Chapter 6

Evolution of Cryptography: Going Global

In the beginning, information was local. Neanderthal Alice and Bob shared meaning eyeball to eyeball, ear to ear, gesture to gesture. Adversaries were local, too. They had to be physically present and privy to the purpose of the gesture, the image, the spoken language in order to gain access to meaning and grab secrets not intended for them.

Suppose that, one Monday morning, cavewoman Alice leads caveman Bob through some fields to a berry patch. Because Bob understands the meaning of the event through gestures and being led to the location, he is able to find the berry patch again the next day. The Monday morning experience leaves pictures in his mind of Alice walking in front and helps him retrieve the meaning later. But now our story takes a tragic turn. Bob eats some berries from a certain bush in the corner of the patch and gets sick. Alice watches him convulse and die. Her response is an anguished howl of despair.[1]

The meaning of those particular berries is now firmly lodged in Alice's cavewoman brain. When Alice takes her kids, Casey and Dawn, to eat berries there again, she howls if they go near the poisonous bush. Casey and Dawn either understand her meaning, or they follow dear old Dad to the caveperson afterlife.

And so meaning came to be stored in and was transferred from one brain to the next.

The use of sound to convey meaning increased in complexity and precision as people envisioned more precise tools. Those grunts and gestures had to be polished into words.

When iceman Bob gave his son, Casey, instruction in flint manufacture, he needed a precise code to convey meaning for each step. Probably Bob also instructed Casey not to offer the information to strangers or other people who didn't need to share their secret. The shared code between father and son locked others out of their personal keys to meaning.

[1] Unless, of course, she intended the foul deed, a strategic maneuver beyond the scope of this text.

Now let's skip ahead a few millennia. During both world wars, the United States military devised something similar to the Bob-and-Casey code. They used the languages of Native Americans from various tribes, particularly the Navaho, to conceal voice messages from the enemy. These languages were a secure encryption method since few people had the key to their meaning. The American Indians were isolated from other cultures, and their language was local, not widespread. The Germans and Japanese were not likely to figure out its underlying meaning, and without the assistance of a local insider they were locked out.

But this method of securing and sharing meaning is less secure when information sharing technology goes from local to global. No longer do you have to be present or nearby in a particular time or place to capture information as it's presented. Having graduated from grunts to speech to writing, Alice can record and preserve the information about which berries are poisonous and where they're located so that her great-great grandchildren don't have to find out the hard way. Recorded information is much more easily shared across time and space, affording adversaries more opportunity to capture your secrets.

Early Cryptography

Oddly enough, some of the earliest cryptographers weren't really trying to hide anything. Rather, they were drawing attention to their subject and showing off their language skills by playing with words.

When the knowledge of written language was not widespread, as in Caesar's time, ciphers didn't need to be very complex. That's because written language, like early spoken language, is a pretty good secret keeper when very few people can read or speak it. Caesar's cipher, simple as it was, was good enough for a while. Even so, ingenious ways of hiding communications—later used during

Crypt from the Crypt

Nearly 4,000 years ago, a scribe deliberately changed the hieroglyphics symbols in an Egyptian tomb, thereby creating the oldest cryptographic writing. According to cryptographic historian David Kahn, the scribe's intention in carving the symbols into stone in a different way was not to hide the message, but perhaps to dignify it—or maybe the scribe was just showing off his knowledge.

As tombs proliferated, so did the instances of Egyptian scribes taking poetic license. For example, sometimes the new hieroglyph had the same first sound as the one replaced, or the scribe might use a play on words. It was done as a game or a decoration to catch the reader's eye.

both world wars—were first written about by Aeneas the Tactician more than 2,000 years ago. In *On the Defense of Fortified Places*, Aeneas explained methods of *steganography*, a form of communications security that used hidden compartments and invisible inks. In one system, Aeneas suggested pricking holes above or below a document's letters to indicate a secret message. German spies used this method in World War I and used a modified version in World War II, marking letters in newspapers with invisible ink.

Nomenclators were a way to add complexity to methods of concealment.

