States to turn the tide of the war after Pearl Harbor, the importance of halting Rommel's tanks in North Africa, and the necessity of ensuring that the Germans believed the Allies' audacious deception and cover plans for D-Day. Budiansky brings to life the unsung code-breaking heroes of this secret war: Joseph J. Rochefort, an intense and driven naval officer who ran the codebreaking operation in "The Dungeon", a dank basement at Pearl Harbor, that effectively won the Battle of Midway; Alan Turing, the eccentric father of the computerage, whose brilliant electromechanical calculators broke the German Enigma machine; and Ian Fleming, whose daredevil espionage schemes to recover codebooks resembled the plots of the 007 novels he later wrote. Among the villains, we meet the Nazi Admiral Donitz, who led the submarine wolf packs against Allied shipping in the North Atlantic with horrific casualty rates -- until the codebreakers stopped him. Budiansky, a Harvard-trained mathematician, demonstrates the mathematical insight and creativity of the cryptographers by showing step-by-step precisely how the codes were broken. This technology -- the flow of information, its encryption, and the computational methods of recovering it from the enemy -- had never before been so important to the outcome of a war. Informative diagrams, maps, appendices, and photographs show exactly how, why, and where the secret war was won. Unveiled for the first time, the complete story of codebreaking in World War II has now been told.

"Chilling... To Hell and Back should be required reading in every chancellery, every editorial cockpit and every place where peevish Euroskeptics do their thinking…. Kershaw documents each and every ‘ism’ of his analysis with extraordinary detail and passionate humanism."—The New York Times Book Review The Penguin History of Europe series reaches the twentieth century with acclaimed scholar Ian Kershaw’s long-anticipated analysis of the pivotal years of World War I and World War II. The European catastrophe, the long continuous period from 1914 to 1949, was unprecedented in human history—an extraordinarily dramatic, often traumatic, and endlessly fascinating period of upheaval and transformation. This new volume in the Penguin History of Europe series offers comprehensive coverage of this tumultuous era. Beginning with the outbreak of World War I through the rise of Hitler and the aftermath of the Second World War, award-winning British historian Ian Kershaw combines his characteristic original scholarship and gripping prose as he profiles the key decision makers and the violent shocks of war as they affected the entire European continent and radically altered the course of European history. Kershaw identifies four major causes for this catastrophe: an explosion of ethnic-racist nationalism, bitter and irreconcilable demands for territorial revisionism, acute

class conflict given concrete focus through the Bolshevik Revolution, and a protracted crisis of capitalism. Incisive, brilliantly written, and filled with penetrating insights, To Hell and Back offers an indispensable study of a period in European history whose effects are still being felt today.

A mathematical tour of some of the greatest unsolved ciphers of all time In 1953, a man was found dead from cyanide poisoning near the Philadelphia airport with a picture of a Nazi aircraft in his wallet and an enciphered message taped to his abdomen. In 1912, a book dealer named Wilfrid Voynich came into possession of an illuminated cipher manuscript once belonging to Emperor Rudolf II, who was obsessed with alchemy and the occult. Wartime codebreakers tried—and failed—to unlock the book's secrets, and it remains an enigma to this day. In this lively and entertaining book, Craig Bauer examines these and other vexing ciphers yet to be cracked. Some may reveal the identity of a spy or serial killer, provide the location of buried treasure, or expose a secret society—while others may be elaborate hoaxes. He lays out the evidence surrounding each cipher, describes the efforts to decipher it, and invites readers to try their hand at puzzles that have stymied so many others.

Cryptology, the science of codes and ciphers, has a long history. Although cryptology is usually thought of in relation to spies and intelligence operations, today this discipline is part of our everyday lives, encompassing even the most sophisticated communications technology.

