SIGNALS-"YOU HAVE A MESSAGE"

Sending a message

TECHNOLOGY drives how messages are sent

- **Visual signals 2,000 years ago**
- **Mechanical Age 18th - 19th century**
- **Electric-Mechanical Age 19th-20th century**
- **Electric-Valve Age 20th century**
- **Digital Age 20th-21st century**

sending a message

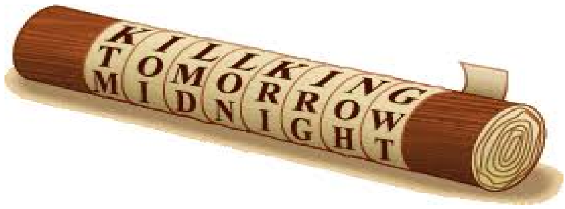
– Visual signals 2,000 years ago
– Mechanical Age 18th -19th Century
– Electric-Mechanical Age 19th-20th century
– Electric-Valve Age 20th century
– Digital Age 20th-21st century

Keep it Secret

Messages can be secret

2,700 years ago, Sparta, a Kingdom in Greece used the scytale (skitali). These were batons of a known diameter to pass secret orders and messages between the King and his commanders. It was described 800 years later by a Roman writer, Plutarch.

The King and Generals carried scytale with the same diameter. The King could wrap a leather strip around his scytale and write the message along the strip. The strip with the message would be removed and sent to the general, The general would wind the strip around his scytale to read the King's message.



In 404 BC a bloody and wounded messenger arrived at the palace of King Lysander of Sparta. He was the last messenger of 5 sent by a spy in Persia reporting that the King of Persia was planning an attack. The message was carried on the belt of the messenger and handed to the King. The King read the warning by wrapping the belt around his scytale.

The scytale was the 'key' to opening the Kings messages and commands, it was a symbol of command

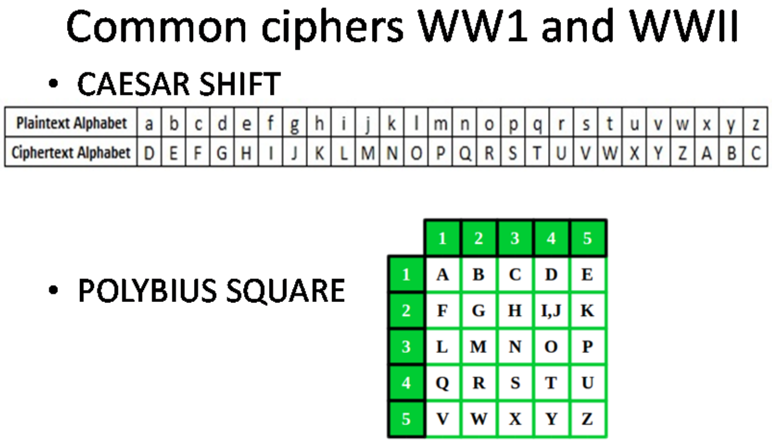
A statue of the **roman Emperor Domitian** 1st Century carrying a symbol of command. Today, the baton is still a symbol of military command and the passing of a baton a symbol of transferring authority.

The scytale with the jumbled letters is an early TRANSPOSITION CIPHER.

Common ciphers WW1 and WWII

2,000-year-old ciphers were as effective for the Romans and Spartans as they were for the Stormtroopers of 1918 and the German and British armies in 1939, or the Camp X Agents parachuted into Europe in WWII.

The most commonly used ciphers through time have been named after Julius Caesar and Polybius.



Common ciphers WW1 and WWII

- CAESAR SHIFT

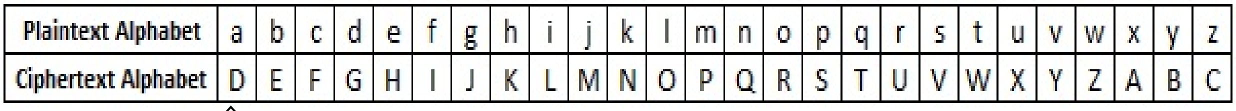
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- POLYBIUS SQUARE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

CAESAR SHIFT

Julius Caesar would send ciphers to his officers. He shifted the cipher alphabet by 3 spaces. ‘a’ becomes ‘D’ in the message and the preceding ABC shifted to the end of the ciphertext alphabet.



