Melissa Martinez

The Code Book by Simon Singh

"If an enemy agent were able to check one of the 400,000,000,000,000,000,000,000,000 possible keys every second, it would take roughly a billion lifetimes of the universe to check all of them and decipher the message."

"Cracking a difficult cipher is akin to climbing a sheer cliff face. The cryptanalyst is seeking any nook or cranny which could provide the slightest purchase." (Has anyone seen *A Beautiful Mind*?) "A false line of attack will sometimes generate a few tantalizing words within a sea of gibberish, which then encourages the cryptanalyst to devise a series of caveats to excuse the gibberish."

"A 2,000 word private essay on the subject on buffalo hunting could be the key." "Alternately, the cryptographer could pick up a book on bird watching and base the key on a series of randomly chosen bird names.

"He grappled day and night with the ADFGVX cipher, in the process losing 15kg in weight."

Concealment is the art of cryptography, and has been part of human culture for centuries. When urgency was not crucial, people would shave their heads and write messages on them and wait for the hair to grow and then travel in complete safety to deliver the message, where they would merely shave their head once more. Chinese wrote messages on silk and then rolled them into little balls and covered them with wax and swallowed the messages. An Italian scientists discovered how to conceal a message on a hard-boiled egg by making an ink mixture of one ounce of alum and a pint of vinegar and then writing on the porous shell, this will penetrate and be invisible outside, but leave the message on the surface of the egg inside.

It wasn't until the fifth century B.C. that increasingly complex cryptography began to take root. Simple ciphers were created where letters would be interchanged. The number of 400… above is the possible outcomes in simple rearrangements of the alphabet. Soon, however, cryptanalysts began to test the repetition of letters and discovered that each letter in a language has a fingerprint, there are frequencies and common organization of letters in relation to other letters that can provide a key to break the cipher. For English, incredibly revealing words would be the, a, and. The difference between a code and a cipher is that a code has some level of simplification in its substitution such as ^ for the, while a cipher is merely simple substitution on the level of letters. From there, things just get complicated, "a nomenclator,is consistent of 23 symbols that were to be substituted for the letters of the alphabet (excluding j,v and w), along with 35 symbols representing words or phrases. In addition, there were four nulls and a symbol which signified that the next symbol represents a double letter."

Historical cases:

Mary Queen of Scotts used the hollow bung of a beer barrel to sneak messages past her guards. Her code was not complex and when someone deciphered it she was discovered to be plotting a

assassination attempt upon queen Elizabeth and was tricked into incriminating every member of her plot. She was beheaded.

The Great Cipher was so secure that French secrets remained hidden until enciphered papers in French archives could not be read and the mysteries remained until 200 years later the secrets of Louis XIV would fascinate historians and they revealed the identity of the Man in the Iron mask, he is believed to possibly be the twin of Louis XIV, in order to avoid controversy over who was the rightful heir. The myths this scandal inspired poetry, prose, and drama.

The Vigenere cipher has been one of the most difficult to crack, it is because each letter can be enciphered in four different ways.

Because of the telegraph, the public became painfully aware of a desire to conceal private information from the necessary operators, and this sparked a public interest in cryptography.

Lovers in Victorian England that were forbidden from expressing their affection publicly, rebelled in encrypted messages sent via the personal columns of a newspaper. These "agony columns" became somewhat of a sport as dabbling cryptanalysts would scan the notes and sometimes be successful. "On one occasion, Wheatstoned deciphered a note from an Oxford student, suggesting to his true love that they should elope. A few days later, Wheatstone inserted his own message, encrypted in the same cipher, advising the couple against this rebellious and rash action. Shortly afterward, there appeared a third message, this time unencrypted and from the lady in question, writing: "Dear Charlie, write no more. Our cipher is discovered."

"Before the overhaul of the postage system, sending a letter cost about a shilling for every hundred miles. However, newspapers could be posted free of charge, and thrifty Victorians used this loophole to use pinpricks to spell out a message of the newspaper and then send the newspaper without having to pay a penny."

