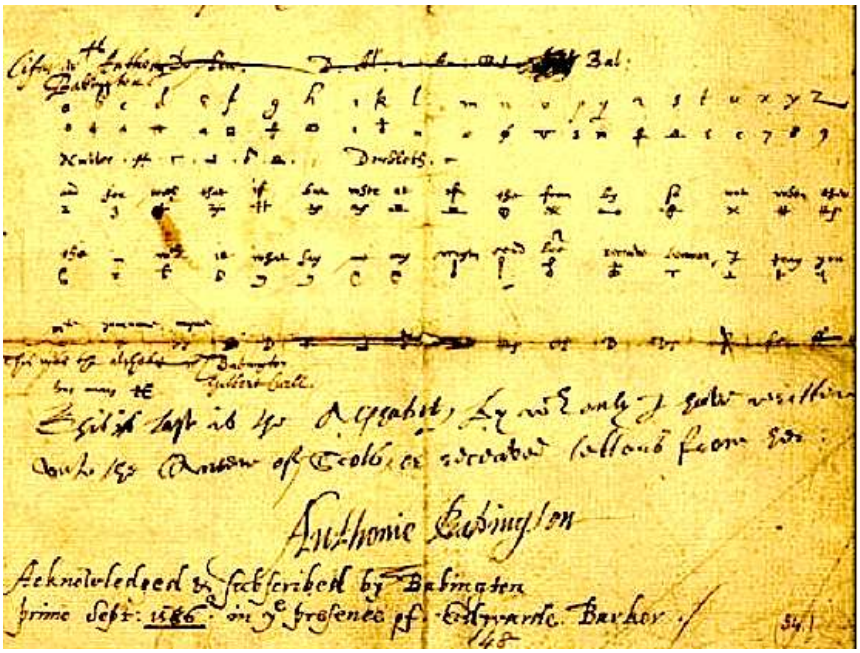
Pen2Paper



Shhhhh!

A History of Written Secrets

On the 18th June 2014, the Duchess of Cambridge reopened Bletchley Park, the best kept secret in wartime Britain. In 1939, a series of wooden huts were rapidly constructed to house the Government Code and Cypher School that would spend the next 6 years trying to solve the infamous codes generated by the Enigma machines. More than 3000 coded messages passed through Bletchley Park every day and their decryption is one of the most remarkable tales of code-breaking in history.

The Duchess of Cambridge at Bletchley Park

Is it a Code or a Cipher?

Many different terms are used to describe the process of hiding information with their differences largely due to the process of concealment. The difference between a code and a cipher, for example, is that a code uses whole words or phrases that may require a code book to translate. A cipher, conversely, makes use of single letters, numbers or symbols which may be rearranged or replaced to conceal information. Once the cipher pattern is understood by the recipient, there is no need for a codebook to aid the retrieval of the information.

The term *cryptography* has its roots in the Greek words *kryptos* and *graphos* and translates as 'secret writing'. Cryptanalysis refers to the science and art of retrieving information that is encoded. Another term commonly used is *steganography* which refers to coded information hidden within an everyday object or text.

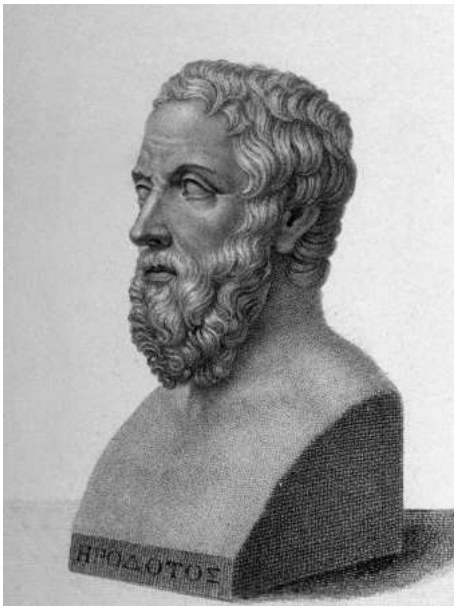
One website describes the difference between cryptography and steganography by looking at their etymological origins; cryptography is 'secret writing' whereas steganography is 'covered writing'. The challenge in cryptography is that unauthorised parties are unable to understand the message, whereas in steganography, unauthorised parties would be unaware of the existence of the message in the first place.[i]