As history unfolded and more people were able to read and write, something had to be done to better deal with the growing number of potential adversaries. The Renaissance birthed combination cipher and code systems, termed *nomenclators*, that were designed to mask communications of popes, royalty, and Renaissance commerce. Mixing codes and ciphers was a way to add complexity to methods of concealment. *Codes* are words, numbers, letters, or symbols used to replace words, letters, and phrases; an example is 007 for James Bond. Nomenclators can consist of thousands of code words or code numbers. Ciphers, as you've seen in previous chapters, replace the message letters with other letters, numbers, or symbols, as in substitution, or they rearrange the individual letters of the plaintext, as in transposition—or a combination of both.

It was also during the Renaissance that cryptanalysis became a profession, with the rise of so-called Black Chambers: groups of people who intercepted and read letters as well-paid employees of governments such as England, France, and Austria in the 1700s. These fledgling cryptanalysts learned through experience how to crack the various cryptographic systems then in use. The best of these early cryptanalysts began to recognize patterns, and over time they unmasked keys and ciphers used by unsuspecting diplomats.

Snoops and Eavesdroppers of Yore

A 10-man team of well-paid snoops was key to Austrian diplomatic strategy in the eighteenth century. Because Vienna was a crossroads city between eastern and western Europe, the Austrian Black Chamber had access to mail from several important embassies. Such mail was secretly brought from the post office to the chamber, where the staff melted seals after forging their designs for later use. Letters were copied and envelopes resealed without disrupting regular postal schedules. Mail in transit from other places was also intercepted.

Handling 80 to 100 letters a day, the team worked one week on, one week off (except in emergencies) to minimize stress. These cryptanalysts won bonuses for solving difficult ciphers and even received unemployment bonuses when keys were stolen instead of having to be cryptanalyzed. Foreign diplomats knew what was happening to the mail but couldn't stop it.

(Continued)

Like the men of the Austrian Black Chamber, America's On the Roof Gang of the late 1920s, a group of radio operators, underwent vigorous training to track the communications of Japan. Part of the group's mission was to understand how to interpret *kata kana*, the Japanese version of Morse code. Those who passed the difficult four-month course, held in a classroom on top of the Navy department building in Washington, D.C., were placed in exotic locations to listen for Japanese dots and dashes.

Commercial and Military Needs

Over time, nomenclators began to be unwieldy. Then, in the mid-1850s, the telegraph brought in Morse code as well as nonsecret codes to shorten commercial communications and make them more cost-efficient. Business executives didn't have time for convoluted encryption with all its unwieldy keys, but the military had a different agenda. The military needed secure ways to communicate quickly and accurately over long distances.

Invention of the telegraph increased the need for secure ciphers during wartime.

The telegraph, much used during the U.S. Civil War in the 1860s, made messages easier to send and intercept, increasing the need for secure ciphers. But the military didn't always make good choices. As pointed out in Chapter 2, Vigenére's table, although easy to attack by knowledgeable cryptanalysts, was mistakenly thought secure by many people for generations. So when the Confederate Army entrusted its military secrets to such a system, the Union Army had the advantage and exploited it. Even so, in 1914 the U.S. Army based its Larrabee cipher on Vigenére's table.

Other types of systems used for military encryption also proved to be ineffective. After 1931, the Japanese beefed up their cryptographic know-how following the publication of *The American Black Chamber* by American

The Need for Speed

Before Samuel F. B. Morse assigned dots and dashes to the alphabet to create Morse code, he counted the letters in a Philadelphia newspaper's type case. Armed with this information about the most frequently used letters, he chose the shorter dot-and-dash symbols for them, increasing the transmission speed of telegraph messages. Cryptography has a similar need for speed. If cryptography is to be widely used to protect the data of millions of people who are traveling the Internet highway, its execution must not slow us down.

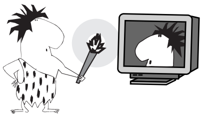
From Red to Purple

In the late 1930s, the Japanese came up with a mechanized cryptographic system they thought was unbreakable. Called Alphabetical Typewriter 97 and code-named Purple, it replaced a machine called Red that the Japanese didn't know the United States had broken. Because the messages in Purple were similar to those in Red, the Americans were able to cryptanalyze the new cipher. An analog of the Purple machine built from telephone selector switches assisted the U.S. cryptanalysts of the Signal Intelligence Service (SIS) in breaking the code. Through most of the 1930s the SIS had an average annual budget of $17,000, spending only $685 on hardware for the Purple analog.

cryptographer Herbert Yardley. This book contained indiscreet disclosures of U.S. knowledge of Japanese codes.