"An absorbing and thoroughly well documented account" of WWII naval intelligence and the Allied hunt for the Nazi code machine known as the Enigma (Warship). From the start of World War II to mid-1943, British and American naval forces fought a desperate battle against German submarine wolfpacks. And the Allies might have lost the struggle at sea without an astounding intelligence coup. Here, the author brings to life the race to break the German U-boat codes. As the Battle of the Atlantic raged, Hitler's U-boats reigned. To combat the growing crisis, ingenious amateurs joined the nucleus of dedicated professionals at Bletchley Park to unlock the continually changing German naval codes. Their mission: to read the U-boat messages of Hitler's cipher device, the Enigma. They first found success with the capture of U-110,—which yielded the Enigma machine itself and a trove of secret documents. Then the weather ship Lauenburg seized near the Arctic ice pack provided code settings for an entire month. Finally, two sailors rescued a German weather cipher that enabled the team at Bletchley to solve the Enigma after a year-long blackout. In "a highly recommended account with a wealth of materials" Seizing the Enigma tells the story of a determined corps of people who helped turn the tide of the war (Naval Historical Foundation).

'The best book on codebreaking I have read', SIR DERMOT TURING 'Brings back the joy I felt when I first read about these things as a kid', PHIL ZIMMERMANN 'This is at last the single book on codebreaking that you must have. If you are not yet addicted to cryptography, this book will get you addicted. Read, enjoy, and test yourself on history's great still-unbroken messages!' JARED DIAMOND is the Pulitzer Prize-winning author of Guns, Germs, and Steel; Collapse; and other international bestsellers 'This is THE book about codebreaking. Very concise, very inclusive and easy to read', ED SCHEIDT 'Riveting', MIKE GODWIN 'Approachable and compelling', GLEN MIRANKER This practical guide to breaking codes and solving cryptograms by two world experts, Elonka Dunin and Klaus Schmeh, describes the most common encryption techniques along with methods to detect and break them. It fills a gap left by outdated or very basic-level books. This guide also covers many unsolved messages. The Zodiac Killer sent four encrypted messages to the police. One was solved; the other three were not. Beatrix Potter's diary and the Voynich Manuscript were both encrypted - to date, only one of the two has been deciphered. The breaking of the so-called Zimmerman Telegram during the First World War changed the course of history. Several encrypted wartime military messages remain unsolved to this day. Tens of thousands of other encrypted messages, ranging from simple notes created by children to encrypted postcards and diaries in

people's attics, are known to exist. Breaking these cryptograms fascinates people all over the world, and often gives people insight into the lives of their ancestors. Geocachers, computer gamers and puzzle fans also require codebreaking skills. This is a book both for the growing number of enthusiasts obsessed with real-world mysteries, and also fans of more challenging puzzle books. Many people are obsessed with trying to solve famous crypto mysteries, including members of the Kryptos community (led by Elonka Dunin) trying to solve a decades-old cryptogram on a sculpture at the centre of CIA Headquarters; readers of the novels of Dan Brown as well as Elonka Dunin's The Mammoth Book of Secret Code Puzzles (UK)/The Mammoth Book of Secret Codes and Cryptograms (US); historians who regularly encounter encrypted documents; perplexed family members who discover an encrypted postcard or diary in an ancestor's effects; law-enforcement agents who are confronted by encrypted messages, which also happens more often than might be supposed; members of the American Cryptogram Association (ACA); geocachers (many caches involve a crypto puzzle); puzzle fans; and computer gamers (many games feature encryption puzzles). The book's focus is very much on breaking pencil-and-paper, or manual, encryption methods. Its focus is also largely on historical encryption. Although manual encryption has lost much of its importance due to computer technology, many people are still interested in deciphering messages of this kind.

Thorough, systematic introduction to serious cryptography, especially strong in modern forms of cipher solution used by experts. Simple and advanced methods. 166 specimens to solve — with solutions.

