Algologic Technical Report # 2/2013

The Indian roots of cryptography

S. Parthasarathy
drpartha@gmail.com

Ref.: indianroots.tex
Ver. code: 20240205g

Keywords : Alice, Bob, Sita, Rama, Vatsyayana, Kamasutra, Hemachandra, Fibonacci, Hindu, Arab, Numeral, Ramanujan, Agarwal, AKS, IITK

Abstract

This note is a sequel to my article [3] 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 ! 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.

1 The Indian roots of cryptography

1.1 Alice and Bob can go on a holiday

Almost every book on cryptography begins with the statement *Alice wants to send a message to Bob* and builds up on all the efforts needed to succeed in this mission. Alice and Bob are just two fictitious characters created for convenience to write a story. Our approach is to create a narration starting with *Sita wants to send a message to Rama*. The article [3] about Alice and Bob, talks about a meaningful alternative to the traditional dramatis personae of cryptography.

Figure 1: Hanuman meets Sita

The statement *Sita wants to send a message to Rama* is inspired from the episode in [2] *Sundara Kanda* (lit. beautiful book) of the Ramayana, where Sita, who was kidnapped by Ravana, is isolated and kept confined to a forest. She is seated under an ashoka tree, when the monkey-God Hanuman, sent by Rama, reaches her. Desperate Sita wants to send a message to Rama through Hanuman (honest man). We also have the usual man-in-the-middle Ravana (rogue), who is waiting to sabotage any communication between Sita and Rama. In addition to the aptly chosen names (Sita=sender, Rama=receiver), this entire episode has some striking similarities to modern cryptography. This choice is very effective in teaching cryptography, because the Ramayana story is widely known, and is retained in memory easily for a longer time (personal experience of the author, who teaches cryptography regularly). For more details on this approach, please see [3].

The author came across many situations when contributions by India are unfairly understated or ignored completely by the cryptography community. We take a quick look at some India-based resources related to cryptography . One remarkable exception is the book by Kim Plofker [16], a well-documented book which is free of bias and exaggeration.

1.2 Kamasutra comes to help

Most books on cryptography invariably include the Caesar's cipher as an example of substitution cipher. It is strange that everybody ignores, or is unaware of another substitution cipher which was known, a few centuries before Caesar's cipher. According to [1] *Cryptography is recommended in the Kama Sutra (ca 400 BCE) as a way for lovers to communicate without inconvenient discovery.* Notice that the Hindu book Kama Sutra is primarily a book of erotism and love making [22].

The Signal Corps Association [4], 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, book-binding 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 secret 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).

How come, this historically-proven fact finds no mention in books on cryptography ?

1.3 Hindu-Arab numerals

It is a well-known fact [11] that cryptology depends heavily on arithmetic and number theory. The origins of today's number systems can be traced to the Hindu/Indian mathematician Aryabhatta (476 – 550 CE). Subsequently, an Arab-Persian by name Abu Jafar Mohammed Ibn Musa Al Khowarizmi (aka Al Khowarizmi) travelled to India, and wrote a small book around 820 CE explaining the Indian numeral system. This book surfaced in Spain at about 1100 CE and resulted in the popularisation of what came to be known as the *Hindu-Arab numeral system* [12]. The place-valued number system, based on the ten decimal symbols had its origins in India.It is interesting to note that this system is known as the Arabic numeral system in India, whereas it is called as Hindu numerals, in the Arab world. This fundamental contribution, along with the concept of "shoonya" (zero) [14], also discovered

in India [7], has made modern day cryptology possible. Rather than use zero as just a place marker, the Hindu shoonya was considered a number, with all fundamental arithmetic operations defined over it.

1.4 Number Theory

India was the birth place of the famous mathematician S. Ramanujan whose contributions to number theory are very well known [6]. Unfortunately, Ramanujan [19] died very young, with much of his work left unpublished [13].

Continuing this remarkable trend, a research group at IIT Kanpur, recently made a breakthrough contribution of fundamental importance to prime numbers and cryptography [9].

