RSA Algorithm
Algorithm Analysis

Geovanny Burgos Retana
Computer Engineering Student
Instituto Tecnologico de Costa Rica
San Jose, Costa Rica
Email: geoburgosretana@gmail.com

Anthony Leandro
Computer Engineering Student
Instituto Tecnologico de Costa Rica
Limon, Costa Rica
Email: Anthonylle@hotmail.com

Bryan Mena Villalobos
Computer Engineering Student
Instituto Tecnologico de Costa Rica
Heredia, Costa Rica
Email: mena97villalobos@gmail.com

***Abstract*—The abstract goes here.**

1. Introduction

RSA algorithm, first published on 1977 by Ron Rivest, Adi Shamir, and Len Adleman, is a public-key cryptosystem, in this days, often used in various web servers, browsers and commercial system to protect web traffic among some other things like email encryption In this type of cryptosystem the encryption key and the decryption key are different also, the encryption is public while de decryption key is private. This cryptosystem is base on the difficulty of factoring to prime large numbers.

2. The Algorithm

Taking the words of Weisstein, E RSA encryption defines as "A public-key algorithm which uses prime factorization as the trapdoor one-way function",

2.1. Before RSA

RSA, in a certain way, was the first implementation of public key encryption but as seen in ***The history of Non-Secret Encryption*** by J.H. Ellis public key encryption was long before been developed, in 1970 J. H. Ellis conceive a non-secret digital encryption(today known as public key encryption), in this time Ellis couldn't see a way to implement this type of encryption but in 1973 an employee of GCHQ came with the basic idea of RSA encryption base on Ellis work, but, as the new techniques discover on GCHQ that are potentially harmful, by definition, are classified information, this implementation was kept on secret.

2.2. Actual panorama

With the breakthrough in quantum computers is known that Shor's algorithm broke a 768-bit key (usually key sizes variate from 1024 to 4096 bits), this give us an idea of how quantum computers may change our way of thinking

3. Methodology

Bla bla bla

4. Experiments

as

5. Analysis and Results

The analysis goes here

6. Conclusion

The conclusion goes here.

References

[1] Boneh, D (November, 1998). Twenty Years of Attacks on the RSA Cryptosystem, Retrieve from: http://crypto.stanford.edu/ dabo/pubs/papers/RSA-survey.pdf

[2] Ellis, J.H. (January, 1970). The possibility of secure non-secret analogue encryption, Retrieve from: http://cryptocellar.org/cesg/possnse.pdf

[3] Ellis, J.H. (May, 1970). The possibility of secure non-secret analogue encryption, Retrieve from: https://www.gchq.gov.uk/file/cesgresearchreportno3007pdf-2

[4] Ellis, J.H. 1987. The History of Non-Secret Encryption. Retrieve from: https://web.archive.org/web/20130404174201/ https://cryptocellar.web.cern.ch/cryptocellar/cesg/ellis.pdf

[5] Weisstein, Eric W. "RSA Encryption." From MathWorld–A Wolfram Web Resource. Retrieve from: http://mathworld.wolfram.com/RSAEncryption.html

[6] R.L.Rivest, A.Sharmir, L.Adleman: A method for obtaining digital signatures and public key Cryptosystems, Tata McGraw-Hill Retrieve from: http://people.csail.mit.edu/rivest/Rsapaper.pdf

[7] Williamson, Malcolm J. (January 21, 1974). Nonsecret encryption using a finite field. Retrieve from: https://www.gchq.gov.uk/sites/default/files/document_files/ nonsecret_encryption_finite_field_0.pdf