'Turing writes on codebreaking with understandable authority and compelling panache.' - Michael Smith, bestselling author of Station X. At Bletchley Park, some of Britain's most talented mathematicians, linguists, and intellectuals were assembled to break Nazi codes. Kept secret for nearly thirty years, we have now come to realise the crucial role that these codebreakers played in the Allied victory in World War II. Written by Dermot Turing - the nephew of famous codebreaker Alan Turing - this illustrated account provides unique insight into the behind-the-scenes action at Bletchley Park. Discover how brilliant and eccentric individuals such as Dilly Knox, Alan Turing and Joan Clarke were recruited, the social life that grew up around the park, and how they dealt with the ever-present burden of secrecy. Including a foreword by Professor Christopher Andrew of Cambridge University, author of MI5's official history The Secret World, this book brings to life the stories of the men and women who toiled day and night to crack the seemingly unbreakable enigma code.

How did the British codebreakers succeed in cracking the apparently unbreakable Enigma code during the Second World War? Was it their gifted amateurism? The brilliance of Alan Turing? The invention of the very first computers? Or the pioneering work of Polish cryptographers? It was all of the above. But there is one other crucial factor, which is much less well known. The same team had done it before. The truth is that many of those most closely involved in cracking the Enigma code - Alistair Denniston, Frank Birch, Dilly Knox - had wrestled with German naval codes for most of the First World War. By the end of the war they had been successfully cracking a new code every day, from their secret Room 40 at the Old Admiralty Building, in a London blacked out for Zeppelin Raids. The techniques they developed then, the ideas that they came to

rely on, the people they came to trust, had been developed the hard way, under intense pressure and absolute secrecy during World War I. Before Enigma tells their story and explains how they managed to crack the supposedly indecipherable code. The book outlines the capture of the Magdeburg and the Hobart, discusses the use of cracked codes to bring German fleets to battle at Dogger Bank and Jutland, and focuses on individuals such as Winston Churchill and Admiral Sir Reginald 'Blinker' Hall and their importance in the development of a British naval code tradition.

“What would it be like to keep a secret for fifty years? Never telling your parents, your children, or even your husband?” Codebreaker Girls: A Secret Life at Bletchley Park tells the true story of Daisy Lawrence. Following extensive research, the author uses snippets of information, unpublished photographs and her own recollections to describe scenes from her mother’s poor, but happy, upbringing in London, and the disruptions caused by the outbreak of the Second World War to a young woman in the prime of her life. The author asks why, and how, Daisy was chosen to work at the Government war station, as well as the clandestine operation she experienced with others, deep in the British countryside, during a time when the effects of the war were felt by everyone. In addition, the author examines her mother's personal emotions and relationships as she searches for her young fiancée, who was missing in action overseas. The three years at Bletchley Park were Daisy's university, but having closed the door in 1945 on her hidden role of national importance — dealing with Germany, Italy and Japan — this significant period in her life was camouflaged for decades in the filing cabinet of her mind. Now her story comes alive with descriptions, original letters, documents, newspaper cuttings and unique photographs, together with a rare and powerful account of what happened to her after the war.

The first comprehensive history of secret communication from ancient times to the threshold of outer space.

With exclusive interviews, a Signal Corps veteran tells the full story of how cryptography helped defeat the Axis powers, at Bletchley Park and beyond. For years, the story of the World War II codebreakers was kept a crucial state secret. Even Winston Churchill, himself a great advocate of Britain’s cryptologic program, purposefully minimized their achievements in his history books. Now, though, after decades have passed, the true scope of the British and American cryptographers’ role in the war has come to light. It was a role key to the Allied victory. From the Battle of Britain to the Pacific front to the panzer divisions in Africa, superior cryptography gave the Allies a decisive advantage over the Axis generals. Military intelligence made a significant difference in battle after battle. In Codebreakers’ Victory, veteran cryptographer Hervie Haufler takes readers behind the scenes in this fascinating underground world of ciphers and decoders. This broad view represents the first comprehensive account of codebreaking during World War II. Haufler pulls together years of research, exclusive access to top secret files, and personal interviews to craft a captivating must-read for

anyone interested in the behind-the-front intellect and perseverance that went into beating the Nazis and Japan.

