A Performance Test On Symmetric Encryption Algorithms - RC2 Vs Rijndael

Neeraj Anand Sharma, Mohammed Farik

Abstract: Cryptography is one of the most integral components when trying to maintain achieve a secure communication medium and determining the best cryptography algorithm is as important as having a secure communication. In this paper, we will find out the two superlative symmetric cryptography algorithms available and used nowadays. Then, observe which algorithm is better than the other and finally give some recommendations based on the results achieved. This will surely narrow down the options as to which algorithm to choose when trying to achieve a secure communication.

Index Terms: Algorithm, Brute-Force, Cipher, Ciphertext, Cryptography, Decryption, Encryption, RC2, Rijndael, Rivest.

1 Introduction

Is it safe to transfer money online from one account to another? Is it safe to make a purchase online? Is it safe to communicate with someone over the internet and exchange personal information? Nowadays, security is an important aspect of the society and there are so many hackers trying to constantly breach communications between party A and B. To avoid hackers from constantly trying to breach and interfere, systems are now using cryptographic algorithms to maintain a secure channel. In this paper, we will examine the two best symmetric encryption algorithms available and are used currently with software's that has the capability to send and receive messages. The two algorithms are RC2 and Rijndael (AES). We will test these two algorithms using brute-force attack tools to determine which is better than the other. Factors tested will be the bit used (key length) and the time it takes to retrieve the message via the means of brute-force attack tools. The above-mentioned tests will be carried out on i7 Laptop, i7 Desktop, and Xeon Server. The sections discussed in this paper are as follow, first we will discuss the concept of cryptography, followed by secret key cryptography, then the two algorithms (RC2 and Rijndael) are discussed, then the experimental design, then results will be discussed, followed by recommendations, and finally, the conclusion.

2 Literature Review

2.1 Cryptography

Cryptography is referred to as cryptology and it is the study of techniques to achieve a secure communication between the presences of a third party who are also usually referred to as adversaries.

Cryptography is a 'Greek' word and it means hidden secret and was first used in 1900 B.C. by an Egyptian scribe who used some non-standard hieroglyphs (pictures, symbols, and ideograms) in an inscription [1-3]. William Stallings defines cryptography as "the type of operations used for transforming plaintext to ciphertext, the number of keys used, and the way in which the plaintext is processed" [3]. Cryptographic systems are usually generalized into the above three individual dimensions. Moreover, cryptography is about creating and analyzing protocols that will eventually prevent third parties or the public from retrieving and reading private messages. Currently, there are five main characteristics of cryptography today, these include privacy/confidentiality, authentication, integrity, non-repudiation, and key exchange [3, 4]. The first characteristic deals with ensuring only the intended receiver can read the message and no one else. The second characteristic deals with authenticating or proving a person's identity to see whether it is the right person or not. The third characteristic deals with the assurance of the correct message received by the receiver and that it has not been altered in any way. The fourth characteristic acts as a mechanism to prove to the receiver that the sender correct sender has sent that message. The final characteristic involves a method where the crypto keys are shared between the sender and receiver. Furthermore, cryptography starts with a series of unencrypted set of data which is known as a plaintext. The plaintexts are encrypted into ciphertext using cryptography algorithms and sent to the receiver. The receiver will be required to decrypt the ciphertext first in order to view the plaintext. The encryption of plaintext and decryption of ciphertext will depend on the type of cryptography scheme used and also depend on some form of the key used with the plaintext. Cryptography algorithms usually use mathematical formulas to encrypt and decrypt [1]. The formula for the process is typically in the form as written below:

Encryption: Ciphertext = Encryption MethodKey (Plaintext)
Decryption: Plaintext = Decryption MethodKey (Ciphertext**)**

There are many types of cryptographic algorithms nowadays, and are categorized as, secret key cryptography (SKC), public key cryptography (PKC), and hash functions [1, 3]. SKC is also known as symmetric encryption where it uses a single key for both encrypting and decrypting of plaintext and is mainly used for maintaining privacy and confidentiality. PKC is also known as asymmetric encryption where it uses two separate keys, one for encryption and the other for decryption

- *Neeraj A. Sharma is currently pursuing Master's Degree program in Information Technology at The University of Fiji. E-mail: neerajs@unifiji.ac.fj*
- *Mohammed Farik (Member IEEE), is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

and it is mainly used for authentication, non-repudiation, and key exchange. Hash functions provide a digital fingerprint with the use of mathematical transformation to irreversibly encrypt data and it is mainly used for message integrity.