The Zimmerman Telegram: "In itself, the telegram was only a pebble on the long road of history. But a pebble can kill a Goliath, and this one killed the American illusion that we could go about our business happily separate from other nations."

"Bletchley's accomplishments remain a closely guarded secret." Ever heard of him? "The bombs were dismantled, and every scrap of paper that related to wartime decipherments was either locked or burned." And this is how we lose history.

"Navajo whispers proved to be flawless." "The language was impenetrable for those on the outside of the tribe." "Though the Navajo were living in harsh conditions and being treated as inferior people, their tribal council supported the war effort and declared their loyalty. Within four months of the bombing of Pearl Harbor, 29 Navajos began an eight-week communications course." Because the language has no equivalent for military jargon, 274 words were coded as other words, like platoons to be mudclans, or Pacific to be pig ant cat ice fox ice cat. There was no worry of a code book falling into the hands of the enemy because they committed everything to memory. This was trivial because their

language traditionally has no written script and they are used to memorizing folk stories and family histories. "To check the strength of the system, a transmission was given to Navy Intelligence, the unit that had cracked Purple, the toughest Japanese cipher. After three weeks of intense cryptanalysis, the Naval codebreakers were utterly baffled by the messages. They called it 'a weird succession of guttural, nasal, tongue-twisting sounds… we couldn't even transcribe it, much less crack it.'" So they began, on the rare occasion when Japanese tried to fool them, "a Navajo message could never be faked, and so could always be trusted," the Japanese merely verified their incompetence. Overall there were 420 Navajo code talkers, they were ignored for decades, until 1968 when the U.S. Government permitted a reunion and named August 14 "National Navajo Code Talkers Day." It remained one of very few codes throughout history that was never broken.

Deciphering Lost Languages and Ancient Scripts:

"These are among the most glamorous achievements of scholarship. There is a touch of magic about knowing unknown writing, especially when it comes from the remote past." Egyptian hieroglyphics is by far the most romantic. The French Rosetta from Cairo was caught in the Treaty of Capitulation and handed to the British, who thought it was a priceless slab of black basalt, but this was the key to an entire people's world.

Cryptology Evolution:

"It really is absolutely secure."

"The best keys are created by harnessing naturally physical process, such as radioactivity, which exhibits truly random behavior." "The display restarts and once gain cycles through the alphabet until it is stopped at random by the next emission, the letter frozen on the display is added to the key, and so on."

Cipher Machines work as scramblers and unscramblers to help with difficult reconfigurations. Enigmas are machines with keyboards that have been wired to be a cipher or code, so most anyone could operate and code or decode a message.

During a phase, very popular documents or maps were used to create codes, such as the Declaration of Independence or the map of the city of London.

Key distribution has remained a hassle in times of secrecy, which dealing with cryptology, is always. There has been evolution on the type of key alterations a cryptologist can distribute so as to not reveal a code, so long as there is a base code to alter. (See image Key Distribution)

Pretty Good Privacy?

"For two thousand years encryption has been of importance only to governments and the military, but today it also has a role to play in facilitating business, and tomorrow ordinary people will rely on cryptography in order to protect their privacy."

“The fundamental dilemma for cryptography is to find a way of allowing the public and business to use encryption in order to exploit the benefits of the Information Age without allowing criminals to abuse encryption and evade arrest.” “Particularly, we fear that those who might benefit most are drug dealers, organized crime, terrorists, and pedophiles.”

Whatever happened to: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks?”

In France there “are roughly 100,000 illegal wiretaps conducted each year. Possibly the greatest infringement of everyone’s privacy.”

“It is now possible to make ciphers in modern cryptography that are really, really our of reach of cryptanalysis. And I think it’s going to stay that way.” “If all the personal computer in the world—approximately 260 million computers—were to be put to work on a single PGP encrypted message, it would take on average an estimated 12 million times the age of the universe to break a single message.”