Keeping Secrets in Ancient Times

One of the oldest examples of writing being disguised or changed to hide meaning is seen in a cuneiform tablet dating from 1500 BC. It is believed to contain the recipe for a pottery glaze which the craftsman did not want to share with his fellow artists.[ii]

A simple cipher known as Atbash is seen in the Old Testament of the Bible. The Atbash cipher involves the reversal and substitution of the letters of the Hebrew alphabet and is used to encrypt the names of places in the Book of Jeremiah which dates from the 6th century BC.[iii]

A century later, Herodotus, the famous Greek historian writes of an intriguingly slow encryption process that involves the tattooing of a shaved slave's head and then allowing the hair to regrow before sending the slave to the recipient of the message. The steganogram would then be revealed when the slave was once again shaved.



Herodotus

"For Histiaios, desiring to signify to Aristagoras that he should revolt, was not able to do it safely in any other way, because the roads were guarded, but shaved off the hair of the most faithful of his slaves, and having marked his head by pricking it, waited till the hair had grown again; and as soon as it was grown, he sent him away to Miletos, giving him no other charge but this, namely that when he should have arrived at Miletos he should bid Aristagoras shave his hair and look at his head: and the marks, as I have said before, signified revolt."[iv]

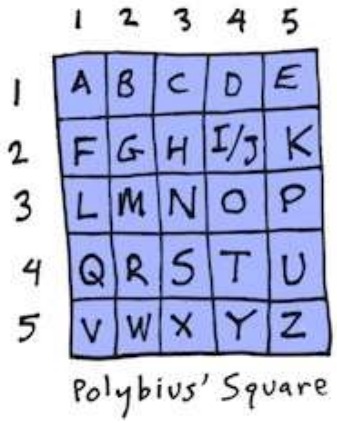
Further methods of steganography described by Herodotus included written messages concealed within wax tablets and perhaps most bizarrely within the body of a hare, delivered by someone posing as a hunter.[v]

Lysander of Sparta, a Spartan admiral who helped to bring about the end of the Peloponnesian War (434-404 BC) is cited as the first recipient of a coded message when in 405 BC he was visited by a servant wearing a belt that when removed and wound around a wooden baton revealed a message that informed Lysander of an impending attack from Persia. This form of encryption is known as a scytale.

A scytale

An ancient Indian text also reveals that the use of cryptography was common amongst leaders from as early as the 4th century BC when the text known as *Arthshashtra* was written. The epic work is known as a treatise on statecraft and in its descriptions of the daily duties of a king, lists interviewing secret agents and receiving secret information from spies as two priorities.

In ancient Greece, Polybius, a historian and scholar of the 2nd century BC developed a system for reducing the letters of the alphabet to simple pairs of numbers, using a device now known as the Polybius square or checkerboard.



An example of a Polybius square

Whilst it was originally conceived by Polybius as a more advanced form of smoke signals, whereby messages could be sent by the raising of pairs of lit torches over distances, it soon was developed as a written cipher. Polybius' original cipher used the Greek alphabet but it can also be applied to the English language amongst others, including Japanese. Because this cipher only requires 5 digits it can also be used as a steganogram, with items in multiples or groupings of five being easily concealed in a variety of media, such as stitches in fabric or knots in a rope.[vi]

Meanwhile, in the Roman Empire, Julius Caesar (100 – 44 BC) wanted to develop a technique for communicating his military tactics and battle plans without any risk of revealing this information to his enemies. His solution was a simple cipher where each letter of a word was substituted with the letter three places further along in the alphabet:

For example - A T T A C K became D W W D F N

This cipher was very simple to use, but this also made it very easy to interpret as there were a finite number of options for the meaning of each letter; that is, limited to the 26 letters of the alphabet. This cipher is often referred to as Caesar Shift.