The magnificent, unrivaled history of codes and ciphers -- how they're made, how they're broken, and the many and fascinating roles they've played since the dawn of civilization in war, business, diplomacy, and espionage -- updated with a new chapter on computer cryptography and the Ultra secret. Man has created codes to keep secrets and has broken codes to learn those secrets since the time of the Pharaohs. For 4,000 years, fierce battles have been waged between codemakers and codebreakers, and the story of these battles is civilization's secret history, the hidden account of how wars were won and lost, diplomatic intrigues foiled, business secrets stolen, governments ruined, computers hacked. From the XYZ Affair to the Dreyfus Affair, from the Gallic War to the Persian Gulf, from Druidic runes and the kaballah to outer space, from the Zimmermann telegram to Enigma to the Manhattan Project, codebreaking has shaped the course of human events to an extent beyond any easy reckoning. Once a government monopoly, cryptology today touches everybody. It secures the Internet, keeps e-mail private, maintains the integrity of cash machine transactions, and scrambles TV signals on unpaid-for channels. David Kahn's The Codebreakers takes the measure of what codes and codebreaking have meant in human history in a single comprehensive account, astonishing in its scope and enthralling in its execution. Hailed upon first publication as a book likely to become the definitive work of its kind, The Codebreakers has more than lived up to that prediction: it remains unsurpassed. With a brilliant new chapter that makes use of previously classified documents to bring the book thoroughly up to date, and to explore the myriad ways computer codes and their hackers are changing all of our lives, The Codebreakers is the skeleton key to a thousand thrilling true stories of intrigue, mystery, and adventure. It is a masterpiece of the historian's art.

The bestselling author of Leonardo da Vinci and Steve Jobs returns with a gripping account of how Nobel Prize winner Jennifer Doudna and her colleagues launched a revolution that will allow us to cure diseases, fend off viruses, and have healthier babies. When Jennifer Doudna was in sixth grade, she came home one day to find that her dad had left a paperback titled The Double Helix on her bed. She put it aside, thinking it was one of those detective tales she loved. When she read it on a rainy Saturday, she discovered she was right, in a way. As she sped through the pages, she became enthralled by the intense drama behind the competition to discover the code of life. Even though her high school counselor told her girls didn’t become scientists, she decided she would. Driven by a passion to understand how nature works and to turn discoveries into inventions, she would help to make what the book’s author, James Watson, told her was the most important biological advance since his co-discovery of the structure of DNA. She and her collaborators turned ?a curiosity ?of nature into an invention that will transform the human race: an easy-to-use tool that can edit DNA. Known as CRISPR, it opened a brave new world of medical miracles and

moral questions. The development of CRISPR and the race to create vaccines for coronavirus will hasten our transition to the next great innovation revolution. The past half-century has been a digital age, based on the microchip, computer, and internet. Now we are entering a life-science revolution. Children who study digital coding will be joined by those who study genetic code. Should we use our new evolution-hacking powers to make us less susceptible to viruses? What a wonderful boon that would be! And what about preventing depression? Hmmm…Should we allow parents, if they can afford it, to enhance the height or muscles or IQ of their kids? After helping to discover CRISPR, Doudna became a leader in wrestling with these moral issues and, with her collaborator Emmanuelle Charpentier, won the Nobel Prize in 2020. Her story is a thrilling detective tale that involves the most profound wonders of nature, from the origins of life to the future of our species.

The award-winning New York Times bestseller about the American women who secretly served as codebreakers during World War II--a "prodigiously researched and engrossing" (New York Times) book that "shines a light on a hidden chapter of American history" (Denver Post). Recruited by the U.S. Army and Navy from small towns and elite colleges, more than ten thousand women served as codebreakers during World War II. While their brothers and boyfriends took up arms, these women moved to Washington and learned the meticulous work of code-breaking. Their efforts shortened the war, saved countless lives, and gave them access to careers previously denied to them. A strict vow of secrecy nearly erased their efforts from history; now, through dazzling research and interviews with surviving code girls, bestselling author Liza Mundy brings to life this riveting and vital story of American courage, service, and scientific accomplishment.

