History of Encryption

We live in a world where technology has improved so much to the extent that it has become a part of our everyday living. It has become so big that people are entrusting their personal data with technology. Encryption is used to protect data from falling into the wrong hands to be used maliciously. To encrypt information means to alter information using code or mathematical algorithms to be unintelligible to unauthorised readers (Dictionary.com, 2016).

Encryption began long before modern technology’s revolution. The earliest known use was words because most people couldn’t read so they wouldn’t comprehend the text hence the messages were confidential (Inquiries Journal, 2016). As civilisation happened, secrecy arose.

As civilisation started, encryption started to develop; the Egyptians used hieroglyphs, pictures used to represent words (Whitman and Mattord, 2003). The Greeks wrote their messages on tape wrapped around a stick of specific diameter so message was only eligible with a stick of similar diameter. Caesar ciphers were used by the Romans, which was when each letter being encrypted was replaced by a letter which was a certain chosen number of letters ahead in the alphabet, such as if the number chosen was 3, the letter ‘a’ would be replaced by the letter ‘d’ (Inquiries Journal, 2016).

In the early 20th century, a German engineer, Arthur Scherbius, created the Enigma machines which were a series of electromechanical rotor ciphers used to encrypt military communication during World War 2. The Germans were so confident that it was unbreakable, that they used it for all decisions made, so information gained would be considered as ultra-intelligence. With assistance of others, Alan Turing created a machine known as the Bombe which could crack the Enigma code and reveal the German secrets and essentially ended the war (Bbc.co.uk, 2016).

Now there are advanced encryption methods. Public key of cryptography which uses two keys, a public key to encrypt messages and private key to decrypt (Globalsign.com, 2016) and Digital Signature, which is a code which is attached to a document to verify its contents and the sender's identity (Oxford Dictionaries | English, 2016).

References:

1. Dictionary.com. (2016). the definition of encryption. [online] Available at: http://www.dictionary.com/browse/encryption [Accessed 16 Oct. 2016].
2. Inquiries Journal. (2016). A Brief History of Cryptography. [online] Available at: http://www.inquiriesjournal.com/articles/41/a-brief-history-of-cryptography [Accessed 16 Oct. 2016].
3. Whitman, M. and Mattord, H. (2003). Principles of information security. Boston, Mass.: Thomson Course Technology.
4. Inquiries Journal. (2016). A Brief History of Cryptography. [online] Available at: http://www.inquiriesjournal.com/articles/41/a-brief-history-of-cryptography [Accessed 16 Oct. 2016].
5. Bbc.co.uk. (2016). BBC - History - Enigma (pictures, video, facts & news). [online] Available at: http://www.bbc.co.uk/history/topics/enigma [Accessed 18 Oct. 2016].
6. Globalsign.com. (2016). What Is Public-Key Cryptography?. [online] Available at: https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/ [Accessed 19 Oct. 2016].
7. Oxford Dictionaries | English. (2016). digital signature - definition of digital signature in English | Oxford Dictionaries. [online] Available at: https://en.oxforddictionaries.com/definition/digital\_signature [Accessed 20 Oct. 2016].