**Early History**

Caesar Cypher one of the first actual use of cryptography to hide messages.

"Caesar used it in order to   
if there was occasion for secrecy, he wrote in cyphers. The way to decipher those epistles was to substitute the fourth for the first letter, as d for a, and so for the other letters respectively." The Twelve Caesars 56.Gaius Suetonius Tranquillus

The Caesar cypher is of course a simple form of cryptography but as it was close to the first use of cryptography it didnt need to be too complex, and the Caesar Cypher was a form of substitution cypher and is even used today in the ROT123 method.

The Vignere cipher was similar to the Caesar cypher but was also the first use of an encryption key. Vignere Cypher was a Cypher first described in the book La cifra del, by Giovan Battista Bellaso in 1553 and then later misattributed to Blaise de Vigenère. The cypher was known to be extremely secure in the era of pen and paper cryptography and so earned the name "le chiffre indéchiffrable".

The Cypher worked using a square grid of alphabets, as shown here.

A close up of a newspaper

Description automatically generated

and a keyword as the encryption key. The encoder would write their message in plain text, and then repeat the keyword inline underneath until the lengths were equal.

|  |
| --- |
| thisisademonstration |
| pizzapizzapizzapizza |

The encoder would then check on the grid where the letter in the plaintext and in the keyword overlapped in the grid, and write down that letter in the encoded message. For example letter b in plaintext and letter p in the keyword would make q in the encoded message.

And the example shown above becomes.

IPHRIHICDMDVRSRPBHNN

**Cryptography and early computing**

The Enigma machine was another method of substitution encoding similar to that of the Caesar cypher. However using a mechanical machine a much more complex system could be developed from the same principles. The enigma machine had keys like a typewriter and a set of rotors which changed the letters being printed by the machine, these rotors moved after every keypress of the machine. This meant that the machines would have a different setting after each keypress making the message wnev more difficult to decode, if an identical machine was set to the same setting however the recipient would only need to type the received message into their own machine, the machine could also have different settings by swapping out rotors and using the plugboard and so had 158,962,555,217,826,360,000 possible settings.

The Bombe machine