2.2 Secret Key Cryptography

Secret key cryptography also commonly known as symmetric encryption methods or algorithms uses a single key to encrypt plaintext and decrypt the ciphertext [1, 3]. Fig 1, shows the entire process of the secret key cryptography and how it uses just one key which can be any bit length to encrypt and decrypt.

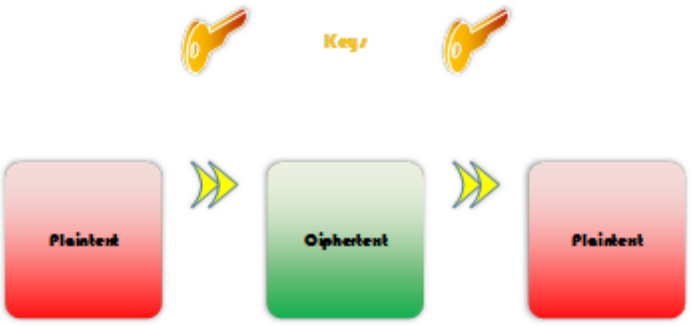

Fig 1: *Secret Key Cryptography*

With this method, it is essential that the key entered by the sender should be the same key entered by the receiver to decrypt the message. For example, Alice wants to send a message to Bob, but Alice is anxious that a middle-man will interfere and read the content of the message. So, Alice decides to use cryptography techniques to encrypt the plaintext with a set of keys and then send the encrypted message to Bob. Bob needs to know the key and the algorithm used while encrypting to successfully decrypt the message from Alice. Furthermore, there are two types of symmetric encryption algorithms, classic and modern. The classic algorithms include and not limited to, Caesar/ Rot-13, Vigenere, Hill, Substitution /Atbash, Playfair, ADFGVX, Byte Addition, XOR, Vernam/ OTP, Homophone, Permutation /Transposition, Solitaire, and Scytale / Rail Fence [5]. The modern algorithms consist of and not limited to, IDEA, RC2, RC4, DES (ECB), DES (CBC), Triple DES (ECB), Triple DES (CBC), Rijndael (AES), MARS, RC6, Serpent, Twofish, DESX, DESL, and DESXL [5]. However, there could be issues arising relating to the type of algorithm used and the length of the bit used as a key. These two factors are important while encrypting and decrypting data as there are middle-man hackers who could use brute-force attack software's to successfully retrieve the message content.

2.3 RC2 Algorithm

RC2 also known as Rivest Cipher was developed to act as a replacement for Data Encryption Standard (DES) and was created by Ron Rivest in 1987 [6, 7]. RC2 is known as a 64-bit block cipher code and has the key size ranging from 8-bit to 128-bit. Each bit size has an increment of 8-bits from the previous key size. The key sizes ranging from 8-bit to 40-bit in RC2 are considered to be weak as using brute-force encrypted messages can be decrypted in a short amount of time. The term key in the case of RC2 is a combination of two things, a KEY and an IV (Initialization Vector). The KEY has 12 characters which support 96-bits and IV consists of 8 characters which support another 64-bits which combined together makes the entire key [1, 6, 7].

2.4 Rijndael Algorithm (AES)

Rijndael algorithms are also known as an Advanced Encryption Standard (AES) is considered a new block cipher which also acts as a new replacement for Data Encryption Standard (DES). AES uses 128-bit blocks with only having three types of encryptions keys that are 128-bit, 192-bit, and 256-bit [8, 9]. AES was officially selected by the National Institute of Standards and Technology (NIST) after carrying out a five-year standardisation process. The famous name Rijndael comes from the Belgium creators, Joan Daemen and Vincent Rijmen [8].

3 Experimental Design

In this section, we will test the two best algorithms available and are used currently with software's that has the capability to send and receive messages. The two algorithms identified were RC2 and Rijndael (AES). We will test these two algorithms using brute-force attack tools to determine which is better than the other. Factors tested will be the bit used (key length) and the time it takes to retrieve the message via the means of brute-force attack tools. The above-mentioned tests will be carried out on i7 Laptop, i7 Desktop, and Xeon Server. Fig 2, shows the experimental setup that was used for this particular paper.