The huge success of Sinclair's The Secret Life of Bletchley Park – a quarter of a million copies sold to date – has been symptomatic of a similarly dramatic increase in visitors to Bletchley Park itself, the Victorian mansion in Buckinghamshire now open as an engrossing museum of wartime codebreaking. Aurum is publishing the first comprehensive illustrated history of this remarkable place, from its prewar heyday as a country estate under the Liberal MP Sir Herbert Leon, through its wartime requisition with the addition of the famous huts within the grounds, from the place where modern computing was invented and the German Enigma code was cracked, to its post-war dereliction and then rescue towards the end of the twentieth century as a museum whose visitor numbers have more than doubled in the last five years. Featuring over 200 photographs, some previously unseen, and text by Sinclair McKay, this will be an essential purchase for everyone interested in the place where codebreaking helped to win the war.

When Richard Hayes, a gifted polymath and cryptographer, was drafted by Irish intelligence services to track the movements of a prolific Nazi spy, Hermann Görtz, it set in motion one of the most remarkable episodes in Irish history. What followed was a high-stakes game of cat and mouse that would wind its way

through the capital and its suburbs, reverberate through the corridors of power, test the sympathies of those in high society, and even expand to jeopardise the Allied war effort. Codebreaker is a riveting and deeply researched account of an extraordinary period of history – when Dublin became a hotbed of Nazi intrigue and the fate of an independent Ireland settled on the shoulders of an unassuming employee of the National Library.

The story of Bletchley Park, the successful intelligence operation that cracked Germany's Enigma Code. Photos.

A TV tie-in edition of The Code Book filmed as a prime-time five-part Channel 4 series on the history of codes and code-breaking and presented by the author. This book, which accompanies the major Channel 4 series, brings to life the hidden history of codes and code breaking. Since the birth of writing, there has also been the need for secrecy. The story of codes is the story of the brilliant men and women who used mathematics, linguistics, machines, computers, gut instinct, logic and detective work to encrypt and break these secrect messages and the effect their work has had on history.

The first edition of this award-winning book attracted a wide audience. This second edition is both a joy to read and a useful classroom tool. Unlike traditional textbooks, it requires no mathematical prerequisites and can be read around the mathematics presented. If used as a textbook, the mathematics can be prioritized, with a book both students and instructors will enjoy reading. Secret History: The Story of Cryptology, Second Edition incorporates new material concerning various eras in the long history of cryptology. Much has happened concerning the political aspects of cryptology since the first edition appeared. The still unfolding story is updated here. The first edition of this book contained chapters devoted to the cracking of German and Japanese systems during World War II. Now the other side of this cipher war is also told, that is, how the United States was able to come up with systems that were never broken. The text is in two parts. Part I presents classic cryptology from ancient times through World War II. Part II examines modern computer cryptology. With numerous real-world examples and extensive references, the author skillfully balances the history with mathematical details, providing readers with a sound foundation in this dynamic field. FEATURES Presents a chronological development of key concepts Includes the Vigenère cipher, the one-time pad, transposition ciphers, Jefferson’s wheel cipher, Playfair cipher, ADFGX, matrix encryption, Enigma, Purple, and other classic methods Looks at the work of Claude Shannon, the origin of the National Security Agency, elliptic curve cryptography, the Data Encryption Standard, the Advanced Encryption Standard, public-key cryptography, and many other topics New chapters detail SIGABA and SIGSALY, successful systems used during World War II for text and speech, respectively Includes quantum cryptography and the impact of quantum computers