Plaintext Alphabet	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
Ciphertext Alphabet	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

⇧

Caesar shift can be used as a Code wheel and has been a tactical cipher from ancient times, through the American Civil War, through WW1 and WII and is still in use today. This is a TRANSPOSITION Cipher, meaning that the letters of the message have been transposed or rearranged, to create a jumble of the letters making an ANAGRAM. An anagram is a word or a phrase formed by rearranging the letters of a word or phrase. To read this message jumbled in the anagram you need to know the ‘KEY’ which is the number of letters the Caesar shift cipher been shifted. In this case the KEY is 3 letters, ‘D’=’a’ in the plain text of the message

POLYBIUS SQUARE

The Greek Polybius square 200BC is used for plain or ordinary text to be represented by a smaller set of numbers or that can be sent by telegraphy. In ancient times this would be by a water jar or by torches.

Using the Polybius square, letters can be substituted for numbers which can be hidden using Steganography by knotting string or putting knots into knitting to represent numbers as a SUBSTITUTION Cipher. Substituting or changing, letters into numbers.

The principle of the Polybius square was used by SOE and SIS Agents parachuted into France and Balkans in WWII. The German armies in 1918 used an adaptation as did the British and the German Armies in 1939 with the Double Playfair code. During the Vietnam War, American prisoners used the Polybius cipher for communicating with each other by tapping the numbers to each other from their cells.

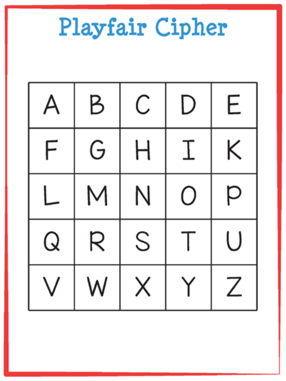
THE POLYBIUS SQUARE 200 BC had a significant impact in 1918. It was developed by Lt Fritz Nebel into the AFDGX Polybius square. A 5x5 code square ADFGVX Cipher-grid square. A two-phase code SUBSTITUTION and TRANSPOSITION. The letters were chosen because they sounded so very different in Morse Code.

The British and the allies also used a Polybius Square for associating numbers with letters in a tactical level code known as "Playfair. Invented by Charles Wheatstone in 1854 but named after his sponsor Lord Playfair.

Playfair

Playfair is a square but instead of encrypting a single letter, the Playfair substitution cipher uses pairs of letters (digraphs). Therefore, it is easier to use than the Vigenere cipher and because the letters are paired, harder to decrypt using frequency analysis, as there are more combinations of letters than the single letters in the alphabet. (60 digraphs rather than 26 alphabet letters).

Playfair was used as an easy, quick low-level code by the British in the Boer War; in WW1 and in WWII by the Australians, the British and the Germans. The German Army, Air Force and Police used a Double Playfair using a second square with jumbled letters for the second letter of each pair of letters.



Playfair Cipher

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

Playfair is a table of 5x5 letters usually using a keyword. To use Playfair:

Fill in the square with the keyword leaving out any duplicate letters, then fill in the remaining letters of the alphabet, and combine I and J. In our example the square is filled with the alphabet

Break the plain text message into two letter groups. The message is "grhkmy". "GR HK MY"

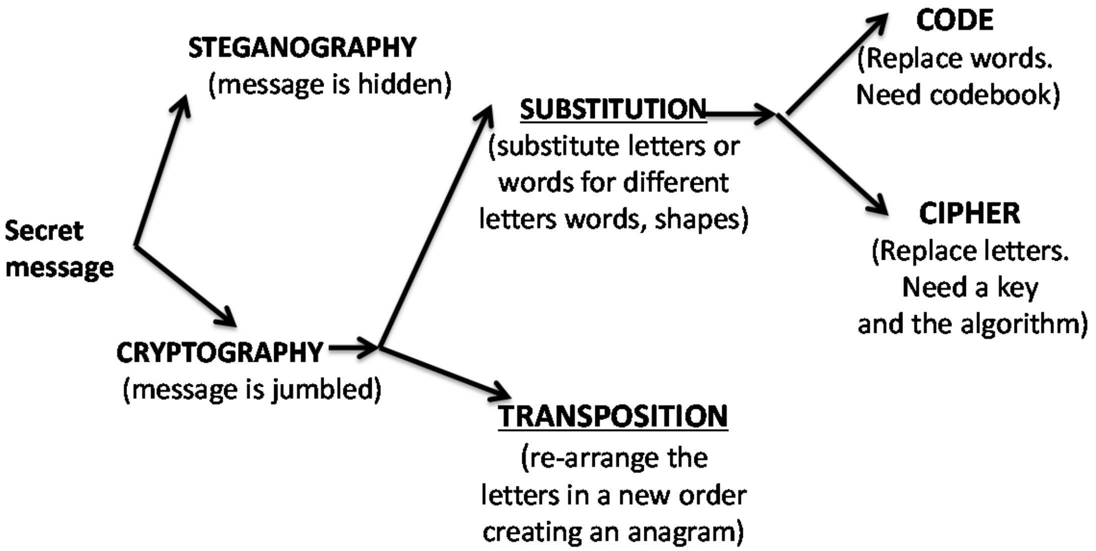
Encipher the letters by finding the letters in a **column line**; a **horizontal line** or in **a box**.

