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 is defined as "A public-key algorithm which uses prime factorization as the trapdoor one-way function". Given the formula $(m^e)^d \equiv m(modn)$ the principle behind RSA is that is easy to find e, d, n such as the formula is true, but is very difficult even impossible, finding d, even knowing m, e, n. As mention before RSA consists of a public key and a private key, public key is used to encrypt and private key is used to decrypt the message in a reasonable time, from the formula given before, public key is represented by the integers e and n, and, the private key, is represented by d this led us with m, m represents the message to encrypt

2.1. How RSA works?

First of all, we imagine that two individuals wants to exchange an encrypted message with RSA, P_1 has a public and a private key, P_1 shares the public key with P_2 when P_2 has the key he proceed to encrypt the message and send it to P_1, is important to clarify that only P_1 has the private key wich is used to decrypt the message, encryption and decryption process are describe below.

2.1.1. Encryption. In encryption process the first step to follow is to turn M (message to send) into an integer m, such that 0 m ¡ n in this step RSA uses a protocol such as the integer m will not felt into a range of integers that isn't secure. After this computing c (encrypted message) will be easy, using Alice's public key e as the following: $c \equiv m^e \pmod{n}$

2.1.2. Decryption. Decryption is as easy as to use the private key d in the following way:
$c^d \equiv (m^e)^d \equiv m \pmod{n}$
This way the message is recovered with the private key

2.2. 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.

2.3. 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 and what a break-out it would be since almost every of our actual encryption methods are base on prime number's difficulty to be generated

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