Frequency analysis allows cryptanalysts to seek out the most commonly used symbol in a cipher. This information combined with the knowledge of the most commonly used letter in a language, in the case of English – 'E', allows for the substitution of that symbol and the beginnings of the decoding process. Other aspects of frequency analysis include identifying one letter words, which in English will represent either the letters I or A and analysing the frequency of three letters words, recognising that 'and' and 'the' are likely to be the most commonly used of these.[vii]

The development of frequency analysis is credited to Al-Kindi who was an Arab mathematician in the early 9th century AD. His book *Manuscript for Deciphering Cryptographic Messages* describes a number of ciphers and cryptanalysis techniques as well as revealing an extensive knowledge of the workings of the Arabic language, which was likely to stem from analytical study of the Qur'an.

Portrait of Al-Kindi

Many of these early monoalphabetic substitution ciphers could be easily decrypted with frequency analysis and this remained the case until the development of the first polyalphabetic cipher which was first described by Leon Battista Alberti in approximately 1467 AD. Alberti's work, together with the *tabula recta* (a square table of alphabets) devised by Johannes Trithemius in 1508, led to the development of Vigenère's cipher in 1586.

The First Polyalphabetic Cipher

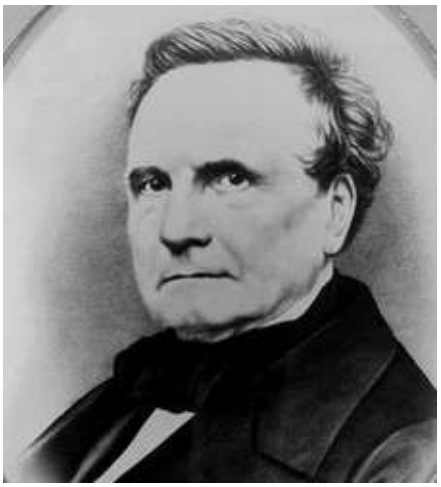
In the 16th century, Blaise de Vigenère developed the first cipher that made use of an encryption key. In its original usage, this term relates to a password or phrase that is known by both the sender and receiver of the coded message and is used as an additional security layer to prevent the decryption of the message by a third party. Vigenère designed an extended Polybius square that contained 26 rows and columns and a complex form of the Caesar shift cipher.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Tabula Recta

To create a code using Vignenère's cipher, the sender takes the first letter of the encryption key and the first letter of the message to be encrypted (known as plaintext) and finds the point at which they intersect on Vigenère's square. This letter becomes the first letter of the coded message (known as ciphertext).

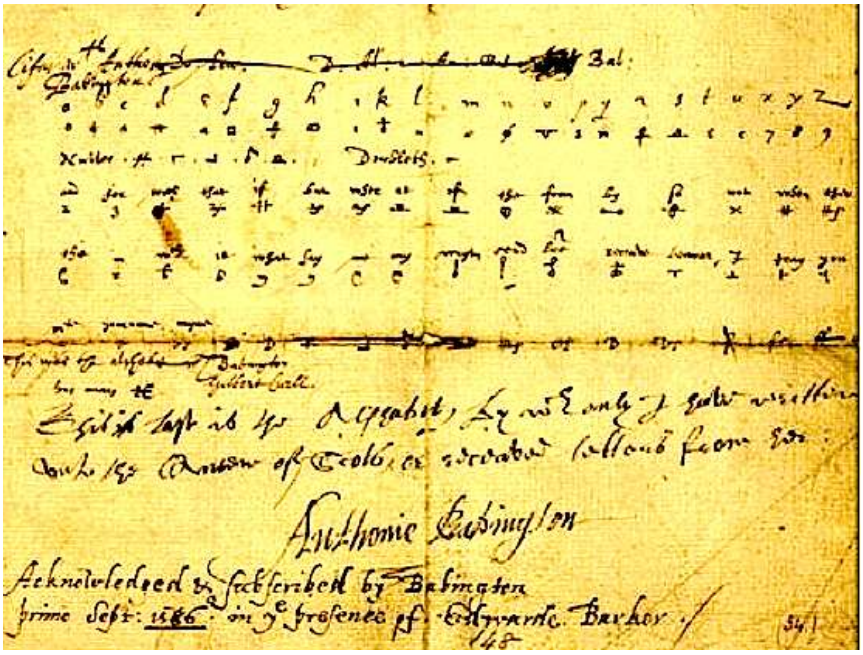
Vigenère's cipher remained unchallenged for three centuries until Friedrich Kasiski, a German cryptographer, published a method for the decryption of the cipher in 1863. It has been suggested that Charles Babbage, the British polymath and father of the computer had previously deciphered Vigenère's method during the Crimean War of the 1850s but this was kept as a military secret. Babbage's role in the decryption of the cipher was not acknowledged fully until the 1980s.