GR are found in the second **column** B-W. The letter below G is M. The letter below R is W. The cipher is RW

HK are found in the second **line** F-K. The letter to the right of H is I. The letter to the right of K wraps around and becomes F at the beginning of the same line.

MY are found in a **box** made up of the letters M-O and W-Y. Choose the opposite diagonals M becomes O and Y becomes W.

Keeping the message secret



Secret message

STEGANOGRAPHY
(message is hidden)

CRYPTOGRAPHY
(message is jumbled)

SUBSTITUTION
(substitute letters or words for different letters words, shapes)

TRANSPOSITION
(re-arrange the letters in a new order creating an anagram)

CODE
(Replace words. Need codebook)

CIPHER
(Replace letters. Need a key and the algorithm)

Keeping the message Secret

We want to send a secret message. The choices can be a single system or multiple systems. For example, we can transpose or shift the letters of the message using the Caesar shift. Then take a photograph of the message, reduce the photograph until it is very small and hide it in a document. We have used cryptography to encipher the message then Steganography to hide the message. Our message is double protected.

STEGANOGRAPHY. Derived from the Greek, **STEGANOS**-covered, to hide the message Staganos meaning covered, graphein meaning to write, therefore Steganography, means hidden writing.
In early times messages could be written in milk or urine, or written on the wood of a wax tablet then covered in wax disguising the message as a blank tablet. In 1941 the Allies discovered that German Agents were using microdots and concealing them in letters. The secret message was photographed and shrunk to the size of a single dot concealed in the letter. More recently Steganography is utilized with Least Significant Bit Insertion (LSB) where the message is broken into data bits and concealed into a picture and attached to an insignificant data bit.

CRYPTOGRAPHY. Derived from the Greek, **KRYPTOS,** the aim is not to hide the message but hide the meaning. Kryptos, meaning hidden and graphein meaning to write.

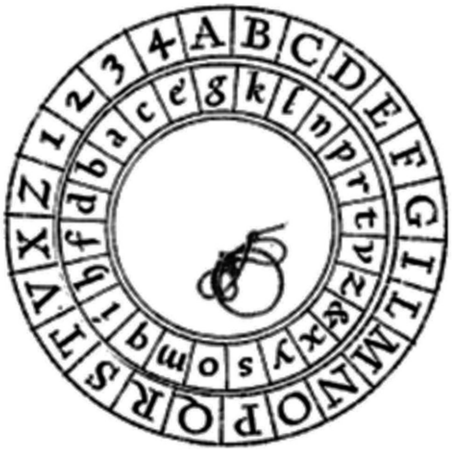
Cryptography may be used in:
TRANSPOSITION. Re-arrange the letters to create an anagram.
In ancient times the Spartan scytale transposed the letters. The key to reading the letter was the diameter of the baton. Later Julius Caesar by shifting the order of the letters created a cipher and the key was the number of the letters shifted.
SUBSTITUTION. Substitute the words or letters with different words or letters.
During the German wars a Roman garrison lead by Cicero was besieged by Germanic tribes. Caesar wrote a message letting Cicero know that help was on the way. Caesar substituted Latin for Greek script as Cicero could read Greek and the tribes were likely to understand Latin. The message was tied to a spear and thrown into Cicero's camp.

In Substitution cipher we can use:
CODES, agreed in a shared code for replacing the words in the message. Generally, codes are more secure than cipher because there are more words than there are letters. Therefore, a code is less vulnerable to Frequency Analysis. (a code breaking technique by counting the frequency of the letters in the cipher text). As in WWII with the ENIGMA codebooks distributed to the German U Boats the books were both a strength and a weakness once the code is captured.
In 1883 there was discussion about what was better Codes or Ciphers. As a result, a principal developed by KERCKHOFF is still used in modern Public Key Encryption. In a cipher text it is only necessary to protect the key rather than both the key and the algorithm. This is the basis of modern security today.

