Algologic Technical Report # 2/2013

The Indian roots of cryptography

S. Parthasarathy
drpartha@gmail.com

Ref.: cryptoroots.tex
Ver. code: 20130723a

Abstract

Most books on cryptography invariably include the Caesar's cipher as an example of substitution cipher. It is strange that they all ignore, or are unaware of another substitution cipher which was in use a few centuries before Caesar's cipher.

1 The Indian roots of cryptography

This note is a sequel to my article [2] about the dramatis personae of cryptography. The article, provoked a world-wide reaction. In fact, a related Google search resulted in over 6 million hits, making me a kind of celebrity !

Most of the reaction was just a hollow ball of cynical comments, based on irrelevant, incoherent and puerile arguments. The reaction clearly smacked of snobbism, xenophobia, and a false sense of supremacy. For those who care to be more reasonable and logical, here is some more evidence to strengthen the proposal I made earlier in my article about Sita and Rama: According to [1] *Cryptography is recommended in the Kama Sutra (ca 400 BCE) as a way for lovers to communicate without inconvenient discovery.*

The Signal Corps Association [3], gives an interesting explanation of the kama sutra cipher. *The kama-sutra cipher is a classical substitution cipher described in "Kama-sutra", a text written in the 4th century AD by the Hindu Brahmin scholar Vatsyayana, but based on manuscripts dating back to the 4th century BC. The Kama-sutra recommends that women should study 64 arts, including cooking, dressing, massage and the preparation of perfumes. The*

list also includes some less obvious arts, including conjuring, chess, bookbinding and carpentry. Number 45 on the list is mlecchita-vikalpa, the art of secret writing, advocated in order to help women conceal the details of their liaisons. One of the recommended techniques involves randomly pairing letters of the alphabet, and then substituting each letter in the original message with its partner. Thus, we infer that the kama sutra cipher (400 BCE) precedes by several centuries, the Caesar cipher, which is attributed to Julius Caesar (100 BCE to 44 BCE).

It is time to accept and realise the facts, and let Alice and Bob go on their well-deserved holiday [2]

2 Concluding remarks

This is a LaTeX document, created under Linux, using Kile. You can get the LaTeX source of this document from `drpartha@gmail.com`. Please mention the Reference Code, and Version code, given at the top of this document.

If you found this article useful, please send a note to `drpartha@gmail.com` As always, constructive comments and suggestions are always welcome.

References

[1] Wikipedia, `http://en.wikipedia.org/wiki/Cryptography\#cite_note-kama-10`

[2] S. Parthasarathy, `http://profpartha.webs.com/publications/alicebob.pdf`

[3] Signal Corps Association `http://www.civilwarsignals.org/cipher/kamasutra.html`

[4] Creative Commons By Attribution - NonCommercial - ShareAlike 3.0 Unported License. `http://creativecommons.org/licenses/by-nc-sa/3.0/deed.en_US`

***