

Topic 18: History of Cryptography

Cryptography has long been used to conceal messages.

- The Greeks used steganography—covered writing. For example, they would write on a wooden tablet and cover it with wax. Or, according to one story, write the message on the shaved head of a messenger and wait for the hair to grow back.
- The Chinese wrote messages in silk, rolled the silk into a ball, covered the ball in wax, and had a messenger swallow it.
- Julius Caesar used the shift cipher.
- The Arabs invented cryptanalysis—they had the sophistication in mathematics, statistics, and linguistics that was required to break messages systematically. An Arab manual for deciphering was even written.
- There are also examples of cryptography in the Old Testament—for example in Jeremiah 25:26 and 51:41 the word "Babel" is replaced by the word "Sheshach." "The first letter of Babel is beth, the second letter of the Hebrew alphabet, and this is replaced by shin, the second-to-last letter; the second letter of Babel is also beth, and so it too is replaced by shin; and the last letter of Babel is lamed, the twelfth letter of the Hebrew alphabet, and is replaced by kaph, the twelfth-to-last letter" (Singh, p26). The use in the bible intrigued monks who wrote their own books on the subject.
- In the early 1500's cryptanalysts began to be employed by royal courts in Europe. For example, Giovanni Soro in Italy, and Francois Viete and Philibert Babou in France. "Babou gained a reputation for being incredibly persistent, working day and night and persevering for weeks on end in order to crack an intercepted message. Unfortunately for Babou, this gave the king ample opportunity to carry on a long-term affair with his wife" (Singh, p28).

- Vigenere was born in 1523. He became a diplomat and spent time in Rome on diplomatic missions. Then, at 39, he devoted his life to the study of cryptography, creating the Vigenere cipher in the process. It was published in 1586. It took almost two centuries for it to gain widespread acceptance.
- In the 1600's a powerful cipher called The Great Cipher was invented by Antoine and Bonaventure Rossignol. It is an enhanced monoalphabetic cipher and was used by Louis XIV in France. Eventually the Great Cipher was no longer used and the details of it were even forgotten, with the result that pages and pages of historical court documents and messages in archives could not be read. In the late 1800's the cipher was re-examined by Etienne Bazeris who spent three years trying to break it. He finally succeeded, discovering that a number in the cipher stood not for a letter but for a syllable.
- By the 1700's cryptanalysis in Europe was a sophisticated enterprise. For example, "Letters which were supposed to be delivered to embassies in Vienna were first routed via the Black Chamber, arriving at 7am. Secretaries melted seals, and a team of stenographers worked in parallel to make copies of the letters. If necessary, a language specialist would take responsibility for duplicating unusual scripts. Within three hours the letters had been resealed in their envelopes and returned to the central post office, so that they could be delivered to their intended destination....Each day a hundred letters would filter through the Viennese Black Chamber." (Singh, p. 59). The success of this and other Black Chambers against monoalphabetic ciphers prompted the adoption of Vigenere and other polyalphabetic ciphers.
- One of the most famous cipher stories of the 1800's concerns the Beale cipher. In 1822 Thomas J. Beale left a locked box with the owner of a hotel in Virginia with instructions to open it in ten years time if Beale had not returned. Beale never did return, and in 1845 the hotel owner finally opened the box. What he found inside were three pieces of paper with ciphertext on them and a letter in English. The letter said the ciphertext documents revealed the location, contents, and heirs to a treasure. Beale promised a key would be sent to the hotel owner, but one never was. A friend of the hotel owner managed to decipher one of the documents—the one listing the contents of the treasure— and he

published a pamphlet telling the story of Beale and providing the three ciphertxts in the hopes that someone else would be able to decipher them. They remain a mystery to this day.

- The history of cryptography in the first half of the 20th century is intertwined with warfare. The most famous cryptographic incident of WWI is the Zimmermann telegram which succeeded in bringing the Americans into the war. In 1917 the German foreign minister, Arthur Zimmermann, sent an encrypted telegram to his ambassador in Mexico via his ambassador in the US asking him to convince the president of Mexico to join with Germany in attacking the US and furthermore to incite Japan to attack as well. The encrypted telegram was intercepted by the British who managed to decipher it. The British knew if they showed the telegram to the Americans they could convince them to fight in the war, but they also knew if they revealed their knowledge of the telegram the Germans would know their cipher had been compromised. So the British arranged first to have the message intercepted in Mexico after the German ambassador in the US had relayed it. This relayed message was slightly different from the original message (eg. different address). The British presented their evidence to US president Woodrow Wilson who promptly joined WWI. The ruse was successful—Germany believed the leak was in Mexico—and the British went so far as to discredit their own intelligence agents to throw the Germans off the track: The admiral "planted a story in the British press criticizing his own organization for not intercepting the Zimmermann telegram, which in turn led to a spate of articles attacking the British secret service and praising the Americans" (Singh, p115).
- The cryptographic story of WWII is Bletchley Park and the cryptanalysis of the Enigma machine. The Enigma machine was a rotor machine that enciphered plaintext using a keyboard and a series of rotors. It was invented in 1918 by the German Arthur Scherbius and marketed to businesses and the military. Unfortunately it failed to gain acceptance with the business community, but the German military did show some interest and by the time WWII had started the Germans had brought 30,000 machines. The British get the credit for breaking the Enigma, but a large part of the groundwork was laid by Polish cryptanalysts who had good reason to want to monitor German intentions. In

fact one Polish cryptanalyst—Marian Rejewski— actually succeeded in breaking a weaker version of the Enigma that was in use in the 1930’s. This was a remarkable achievement. Just before Poland was invaded in 1939 the Poles turned over to the British all they had learned about the Enigma. The British cryptanalysts were based at Bletchley Park, in the heart of Britain, and their work was so secret even the townspeople had no idea why the cryptanalysts were there. It is astounding the secret never leaked, but the devotion to duty was so ingrained that even years later some people were reluctant to speak about it. The Enigma was broken here under the leadership of Alan Turing using a number of techniques, the most famous of which was an electronic computing machine, a forerunner of the computer.

- More detail on the Enigma.... The Enigma has three main components:
 1. a keyboard for input
 2. a system of rotors for scrambling the input
 3. a display board for output (with illuminating lamps for each letter)

To encrypt, the operator presses a key on the keyboard. This sends an electric signal through the rotor system which enciphers the letter and lights up the lamp corresponding to the output. The rotors are internally wired to map each plaintext letter to a ciphertext letter. Simply described like this it appears that the machine is just a fancy substitution cipher! However, several rotors are aligned in parallel so the output of one rotor is the input to the next. But this is still unsophisticated. However, there is an additional step: at each stage the rotor rotates one position. This makes the system polyalphabetic. An additional reflector rotor makes decryption easier. Further complications are interchangeable rotors (so the rotors can be permuted) and a plugboard that allows six letters (of the operator’s choice) to be swapped.

The key is the initial position setting of the rotors. Both Alice and Bob must have Enigma machines and a codebook indicating the starting positions for the rotors, the order of the rotors, and the plugboard positions.

Notes created 2001 by A.M. Hamel. Material taken from Singh, The Code Book