This is the first biography of Capt. Joe Rochefort, the Officer in Charge of Station Hypo the U.S. Navy’s decrypt unit at Pearl Harbor and his key role in breaking

the Imperial Japanese Navy's main code before the Battle of Midway. It brings together the disparate threads of Rochefort's life and career, beginning with his enlistment in the Naval Reserve in 1918 at age 17 (dropping out of high school and adding a year to his age). It chronicles his earliest days as a mustang (an officer who has risen from the ranks), his fortuitous posting to Washington, where he headed the Navy's codebreaking desk at age 25, then, in another unexpected twist, found himself assigned to Tokyo to learn Japanese. This biography records Rochefort's surprising love-hate relationship with cryptanalysis, his joyful exit from the field, his love of sea duty, his adventure-filled years in the '30s as the right-hand man to the Commander in Chief, U.S. Fleet, and his reluctant return to codebreaking in mid-1941 when he was ordered to head the Navy's decrypt unit at Pearl (Station Hypo). The book focuses on Rochefort's inspiring leadership of Hypo, recording first his frustrating months in late 1941 searching for Yamamoto's fleet, then capturing a guilt-ridden Rochefort in early 1942 mounting a redemptive effort to track that fleet after the Japanese attack at Pearl Harbor . It details his critical role in May 1942 when he and his team, against the bitter opposition of some top Navy brass, concluded Midway was Yamamoto's invasion target, making possible a victory regarded by many as the turning point in the Pacific War. The account also tells the story of Rochefort's ouster from Pearl, the result of the machinations of key officers in Washington, first to deny him the Distinguished Service Medal recommended by Admiral Nimitz, then to effect his removal as OIC of Hypo. The book reports his productive final years in the Navy when he supervises the building of a floating drydock on the West Coast, then, back in Washington, finds himself directing a planning body charged with doing spade work leading to the invasion of Japan. The Epilogue narrates the postwar effort waged by Rochefort's Hypo colleagues to obtain for him the DSM denied in 1942—a drive that pays off in 1986 when President Reagan awards him the medal posthumously at a White House ceremony attended by his daughter and son. It also explores Rochefort's legacy, primarily his pioneering role at Pearl in which, contrary to Washington's wishes, he reported directly to Commander in Chief, US Fleet, providing actionable intelligence without any delays and enabling codebreaking to play the key role it did in the Battle of Midway. Ultimately, this book is aimed at bringing Joe Rochefort to life as the irreverent, fiercely independent and consequential officer that he was. It assumes his career can't be understood without looking at his entire life. It seeks to capture the interplay of policy and personality, and the role played by politics and personal rifts at the highest levels of Navy power during a time of national crisis. This bio emerges as a history of the Navy's intelligence culture.

? Protesters called it an act of war when the U.S. Coast Guard sank a Canadian-flagged vessel in the Gulf of Mexico in 1929. It took a cool-headed codebreaker solving a "trunk-full" of smugglers' encrypted messages to get Uncle Sam out of the mess: Elizebeth Smith Friedman's groundbreaking work helped prove the boat was owned by American gangsters. This book traces the career of a

legendary U.S. law enforcement agent, from her work for the Allies during World War I through Prohibition, when she faced danger from mobsters while testifying in high profile trials. Friedman founded the cryptanalysis unit that provided evidence against American rum runners and Chinese drug smugglers. During World War II, her decryptions brought a Japanese spy to justice and her Coast Guard unit solved the Enigma ciphers of German spies. Friedman's "all source intelligence" model is still used by law enforcement and counterterrorism agencies against 21st century threats.