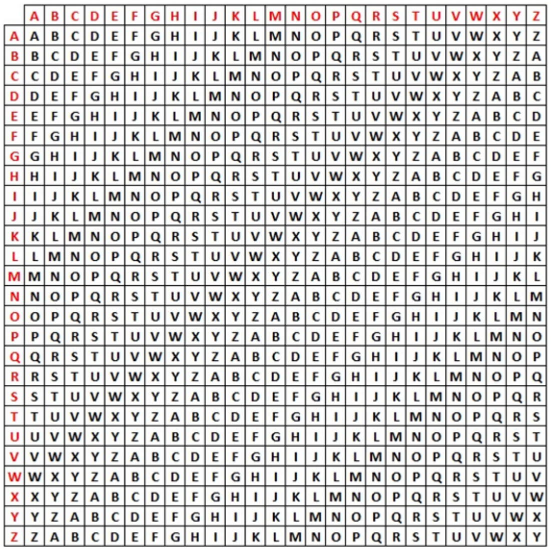
CIPHER. Replace each letter in the plain text alphabet with a letter or symbol using the cipher key. It is the key and the plain text that creates the algorithm. To read the algorithm you will need the key.

If you want to know more, I recommend THE CODE BOOK by SIMON SINGH

Keep the message secret


A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
g k l n p r t v z & x y s o m q i h f d b a c e

Alberti Wheel 1467



	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

Vigenere Cipher 1586

Alberti Wheel and Vigenere cipher

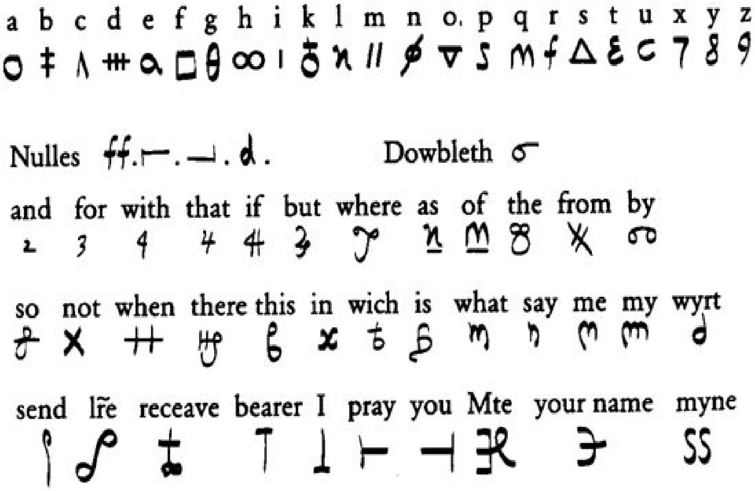
If you ever wondered where ENIGMA came from, this is its father. In 1467 **Leon Alberti** invented a poly alphabetic (more than one alphabet) cipher disc and code. The cipher wheel could be changed and also included numbers which could be mixed with phrases in a codebook. This offered a possible combination of a progressive cipher and a code. 500 years later the ENIGMA electro mechanical machine used a three-wheel progressive cipher that was later improved with a variety of code books.

The Vigenere cipher 26 alphabets like the Caesar cipher based on the letters of a KEY WORD and polyalphabetic substitution. First described in 1553 then attributed to Blaise de Vigenere. The Cipher became known as the Indecipherable Code and stayed unbroken for 300 years until 1854.

In 1854 **Charles Babbidge** deciphered Vigenere. However, Britain was at War with Russia in the Crimea and the government asked him not to publish his research. Russia placed faith in the Indecipherable code and the Government wished Babbidge to maintain this advantage and continue to break the Russian Vigenere cipher. Babbidge developed an Analytical Engine based on fundamentals that are considered the antecedent of what became known as the “Turing-Complete”. In 1863 a Prussian officer called **Kasiski** published a decrypt for the Vigenere. The Vigenere had the equivalent of 26 alphabets to encipher a message, whilst the early Enigma had three alphabet wheels and the Lorenz had twelve.