Charles Babbage

Life and Death and Coding

A variation on a simple monoalphabetic cipher was used by Mary Queen of Scots in her bid to overthrow Elizabeth the First. Her cipher used a symbol in substitution for each letter of the alphabet. Whilst her coded correspondence with Anthony Babington, was more complex in coded nature to previous methods, it could still be solved with frequency analysis. Sir Francis Walsingham who was responsible for Elizabeth's security intercepted these messages and was able to decipher the code, leading to Mary's execution for treason in 1587.



The Babington Plot coded letter

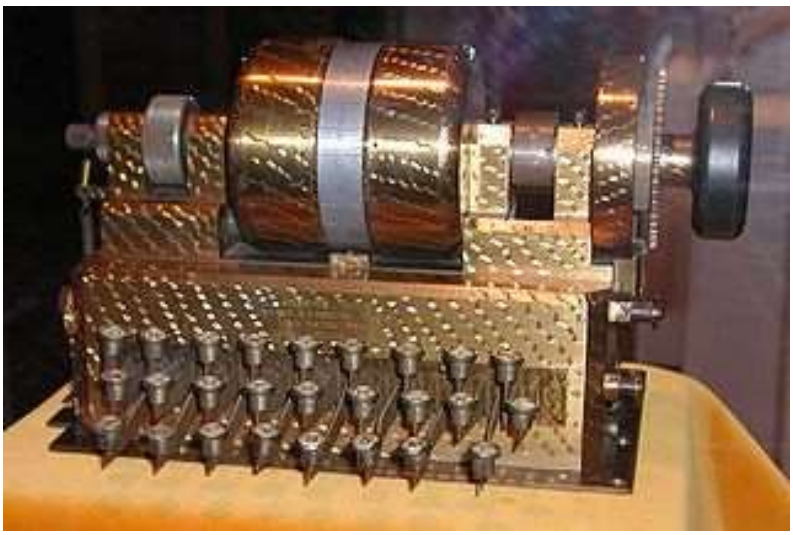
Machine Generated Coding

Morse code is arguably the best known example of code although it might be better described as a form of writing system as it is in no way secretive. Its use in the communication of encrypted messages is however, very significant.

Samuel Morse was an Arts and Design professor at New York University. He developed a system in 1836 that used an electrical current over a wire to move an electromagnet, which in turn moved a marker to record codes onto a strip of paper. A modification of this system in the following year saw the paper embossed with dots and dashes. Morse sent his first message, with the help of his assistant Alfred Vail, across a two mile stretch of wire in Morristown, New Jersey in 1838.

The United States Congress were so impressed with Samuel Morse's invention that they provided $30,000 of funds (the equivalent of roughly $10 million today) to establish a telegraph line over the forty mile distance between Baltimore and Washington D.C. in 1843. Although Morse considered placing the cables underground to begin with, he determined that overhead cables suspended from poles would be more effective.

The first mechanical device to generate codes was invented by Edward Hebern towards the end of the Frist World War, and was known as the Hebern rotor device. Hebern's invention was built from both electrical and mechanical typewriter parts and featured a two sided disc containing the letters of the alphabet and small electrical contacts. When the user pressed a key on the typewriter keyboard, contact would be made with a differing letter on the rotor which would be the first coded letter of the message.



