Network Security Project – Proposal

Nicholas Capo - Nicholas.Capo@Gmail.com

January 25, 2012

1 Proposal

To develop an implementation of the Serpent-1 Cipher [3][1] in `C` and `Python`.

Both implementations of the cipher shall be constructed using threads to take advantage of the parallelism of the Serpent Algorithm. The number of threads to be used (up to a limit) shall be specified at runtime.

Each implementation shall be cipher-text compatible with each other and also the reference implementations [2].

References

[1] Ross J. Anderson. *Serpent Home Page*. [Online; accessed 26-January-2012]. URL: https://www.cl.cam.ac.uk/~rja14/serpent.html (cit. on p. 1).

[2] Frank Stajano. *Serpent reference implementation*. [Online; accessed 26-January-2012]. URL: https://www.cl.cam.ac.uk/~fms27/serpent/ (cit. on p. 1).

[3] Wikipedia. *Serpent (cipher) — Wikipedia, The Free Encyclopedia*. [Online; accessed 26-January-2012]. 2012. URL: http://en.wikipedia.org/w/index.php?title=Serpent_(cipher)&oldid=469573199 (cit. on p. 1).