The Cipher of Mary Queen of Scots

- By the 15-16th century the City States of Europe increased diplomacy and coded messages. Use of frequency analysis began changing cryptography
- 1467 polyalphabetic cipher and disc
- 1506 Venice established a Cipher secretary.
- 1586 Vigenere developed the undecipherable cipher
- 1586 Queen Elizabeth's spymaster decoded the cipher of Mary Queen of Scots who was executed Feb 1587


a b c d e f g h i k l m n o p q r s t u x y z
Nulles ff. — . — . d.
Dowbleth
and for with that if but where as of the from by
so not when there this in wich is what say me my wyrt
send lre̅ receave bearer I pray you Mte your name myne

In the 15th-16th century civilizations moved towards becoming city states resulting in European wars. The City States of Europe increased diplomacy and the use of coded messages. The use of frequency analysis was copied from the Arab cryptographers and this changed cryptanalysis placing codebreaking as a weapon of diplomacy. Cypher rooms and Black Chambers were used by governments, kings and statesmen. This pattern of organised code breaking has not dramatically changed through to the present day. Key events were in 1467 when Leon Alberti invented the polyalphabetic cipher and disc. In 1506 Venice appointed Giovanni Soro as a cipher secretary. Soro was considered as one of the foremost codebreakers and his writings were followed by Francis Walsingham the spymaster for Queen Elizabeth of England.

In 1586 Blaise de Vigenere was attributed with creating the undecipherable cipher which was not broken for 300 years. Also, in 1586, Mary Queen of Scots was on trial for treason against her cousin Queen Elizabeth 1. Thomas Phelippes a codebreaker working for Francis Walsingham the spymaster for Queen Elizabeth, deciphered the messages of Mary Queen of Scots. Evidence against Mary was based on these messages and Mary was executed in Feb 1587. In an age of Spy Masters, monarchs had to exercise vigilance.

Black Chambers

The Black Chambers were Intelligence gatherers on an Industrial scale and by the 18th century the centre of cipher excellence was the Black Chamber in Vienna, Austria.

The Vienna Black Chamber had a strict timetable for gathering messages

7 am letters entering Austria are collected from the Post Office. Seals are melted off and the letters copied then translated.
10 am the letters are resealed and returned to the Post Office to be delivered to the Embassies.

10 am letters in transit through Austria arrive from the Post Office and the Intercept process begins again and the resealed letters are returned to the Post Office
4 pm letters leaving Austria from Embassies were received from the Post Office and the intercept process begins again.

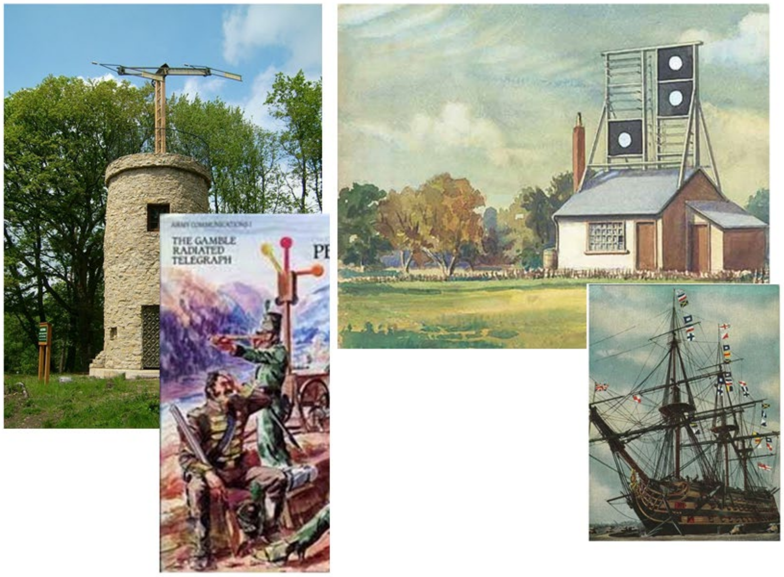
The intercept process had three parts
1. The envelope is opened and seal copied.
2. Message is copied and decoded.
3. The original letter replaced and envelope resealed in time to be placed back into the Postal system for delivery.
In 1774 the French embassy Secretary paid 1,000 ducats to the Vienna Black Chamber and received 2 secret information packages which he forwarded to Louis XV in Paris.

MECHANICAL AGE Telegraph Stations

Transitioning from the speed of a horse and a ship at sea, the telegraph cut messaging from weeks to days and even hours. Claude Chappe in 1792 had a telegraph system of moving mechanical arms across France.