A Hebern encoding machine

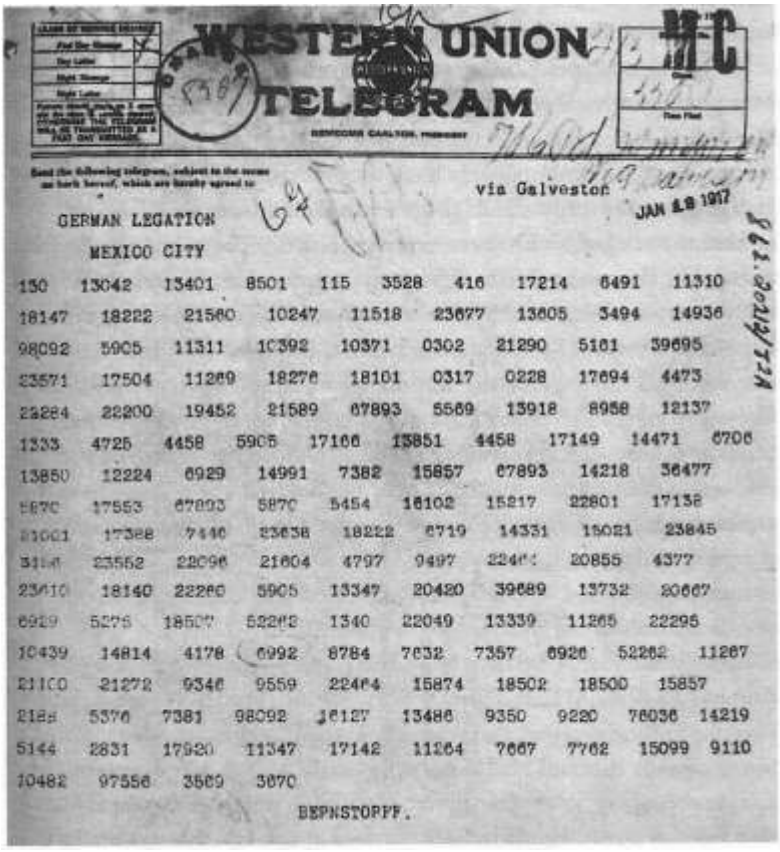
The passing of current through the contacts on the rotor would generate a typed encrypted letter and each subsequent key stroke would shift the rotor so that the cipher used multiple alphabets in the same manner as Vigenère's cipher.

The decryption of the message required the rotor to be reversed so that when the cipher text was typed into the machine, the plain text would appear on the page. It was this technology upon which the famous Enigma machine of the Second World War was based, using multiple rotors to generate coded messages in more than 150 million million million different ways. [viii]

Coding in wartime

The importance of coding in wartime must not be underestimated and has literally changed the course of history. It has been said that the decryption of the Enigma machine used by the Germans during the Second World War brought about the end of the war sooner by as much as two years.

Coded messages in the First World War also held much significance with the interception and decryption of the Zimmerman telegram signalling the beginning of American involvement in the conflict. The telegram sent by the German Foreign Secretary, Zimmerman to the Mexican government intended to broker an alliance between the two countries with a view to assisting Mexico in reclaiming some of the bordering American states.



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17136
21001 17388 7446 23638 18222 6719 14331 15021 23845
3184 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
21824 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

The Zimmerman telegram

Simple codes such as the number patterns seen in the Polybius squares have been used as an auditory code by prisoners of war in conflicts such as the Vietnam War, or earlier in the Spanish Civil War as author Arthur Koestler experienced and then described in his 1940 novel *Darkness at Noon* which focuses on the lives of prisoners during Stalin's Great Purge in 1938:

"No. 402 was now tapping regularly; three times with short intervals, then a pause, then again three times, then again a pause, then again three times. Rubashov repeated the same series to indicate that he heard. He was anxious to find out whether the other knew the 'quadratic alphabet'—otherwise there would be a lot of fumbling until he had taught it to him."[ix]

The Enigma Machine

Perhaps the most famous example of coding in the 20th century was that employed by the Germans before and during the Second World War. The Enigma machine was developed as a cipher machine using multiple rotors, for communications between the German army, air force and navy.