1.5 Hemachandra and Fibonacci

Yet another example of indifference to Indian mathematical contributions is the case of Hemachandra [15]. Hemachandra (1089-1173) [18] discovered the famous numbers series, commonly called as Fibonacci series, at least a good 50 years before Fibonacci (1170-1250). Fibonacci numbers and the Fibonacci series find prominent mention in the number theory literature. But there is practcally no mention anywhere about a similar series found almost a century earlier by a Hindu/Jain monk – Hemachandra. About 50 years earlier than Leonardo Pisano Fibonacci (1170-1250) , Hemachandra (1089-1173) counted the number of ways a line of poetry can be composed of short syllables of length 1 and long syllables of length 2. A line of length 1 can only be a short syllable; one of length 2 either two shorts or 1 long; etc. The same sequence 1, 2, 3, 5, 8, ... results. Apparently Gopala had studied these numbers in about 1135, other Indian mathematicians as early as the 7th century, and perhaps even Pingala, the author of the Chandastra, centuries before that. Sadly, even books written by Indian authors make no mention of this fact.

It is time to set the records straight. All prospective authors from the Indian sub-continent should make necessary changes to the books related to cryptography (and mathematics) they are planning to write.

2 Concluding remarks

This article is very incomplete. It cannot fully measure all the contributions made by Indian mathematicians. But it is a fitting response to the xenopho-

bic and puerile comments made by ill-informed readers to a proposal, made earlier by this author [17]. Also take a look at the contrasting comments made by a Professor of Mathematics [20].

This article is the transcript of an invited lecture given at Queensland University of Technology, Brisbane, Australia. It is also part of the cryptography course conducted by the author in Kathmandu University, Nepal [21].

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.

This article, and several other articles on crytography are available for download, from the author's website [10] .

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

This document is released under a Creative Commons By Attribution - Non Commercial - ShareAlike 3.0 Unported License. See[5]

References

[1] Wikipedia, http://en.wikipedia.org/wiki/Vatsyayana_cipher

[2] Wikipedia, Sundara Kanda, http://en.wikipedia.org/wiki/Sundara_Kanda

[3] S. Parthasarathy, Alice and Bob can go on a holiday, https://drpartha.org.in/publications/alicebob.pdf

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

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

[6] Paul Erdős, Ramanujan and I, Resonance Volume 3, Issue 3, pp 81-92, March 1998.

[7] AMS, All for Nought, http://www.ams.org/samplings/feature-column/fcarc-india-zero

[8] Wolfram, Ramanujan Prime, http://mathworld.wolfram.com/RamanujanPrime.html

[9] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, PRIMES is in P, www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf

[10] S. Parthasarathy, Downloadable documents on cryptography, http://drpartha.org.in/publications/downloadcrypto.htm

[11] M Waldschmidt, Arithmetic and cryptography, Resonance,Vol. 13, No. 5, May 2008.

[12] T. Padmanabhan, Indo-Arabic numerals, Resonance,Vol. 15, No. 12, Dec. 2010.

[13] K.G. Ramanathan, The unpublished manuscripts of Srinivasa Ramanujan, Resonance,Vol. 15, No. 2, Feb. 2010.

[14] Wikipedia, Indian mathematics, http://en.wikipedia.org/wiki/Indian_mathematics

[15] Hemachandra vs Fibonacci, https://www.quora.com/Why-do-we-credit-Fibonacci-and-not-Hemachandra-for-the-series-that-Hemachandra-invented-100-years-before

[16] Kim Plofker, Mathematics in India, Princeton University Press, 2008, (ISBN-13: 978-0691120676)

[17] S. Parthasarathy, Alice and Bob can go on a holiday !, Algologic Technical Report 11/2012. July 2013.

[18] Wikipedia, Hemachandra (1089-1173) https://en.wikipedia.org/wiki/Hemachandra

[19] S. Parthasarathy, Remembering Ramanujan https://drpartha.org.in/drpartha/ramanukumbak.htm

[20] Mira Bhargava, Only a leader can notice a leader, https://drpartha.org.in/profpartha/mirabhargava.htm

[21] S. Parthasarathy https://drpartha.org.in/profpartha/cryptokath.htm

[22] Wikipedia, Kama Sutra,
https://en.wikipedia.org/wiki/Kama_Sutra

***