Telegraph stations-

The Mechanical Age. 18th-19th century



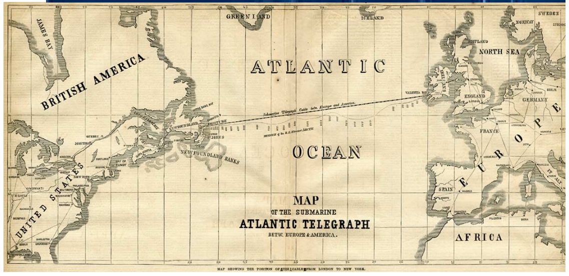
(Top left) Chappe telegraph station. (bottom left) a portable Telegraph of John Gamble. (Top right) a Murray Admiralty station (bottom right) HMS Victory with signals flying.

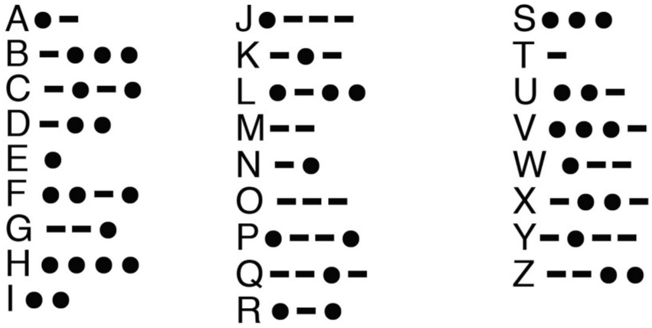
Telegraph stations were cutting edge technology at the end of the 18th century and Claude Chappe's telegraph system of moving arms was used across France to Venice and Strasburg. Napoleon used the 'Le systeme Chappe' for coordinating his armies. A message from Paris could reach Strasburg in 4 hours. A priority message such as the announcement of the birth of Napoleon's son was sent from Paris to Strasburg in 60 minutes.

By 1796 the Royal Navy had the Murray Admiralty telegraph system enabling messages from ships in the English Channel to be sent to Plymouth Naval Base and to London in 15 minutes. This system was too cumbersome for Field Armies until John Gamble developed the Radiated Telegraph used by The Duke of Wellington in Portugal and Spain.
The visual telegraph effectively ended in the 1840s as electronic telegraphy set up along the new railway lines began to take over.

Electric Telegraph and Morse Code

The Electric-Mechanical Age-19th-20th Century





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

Electro Mechanical Age 19th-20th century

Electric Telegraph and Morse Code

Between 1800 and 1824 the electric battery, and the Electro magnet had been invented.

By 1839 the Wheatstone and Fothergill Electro Magnetic telegraph ran its Telegraph cables 29 km along the new Railways.

Morse Code

John Vail and Samuel Morse developed the electro Magnet to send dots and dashes on to paper. The dots and dashes represented the letters of the alphabet. In 1851 there was a European form of Morse Code accepted internationally.

The Wheatstone and Fothergill Electro Magnetic telegraph used magnetized needles on a letter board that responded to pulses of electricity carried by cable. 1844 the birth of Queen Victoria's son, Prince Alfred was telegraphed from Windsor to the Times newspaper by the new telegraph.

The **Trans-Atlantic telegraph cable** had been laid by 1858 and Queen Victoria was able to send the first message to the American President.

Telegraph and Morse Code on the Battlefield

The Telegraph Cable carried messages across the world.

Delivering the message from the Telegraph to the battle field was still Visual Signals mainly by flags.

The war in The Crimea provided an opportunity for telegraph to connect governments with its armies deployed vast distances away. In 1854 a telegraph cable was dug from Lord Raglan's headquarters in the Crimea, 7 miles to the coast, then linked 547 km across the sea to the European mainland connecting Balaclava to Paris and London. General Simpson the Chief of Staff complained about the number of messages from London, "The confounded telegraph has ruined everything."

Where the Telegraph stopped, any communication was by courier, semaphore or by signal flags. In 1869 Henry Mance developed the signaling mirror into the Heliograph which was still issued to Canadian Signals units in 1941 and last used in conflict in 1967. It used a mirror and an oscillating mirror to reflect sunlight in short and long flashes to send Morse Code.

In the South African war with Telegraph and Heliograph a message could now be sent from London to Johannesburg in 4 days. In Canada Lord DunDonald, General Officer commanding the Canadian Militia was so impressed with the Heliograph that he reported.

"I would like to see heliographs brought into use, to enable me to signal my forces at a distance and I believe there should be established schools of instruction in signaling," On Oct. 24, 1903 Lord Dundonald, by Special General Order 167 created the Canadian Signaling Corps (Militia). This Canadian Militia unit was the first formed Signal unit in the British Empire. In Britain, the Corps of Signals was formed on 28 Jun 1920.