Each day, operators of Enigma machines would consult the codebook which would inform them of the correct settings for the machine for that day – namely the starting position, the connections to the plugboard and the order of the rotors. When an operator pressed a key on the typewriter keyboard, a different letter would alight on the lampboard thus generating an encrypted message. These messages would then be sent via Morse code to their recipients.

The Enigma machine

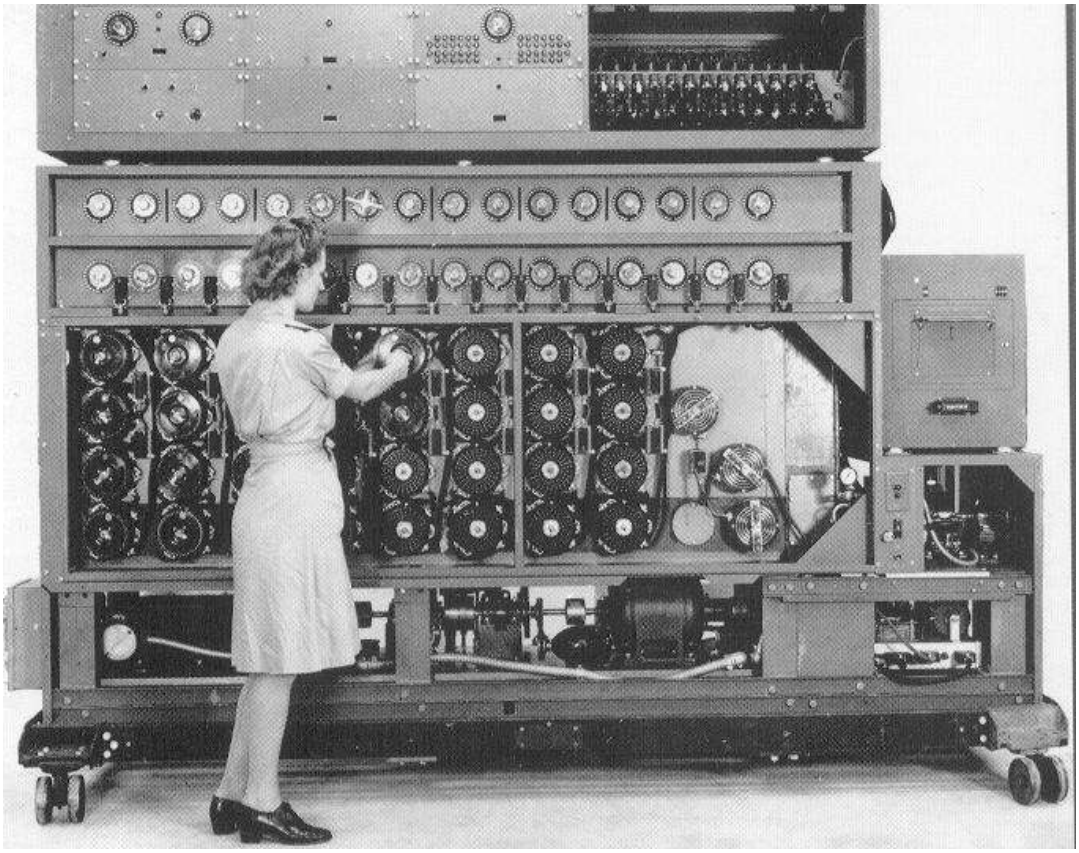
A team of Polish cryptanalysts, including Marian Rejewski, Jerzy Rozycki and Henryk Zygalski, made significant progress towards cracking the code prior to the outbreak of the Second World War. As the threat of war loomed, circumstances became more challenging for the team at Poland's Cipher Bureau. Their models and drawings of the Enigma machine were shared with the British and French who continued with this mammoth task as the war broke out.