Military history has confirmed that the tide of war can turn on who knows what about whom and when. Perhaps the best advantage comes when you can grab the keys to your opponent's system without the opponent realizing you've got them.

Entering the Computer Age



Making sure that you use a strong method or algorithm and keeping keys secure are ongoing concerns. Math and computers are the means we use today to provide that security. The work of two American men and one American husband-and-wife team during this century significantly contributed to elevating cryptology to a mathematical science. They were geneticist-turned-cryptanalyst William Friedman and his wife, Elizabeth Friedman, who had a college degree in English; mathematics professor Lester Hill; and expert tightrope walker, unicycle rider, and brilliant engineer-mathematician Claude Elwood Shannon.

During the 1920s William Friedman, who began solving ciphers for the American government before WWI and developed cryptanalysis training programs for the federal government, published a paper that linked cryptography and mathematics. He presented the distribution of letters as a curve having characteristics that could be quantified with statistics. Later he developed a well-defined mathematical test, the kappa test, that allowed him to apply probability studies that would correlate plaintext and ciphertext letters. In the 1960s he lived to see computers apply his test to cryptanalyze ciphertext very rapidly.

Along with her husband, Elizabeth Friedman worked for the U.S. Army as well as doing cryptanalysis for the Navy and the State Department. During

Prohibition in the 1920s she helped the Coast Guard decrypt messages from bootleggers. The Friedmans became a team before World War I at an Illinois think tank called Riverbank, where they began working with cryptography by investigating the authorship of the works attributed to William Shakespeare.

In 1929 Lester Hill, while assistant professor of mathematics at New York City's Hunter College, published a paper showing how to use algebraic equations in cryptography. Although his system was too complex for widespread use, Hill's work broke ground that led more mathematicians to investigate cryptography.

In the 1940s Shannon—trained at MIT and honed at Bell Labs—described cryptology in terms of information theory, a field he gave birth to. Math-dense information theory explains that languages use more symbols than are needed to transmit meaning, a phenomenon called *redundancy*. Shannon wrote that in most ciphers "it is only the existence of redundancy in the original messages that makes a solution possible." Shannon also coined the terms *diffusion* and *confusion*.

Such mathematical analysis of cryptography has allowed computers to take over much of the brain-cracking work of cryptanalysis and has spread cryptography everywhere that there's a computer. For that we can thank the British mathematical genius Alan Turing, whom cryptographic historian David Kahn calls "the intellectual father of the computer." Turing's mathematical brainchild was the blueprint for the Colossus, the codebreaking device built by the British to crack Germany's advanced enciphered teletype transmissions during World War II. Turing's ideas were also vital to the building of the Bombe, a machine that rapidly found the keys for German communications enciphered with the Enigma machine.

Computers have made it a snap to add complexity to cryptography.

Computers have made adding complexity to cryptography a snap. They have also made solving complexity more of a snap. Because of rapidly advancing technology, secure systems must constantly be assessed for the possibility of new attacks if security is to be maintained. Secret sharing and hiding is still a tug of war between clever cryptographers and ingenious cryptanalysts with new tools in their belts. If the algorithm is so secure that it can be made public, is there less to worry about?

Alice and Bob and Casey and Dawn must still be vigilant in their communications. No longer can they judge strangers, eyeball to eyeball, to assess the person they're sharing secrets with, as in their caveman days. They need an electronic method to feel assured that their secrets are being shared only with a trusted few, that their messages aren't being tampered with, and that they always know the person with whom they are communicating. Chapter 7, "Secret Key Assurances," shows how secret key cryptography can provide the assurances we seek. The limitations of secret key cryptography are then shown in Chapter 8, "Problems with Secret Key Exchange." The rest of the book shows how you can use public key cryptography to solve the problems of secret key cryptography.

Review

From the beginning of humankind, language was a way to both convey and hide meaning. The invention of writing gave people a way to hide meaning that was effective until increasing numbers of people learned how to read and write. Widespread understanding of written and spoken language made cryptography essential if one was to conceal meaning.

The Renaissance gave birth to combinations of ciphers and codes to help make cryptography more complex. However, complexity has never been an automatic guarantee of security.

Cryptography was elevated to a mathematical science through the work of several Americans in this century. But the work of one Briton, Alan Turing, the intellectual father of the computer, is what makes computer cryptography possible. Despite technological advances, however, the need to be vigilant in choosing the methods and keys still applies.