The New York Times
nytimes.com

November 7, 1999

Cryptanalyze This

By ROBERT OSSERMAN

THE CODE BOOK
The Evolution of Secrecy
From Mary Queen of Scots
to Quantum Cryptography.
By Simon Singh.
Illustrated. 402 pp. New York:
Doubleday. $24.95.

A very old joke -- one that does not quite work in written form -- goes, "If 9W is the answer, what is the question?" One reason mathematicians are fond of this joke (whose punch line is below) is that it is a perfect example of an "inverse problem," one that arises when one knows the outcome of some process and needs to deduce what led to it. Coding and decoding -- or in Greek terminology, cryptography and cryptanalysis -- are perfect examples of direct and inverse problems. They share the basic features of both: the inverse problem is generally far more difficult to solve, and there may not be a unique answer. A direct operation playing a major part in current cryptography involves multiplying together two large numbers. The inverse takes the resulting even larger (say, 300-digit) number and tries to factor it to find the original two numbers.

"The Code Book: The Evolution of Secrecy From Mary Queen of Scots to Quantum Cryptography," by Simon Singh, grew out of one section of "Fermat's Enigma," Singh's earlier book recounting the 350-year effort to find a proof of what was the most famous unsolved problem in mathematics, Fermat's last theorem. Singh's approach is to make each of a series of historical incidents the frame for holding the reader's interest as he fills in technical details of successive coding systems. His exposition is especially effective at putting the reader in the code breaker's shoes, facing each new, apparently unbreakable code, until the discovery of a breakthrough idea uncovers a new form of vulnerability.

The book opens with the cloak-and-dagger suspense story of the Babington plot in 1586 to assassinate Queen Elizabeth and put Mary, Queen of Scots on the English throne. That motivates a history of the development of cryptography up to that time. The main tool had been the monoalphabetic substitution cipher -- scrambling a message by substituting for each letter of the alphabet some other one. The first big breakthrough in decipherment was made in the ninth century by the Arab philosopher al-Kindi in a treatise only recently rediscovered. For a thousand years or more, a message coded in a random monoalphabetic cipher was considered undecipherable unless one had the key to the code. Al-Kindi hit upon the method of listing the number of times each letter appears in the scrambled message in order of frequency and matching them with a known list of frequencies of letters in the original language. That ingenious insight was a key to deciphering a coded message from Mary, and proved her downfall.

It may seem natural that mathematics and cryptography would have significant overlap, but not until this century did the two really come together. The introduction of the German "Enigma" machine before World War II provided the impetus to resort to serious mathematical methods for cryptanalysis. Singh recounts the pioneer efforts of the Poles in the 1930's to break the Enigma by recruiting a group of 20 mathematicians, one of whom, Marian Rejewski, found the key to success. Just before the Nazi invasion in 1939, the Poles passed on their secret methods to London, providing the British with a critical lead in eventually defeating the far more complicated version of the Enigma used during the war.

But the most unexpected and powerful use of mathematical methods

was yet to come. That was public-key cryptography. Singh tells us it is "considered to be the greatest cryptographic achievement since the invention of the monoalphabetic cipher, over 2,000 years ago." It is based on the revolutionary idea that it is possible for someone to announce publicly the precise method of coding a message that anyone may wish to send him, while retaining a secret private key for decoding it. Without that key someone who intercepts the message, even knowing how it was coded, would not be able to decipher it. The theory behind this method was published in 1976 by Whitfield Diffie and Martin Hellman, and cryptography has never been the same.

One of the surprising features of public-key cryptography was that the apparently purest and least applicable part of mathematics, the theory of numbers, found a practical application. Number theory deals with properties of ordinary whole numbers. For example, any whole number raised to the fifth power will always end in the same digit as the original. Such facts seem more like curiosities than of any practical use. The noted, eccentric English mathematician G. H. Hardy, in his book "The Mathematician's Apology," proudly proclaimed, "No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world." He also said, "The great bulk of higher mathematics is useless," citing the theory of numbers in particular.

Number theory did seem "useless," but in 1977 three mathematicians at the Massachusetts Institute of Technology, Ronald Rivest, Adi Shamir and Leonard Adleman, came up with an ingenious method, later patented as the RSA algorithm, to turn the Diffie-Hellman concept into a practical system. At its heart is a fact one finds in every introductory book on the theory of numbers, known as Fermat's little theorem (same Fermat as in Fermat's last theorem and the same theorem behind the curious fact about fifth powers mentioned earlier). This simple but clever use of a little-known elementary result from number theory has evolved into a business with a $200 million annual revenue, and over 300 million copies of RSA programs installed on computers worldwide.

From its first days, public-key cryptography was seen as a threat in some governmental circles; Hellman, working at Stanford, soon found he even had to consult university lawyers about possible suits if he published his research. Singh presents fairly both sides of the continuing conflict between the government's interest in allowing only those codes to be made public that it can decipher, in order to deter criminal activity, and citizens' interest in communicating freely without being snooped on. While this goes on, the National Security Agency, which coordinates all of the government's code making and code breaking, continues trying to invent "unbreakable" codes and to decipher existing ones, and it has become the largest employer of Ph.D. mathematicians anywhere.

Of course, Singh can only speculate on what goes on inside the N.S.A. and similar organizations in other countries. His last chapter describes one possible candidate: the quantum computer and quantum cryptography. Although quantum cryptography may sound like science fiction, there is solid science behind it. On the other hand, when he describes the so-called Beale ciphers as "a true 19th-century story" with many of the same elements as "The Gold Bug," by Edgar Allan Poe, he begins to blur fiction and reality. Many readers will wonder whether an ostensible coded message that nobody has ever deciphered and that purports to give the location of treasure buried in Virginia 180 years ago may not be a hoax. But Singh never raises that possibility until the very end, when he cites one leading cryptographer's reasons for suspecting it is fabricated. He then refers to another analysis by James Gillogly, president of the American Cryptogram Association, as "evidence for the integrity of the Beale ciphers," despite the fact that Gillogly says his evidence suggests the story is a hoax.

FOR the most part, however, Singh does a fine job of presenting highlights in the history of cryptography. Newcomers to codes will find that the technical parts are generally explained clearly. For aficionados much of what is here will be familiar, although some parts are not well known, or only recently discovered. For anyone who wants to try, Singh includes a 16-page "Cipher Challenge" -- the first reader to decode a 10-stage puzzle before Jan. 1, 2010, can win $15,000 from him.

The almost universal fascination with codes undoubtedly derives from the extraordinary feats of ingenuity that have gone into devising and breaking them, as well as their enormous impact on world events. Singh's book offers more than its share of both.

And yes, if the answer is 9W, the question is "Do you spell your name with a 'V,' Herr Wagner?"

Robert Osserman, a member of the faculties of Stanford University and the Mathematical Sciences Research Institute in Berkeley, Calif., is the author of "Poetry of the Universe: A Mathematical Exploration of the Cosmos."