The encrypted Morse code messages were intercepted at Y stations, where operators would record them at a rate of up to 90 letters per second. An average of 3000 messages were intercepted and sent on to Bletchley Park every day, where teams of code-breakers would attempt to reveal their contents.

A Y station operator

With 3000 coded messages arriving each day, and the clock ticking until the Enigma machines would be reset with a new coding system, the cryptanalysts needed to find common patterns of words that would appear daily, such as those in weather reports.

Bletchley Park had their own electro-mechanical machines known as Bombes, invented by brilliant mathematician and pioneer of computing, Alan Turing. These machines were able to check through combinations of letters looking for possible clues, far quicker than a human was able to.



A Bombes decoding machine

An early breakthrough came in 1941, when the crew of a German submarine surrendered after being forced to surface by allied ships. When a search of the deserted submarine was conducted, an Enigma machine and codebook were retrieved and photographed by staff from Bletchley Park.

As the war progressed, so too did the technology at Bletchley Park that was charged with the task of checking possible combinations of letters. Cryptanalysts knew that every 24 hours, when the Enigma machines were reset, they would have to begin the code breaking process again and therefore it was vital to speed up the checking process.

In 1943, Tommy Flowers and a team of fellow Post Office engineers created Colossus, a vast machine that filled an entire room that could check up to 5000 letters a second. The information that it generated became known as ULTRA and remained highly classified until long after the war had ended. ULTRA enabled the Allies to reduce the impact of enemy operations, although at times it was necessary to take no action to prevent suspicion that their codes may have been cracked.

The role of the decryption of Enigma was so vital that those who worked at Bletchley Park were sworn to secrecy about their work, even long after the cessation of conflict. In addition to security fears, there was also concern that the Germans might suggest that they were not fairly beaten if they were fully aware of the repercussions of the events at Bletchley Park. [x]

"Codebreaking did not win the war, but it probably helped to shorten it - perhaps by a year or more"[xi]

Contemporary Coding

The other significant impact of the remarkable work conducted at Bletchley Park is the development of the modern computer. Until the Second World War ended, codes and ciphers were a part of the military domain, rarely used or needed by civilians. In the second part of the 20th century, businesses saw the need to use codes as a method of protecting the design of their products from competitors. IBM began work on designing an encryption method for its customers as early as the 1970s and in 1973 their cipher, known as Lucifer, was launched.

As computers were so expensive at this time, cryptology was largely financed and driven by government. In later years the Lucifer cipher was adopted by the United States government and became known as DES or the Data Encryption Standard. By 1997, the cipher had been broken due to the insufficient size of the encryption key. DES was replaced by a more complex cipher in 2000, known as Rijndael and renamed AES or Advanced Encryption Standard.

As the digital age has advanced, both businesses and individuals have demanded effective data encryption methods to protect everything from instant What's App messages to online banking transfers. Whatever the nature of the data that requires encryption, the principle of protecting that message remains the same as it did in the days of Lysander of Sparta. This principle is known as Kerckhoffs' principle.

Auguste Kerckhoff wrote two journals on *La Cryptographie Militaire* in 1883 in which he identified a number of principles to be considered when designing a military cipher. The most fundamental of these is the importance of the secrecy of the encryption key, even if all other information about the cipher or coding system is in the public domain. It is impossible to expect the existence of a coding system or coded messages to remain a secret, in much the same way as it is impossible to expect the location of a bank's vault to be unknown. As long as the keys are protected the precious data (or wealth) held within will remain secret and secure.