A sweeping, in-depth history of NSA, whose famous "cult of silence" has left the agency shrouded in mystery for decades The National Security Agency was born out of the legendary codebreaking programs of World War II that cracked the famed Enigma machine and other German and Japanese codes, thereby turning the tide of Allied victory. In the postwar years, as the United States developed a new enemy in the Soviet Union, our intelligence community found itself targeting not soldiers on the battlefield, but suspected spies, foreign leaders, and even American citizens. Throughout the second half of the twentieth century, NSA played a vital, often fraught and controversial role in the major events of the Cold War, from the Korean War to the Cuban Missile Crisis to Vietnam and beyond. In Code Warriors, Stephen Budiansky—a longtime expert in cryptology—tells the fascinating story of how NSA came to be, from its roots in World War II through the fall of the Berlin Wall. Along the way, he guides us through the fascinating challenges faced by cryptanalysts, and how they broke some of the most complicated codes of the twentieth century. With access to new documents, Budiansky shows where the agency succeeded and failed during the Cold War, but his account also offers crucial perspective for assessing NSA today in the wake of the Edward Snowden revelations. Budiansky shows how NSA's obsession with recording every bit of data and decoding every signal is far from a new development; throughout its history the depth and breadth of the agency's reach has resulted in both remarkable successes and destructive failures. Featuring a series of appendixes that explain the technical details of Soviet codes and how they were broken, this is a rich and riveting history of the underbelly of the Cold War, and an essential and timely read for all who seek to understand the origins of the modern NSA.

Provides a review of cryptography, its evolution over time, and its purpose throughout history from the era of Julius Caesar to the modern day.

This vintage book contains Alexander D?Agapeyeff?s famous 1939 work, ?Codes and Ciphers - A History of Cryptography?. Cryptography is the employment of codes and ciphers to protect secrets, and it has a long and interesting history. This fantastic volume offers a detailed history of cryptography from ancient times to modernity, written by the Russian-born English cryptographer, Alexander D'Agapeyeff. Contents include: ?The beginnings of Cryptography?, ?From the Middle Ages Onwards?, ?Signals, Signs, and Secret Languages?, ?Commercial Codes?, ?Military Codes and Ciphers?, ?Types of

Codes and Ciphers?, ?Methods of Deciphering?, etcetera. Many antiquarian texts such as this, especially those dating back to the 1900s and before, are increasingly hard to come by and expensive, and it is with this in mind that we are republishing this book now in an affordable, modern, high quality edition. It comes complete with a specially commissioned new biography of the author.
For a hundred years GCHQ--Government Communications Headquarters--has been at the forefront of British secret statecraft. Born out of the need to support military operations in the First World War, and fought over ever since, today it is the UK's biggest intelligence, security and cyber agency and a powerful tool of the British state. Based on unprecedented access to documents in GCHQ's archive, many of them hitherto classified, this is the first book to authoritatively explain the entire history of one of the world's most potent intelligence agencies
An inspiring true story, perfect for fans of Hidden Figures, about an American woman who pioneered codebreaking in WWI and WWII but was only recently recognized for her extraordinary contributions. Elizebeth Smith Friedman had a rare talent for spotting patterns and solving puzzles. These skills led her to become one of the top cryptanalysts in America during both World War I and World War II. She originally came to code breaking through her love for Shakespeare when she was hired by an eccentric millionaire to prove that Shakespeare's plays had secret messages in them. Within a year, she had learned so much about code breaking that she was a star in the making. She went on to play a major role decoding messages during WWI and WWII and also for the Coast Guard's war against smugglers. Elizebeth and her husband, William, became the top code-breaking team in the US, and she did it all at a time when most women weren't welcome in the workforce. Amy Butler Greenfield is an award-winning historian and novelist who aims to shed light on this female pioneer of the STEM community.
The fast and easy way to crack codes and cryptograms Did you love Dan Brown's The Lost Symbol? Are you fascinated by secret codes and deciphering lost history? Cracking Codes and Cryptograms For Dummies shows you how to think like a symbologist to uncover mysteries and history by solving cryptograms and cracking codes that relate to Freemasonry, the Knights Templar, the Illuminati, and other secret societies and conspiracy theories. You'll get easy-to-follow instructions for solving everything from the simplest puzzles to fiendishly difficult ciphers using secret codes and lost symbols. Over 350 handcrafted cryptograms and ciphers of varying types Tips and tricks for cracking even the toughest code Sutherland is a syndicated puzzle author; Koltko-Rivera is an expert on the major symbols and ceremonies of Freemasonry With the helpful information in this friendly guide, you'll be unveiling mysteries and shedding light on history in no time!