Algologic Technical Report # 11/2012

Alice and Bob can go on a holiday !

S. Parthasarathy
drpartha@gmail.com

Ref.: alicebob.tex
Ver. code: 20130719b

Abstract

Any book on cryptography invariably involves the legendary characters Alice and Bob. It is always Alice who wants to send a message to Bob. This informal article replaces the traditional dramatis personnae of cryptography, with characters drawn from Hindu mythology.

Contents

1 Alice and Bob

Any book on cryptography invariably involves the characters Alice and Bob [1]. It is always Alice who wants to send a message to Bob. We also encounter another couple: Carol and Dave. And then, we also have evil Eva (the eves-dropper), malicious Mallory and rude Rudy (the intruder). Apart from the alphabetic order of their names, we see little or no connection to cryptography in their names. We will now see a smarter alternative to these characters.

[1]This is a LaTeX document. 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

Alice and Bob have been around for many years. Using the fictititious characters Alice and Bob does make it easy to explain and understand certain tricky concepts in cryptography. Many of us (including the author of this article) have grown up learning cryptography with Alice and Bob. In fact, Bruce Schneier, the renowned crypto guru, immortalizes these characters in a video lecture available on Youtube [2].

2 Enter Sita and Rama

For several years, I have been using a very different set of characters, to introduce cryptography to my students : enter Sita and Rama. Sita and Rama are the two central characters in the Hindu mythological epic Ramayana [5]. The Alice and Bob story can now be re-scripted as: *Sita wants to send a message to Rama*

The statement *Sita wants to send a message to Rama* is inspired from the episode in [3] *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, 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).

This choice makes more sense, because :

- Sita and Rama have very strong reasons to communicate with each other.
- The above episode symbolises the difficulties in sending important and confidential messages through a hostile environment. The sender Sita, and the receiver Rama, are separated by a hostile environment. They can trust nobody, and have to take a lot of precautions.
- The first letters of their names S (**S**ita) and R (**R**ama) hint at sender and receiver respectively.
- Hanuman (honest man) is the trusted medium for carrying the message.

- Badmash (bad man) is the mailicious man-in-the-middle. We propose Badmash (lit. bad man), although he is not part of Ramayana. The real name of the villain: Ravana, is a bad choice, since the first letter (R) of the name, can be confused for Receiver [2].

- Hanuman is known to be a strong person. We need a strong (secure) medium to transmit our messages.

- Hanuman is famous for his devotion to Rama and Sita. The medium we choose must be trustable.

- Hanuman is often tactful and can change his appearance and shape (and even become invisible). The medium should be intelligent, to conceal and protect messages under its custody.

- Hanuman can fly, and avoid obstacles in his way. This is a quality we expect of the medium (or the method adopted to transmit messages).

In addition to the above, we find some more striking similarities to concepts used in modern cryptography.

- When Hanuman approaches Sita and presents himself as Rama's emissary, Sita does not believe him. She asks him to prove his credentials. Hanuman does this by presenting the ring which Rama usually wears [5]. This may be compared to a digital certificate.

- In modern public key cryptography, the sender needs the receiver's public key to send a confidential (protected / encrypted) message. Sita uses an entity (person) sent by Rama.

- When Sita gives her message for Rama, to Hanuman, she has to authenticate the message. This is

[2]Based on a comment in Bruce Schneier's blog dated 27 Sept. 2012 [4]

necessary to assure Rama that it is not a spurious message from an impostor pretending to be Sita. She does this, by giving Hanuman her *choodamani* (a jewel which Hindu women wear on their head hair). This is comparable to a digital signature.

For those who do not know Ramayana: The above story has a happy ending. Rama gets the message sent by Sita. He now knows where Sita is, and invades Lanka (Ravana's kingdom). Ravana is killed, and the Sita – Rama couple is united. Amen.

Alice and Bob can now go on their much deserved (and delayed) holiday !

3 Concluding remarks

Cryptography is a fairly complex subject. The number of entities involved, and the strategies they adopt are not easy to visualise. Teaching such a subject can be challenging, and requires the use of some innovative approaches and props. The "Alice and Bob" approach has a much better and more effective alternative : the "Sita and Rama" approach. Other things being equal, the choice of props with some symbolic relationship to cryptography is much more effective than props with randomly chosen names like Tom, Dick and Harry. In fact, one humorous but sensible proposal which was made, stated *Shamir wants to send a message to Rivest*. It is only a matter of personal choice and preference. Of course, analogies often involve some amount of exaggeration and distorsion and limitations, and so, should be used with caution.

Some people who read the first version of this article (originally published in August 2012), seemed to have issues with using Hindu names, adding a religious and xenophobic flavour to the conversation. This is a point of view, which the author prefers to ignore. A sequel to this article will demonstrate that cryptography has roots in ancient India (ca 400 BCE) [7]

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] Bruce Schneier, Applied Cryptography, Pub.: John Wiley & Sons, 1996 ISBN 0-471-11709-9

[2] Bruce Schneier - Who are Alice & Bob? YouTube Video `http://www.youtube.com/watch?v=BuUSi_QvFLY`

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

[4] Bruce Schneier, Schneier on Security – A blog covering security and security technology, `http://www.schneier.com/`, Sept. 2012.

[5] The Ramayana at Syracuse University South Asia Center `http://sites.maxwell.syr.edu/ramayana/toc.html`

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

[7] S. Parthasarathy, The Indian roots of cryptography (to be published shortly)

***