---

[i] Information gathered from *Evolution of Steganography* video located online at http://stegano.net/tutorial/steg-history.html

[ii] Information originally located in David Kahn's *The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet,* Scribener, 1996, referenced in the History of Cryptography article located at http://en.wikipedia.org/wiki/History_of_cryptography

[iii] An example of the Atbash cipher can be seen in Jeremiah 51.1

[iv] Quotation taken from *The Histories of Herodotus* referenced in *Cryptography: Herodotus* article located online at http://www.machinae.com/crypto/herodotus.html

[v] See endnote iv

[vii] Information gathered from C Ellis' article *The Secret World of Codes and Codebreaking* located online at http://nrich.maths.org/2197

[viii] Statistic taken from http://archive.iwm.org.uk/upload/package/10/enigma/enigma7.htm

[ix] A Koestler, *Darkness at Noon ,* 1940. Quotation taken from p 8 of ebook version located at https://libcom.org/files/[Arthur_Koestler]_Darkness_at_Noon.pdf

[x] Information gathered from B Fenton's article *Enigma and the British code of honour* published in The Telegraph, June 2006 and located online at http://www.telegraph.co.uk/news/1521928/Enigma-and-the-British-code-of-honour.html

[xi] Quotation taken from http://archive.iwm.org.uk/upload/package/10/enigma/enigma14.htm

IMAGE CREDITS

Image of Duchess of Cambridge at Bletchley Park -
http://news.bbcimg.co.uk/media/images/75619000/jpg/_75619148_6du7mnin.jpg
Image of Herodotus - http://www.forbidden-history.com/images/herodotus.jpg
Image of scytale - http://upload.wikimedia.org/wikipedia/commons/5/51/Skytale.png
Image of Polybius square –
http://3.bp.blogspot.com/-QimKrREyRtY/T7MdntRDngI/AAAAAAAABcM/MXN1PGmZLrc/s1600/PolybiusSmall.jpg
Image of Al-Kindi - http://www.muslimheritage.com/uploads/Al_Kindi.jpg
Image of Tabula Recta –
http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4360089_orig.jpg?387
Image of Charles Babbage –
http://news.bbcimg.co.uk/media/images/55497000/jpg/_55497003_h4020548-charles_babbage,_english_mathematician-spl.jpg
Image of coded letter
http://drferris68.files.wordpress.com/2012/10/babington-plot-22bloody-letter22-jpeg.jpg
Image of Hebern machine - http://upload.wikimedia.org/wikipedia/commons/thumb/1/1a/Hebern1.jpg/320px-Hebern1.jpg
Image of Zimmerman telegram - http://www.firstworldwar.com/source/graphics/zimmermann_coded.jpg
Image of Enigma machine - http://upload.wikimedia.org/wikipedia/commons/3/3e/EnigmaMachineLabeled.jpg
Image of Y station - http://www.cryptomuseum.com/df/hro/img/YStation.jpg
Image of Bombes - http://www.cryptomuseum.com/crypto/bombe/img/us_bombe_full.jpg

BIBLIOGRAPHY

http://stegano.net/tutorial/steg-history.html
http://www.bbc.co.uk/history/people/alan_turing#p00chn46
http://www.nsa.gov/public_info/_files/cryptologic_quarterly/the_zimmermann_telegram.pdf
http://en.wikipedia.org/wiki/History_of_cryptography
http://www.machinae.com/crypto/herodotus.html
http://nrich.maths.org/2197
http://archive.iwm.org.uk/upload/package/10/enigma/enigma7.htm
https://libcom.org/files/[Arthur_Koestler]_Darkness_at_Noon.pdf
http://www.telegraph.co.uk/news/1521928/Enigma-and-the-British-code-of-honour.html
http://archive.iwm.org.uk/upload/package/10/enigma/enigma14.htm
http://www.smithsonianmag.com/history/document-deep-dive-what-did-the-zimmermann-telegram-say-29792028/?no-ist
http://www.archives.gov/education/lessons/zimmermann/
http://www.quadibloc.com/crypto/ro020301.htm
http://en.wikipedia.org/wiki/Friedrich_Kasiski
http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Kerckhoffs__principle.html
http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
http://en.wikipedia.org/wiki/Arthashastra#Internal_strife
http://en.wikipedia.org/wiki/Polybius_square
http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-27808962?print=true
http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html
https://securityblog.redhat.com/2013/08/14/a-brief-history-of-cryptography/
http://www.studentpulse.com/articles/41/a-brief-history-of-cryptography
http://www.childrenofthecode.org/Tour/c5/

