No interpreter required

Description

If only people speaking different languages could communicate without the need of an interpreter. Iâ??m thinking of the Trump-Putin encounters with translators present. Only unscrupulous leaders would bar their translators from disclosing to other trusted officials what was said.

But Iâ??m also thinking of Leon Battista Albertiâ??s justification of his cipher technique, which was to enable confidential communication between rulers â?? without the need of interpreters.

> â??I can justly consider this cipher worthy of sovereigns, who can use it quite easily, with little effort and without being encumbered by use of an interpreterâ?• (180).

Of course, in this case those in communication are many miles apart, share the same language, and the interpreter is a functionary who would receive a coded message and had the equipment and the knowledge to decode it and pass the translation on to the sovereign. Albertiâ??s cipher wheel was so simple that even a king could use it.

Couriers and interpreters lived dangerous lives, not least for the secrets they knew. Human translators canâ??t easily have their memories erased, but easy-to-use translation machines reduce the risk of message leakage from a circuit of human intermediaries.

Polyalphabetics

Albertiâ??s cipher wheel looked something like this, providing a simple equivalence mapping between letters of the alphabet.

He used the Latin alphabet, and excluded a few letters as well, perhaps for symmetry (24 â??housesâ?•). According to a helpful YouTube clip by *Ciphertown*, the cipher disk user would represent H with two Fs, J with two Is or similar secondary coding. Iâ??ll restrict myself to Albertiâ??s character set here to encode the simple communication:

AM I A PVPPET

With the disks in the position shown above that would result in a simple one-to-one mapping between characters. As long as you know how to align the two disks you could convert the secret message above to

g& v g shhpi

With the same cipher disk design and alignment the receiver could decode that back to the original message. But thatâ??s also relatively easy for a cryptanalyst to decipher, especially with a longer message, considering letter frequency, something about the context, and iteration through combinations.

Cipher++

Hereâ??s another encryption that is more difficult to decode using the same disk design, and knowing that the letter â??gâ?• is to serve as an indicator:

Ag& v g Cxxlm

The appearance of the letter A means align g on the inner disk with A on the outer disk. Taking each letter at a time, when the decoder encounters the upper case letter C she/he rotates the inner disk to align g with C to give a different set of mappings. The coder can insert such rotation cues throughout a long message. That would make it extremely difficult for an intercepting cryptanalyst to decode the message.

Shifting the index

Itâ??s simple really, and there are elaborations on the method to make code breaking even more difficult. Alberti described the shift in alignment â??changing the indexâ?•, and the family of such methods of shifting the alphabetical ordering at different points in the message is now called *polyalphabetic encryption*.

The WW2 German Enigma machine belonged to the same family of encryption machines, the method that eventually was broken by the cryptanalysts of Bletchley Park. See post: Phone hacking enigmas.

References

- Alberti, Leon Battista. 2010. De Componendis Cifris. In Kim Williams, Lionel March, and Stephen R. Wassell (eds.), *The Mathematical Works of Leon Battista Alberti*: 169â??187. Basel: Springer Basel.
- Ciphertown. 2015. How to Use the Alberti Cipher Disk device with Method 1. *Youtube*, 1 November. Available online: https://www.youtube.com/watch?v=4mNRU7h9Q_o (accessed 16 January 2019).
- DuPont, Quinn. 2017. The printing press and cryptography: Alberti and the dawn of a notational epoch. In Katherine Ellison, and Susan Kim (eds.), *A Material History of Medieval and Early Modern Ciphers*: 95-117. London: Routledge.
- Miller, Greg. 2019. Trump has concealed details of his face-to-face encounters with Putin from senior officials in administration. *Washington Post*, 13 January. Available online: https://www.washingtonpost.com/world/national-security/trump-has-concealed-details-of-his-face-to-face-encounters-with-putin-from-senior-officials-in-administration/2019/01/12/65f6686c-1434-11e9-b6ad-9cfd62dbb0a8_story.html?noredirect=on&utm_term=.66249f1bd7b9 (accessed 17 January 2019).

Note

- See creative commons license for the above image, modified/rotated by the author.

Category

1. Architecture

Tags

1. blockchain
2. cipher
3. ciphercity
4. encryption

Date Created
January 19, 2019
Author
rcoyne99