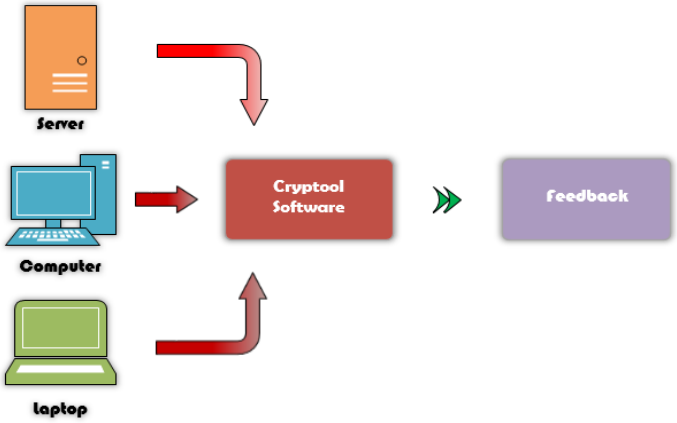

Fig 2: *Experimental Design*

The experiment was carried out on these three machines and their specifications are outlined as well, firstly, HP ProBook i7 @ 2.40GHz processor x 4 Cores and 16GB RAM laptop. Secondly, Asus Gaming Machine i7 @ 3.40GHz processor x 8 Cores and 16GB RAM desktop. Finally, Intel Xeon Server @ 2.50GHz x 24 Cores and 24GB RAM. All three machines were chosen on the basis of performance and technology type that is a laptop, desktop and server. The software used to determine the key length and approximate time to search all keys was the latest Cryptool software. Cryptool is a software that allows users to encrypt and decrypt data using any algorithms regardless of symmetric or asymmetric cryptography [5]. They can carry out performance evaluation as well by using the software's analysis feature to determine the best algorithm and to also see how long any brute-force software will take to decrypt a message. Moreover, the tests were carried out to determine which algorithm - RC2 or Rijndael (AES), is the best.

4 Results

The comparative analysis of both the algorithms was carried out and results are shown in table 1. In that it shows, for the common key length that is 128-bit RC2 algorithm performs seven times better than Rijndael. This nevertheless will stand if you are only going to use a 128-bit key length for your message. However, if you think your message is far more important and will require a 192-bit or 256-bit key length than it will take a server that has 24 cores running at 2.50GHz $9.16x10^{42}$ years and $2x10^{62}$ years respectively.

TABLE 1
A comparative analysis between RC2 and Rijndael

Computer Type	Key Length (bits)	RC2 Algorithm Time	Rijndael Algorithm (AES) Time
HP ProBook i7, 4 Cores x 2.40GHz	8	1 Second	-
	40	25.86 days	-
	64	$1.25x10^{4}$ years	-
	128	$22.25x10^{22}$ years	$2.75x10^{22}$ years
	192	-	$5.5x10^{43}$ years
	256	-	$1.2x10^{63}$ years
Asus i7 Desktop, 8 Cores x 3.40 GHz	8	1 Second	-
	40	6.64 days	-
	64	$0.33x10^{2}$ years	-
	128	$7x10^{24}$ years	$0.94x10^{24}$ years
	192	-	$1.88x10^{43}$ years
	256	-	$4.13x10^{62}$ years
Xeon Server, 24 Cores x 2.50GHz	8	1 Second	-
	40	1 day	-
	64	$0.21x10^{6}$ years	-
	128	$3.7x10^{24}$ years	$0.49x10^{24}$ years
	192	-	$9.16x10^{42}$ years
	256	-	$2x10^{62}$ years

The comparative analysis in Table 1, shows the limitations. If you decide to use an RC2 algorithm with key length in the range of 8-bit to 40-bit then your message can be easily decrypted with any brute-force software.

5 Recommendations

Following the results, users should be able to predict based on the analysis how fast a supercomputer or a quantum computer can decrypt your message. In a world where quantum computers already exist, no one knows how long another more powerful computer comes into the act so it is highly recommended that you use Rijndael algorithm (AES) with 256-bit key length as your number one option to achieve a secure message transmission between you and your companion. However, there could be a new research carried out to increase the key length capability in RC2 algorithms then of course by tests and theory it will perform way better than the current best algorithm which is Rijndael. RC6 looks to be the perfect test case between it and Rijndael, but so far RC6 has not been officially selected to be AES [1]. Unless and until that happens, RC2 remains the best Rivest Cipher out of all.

6 Conclusion

It can be concluded, that even though the RC2 algorithm is performing better than Rijndael algorithm (AES) when it comes to 128-bit key length but RC2 algorithms still doesn't support 192-bit and 256-bit key length. That is where the Rijndael algorithm becomes the most preferred and recommended algorithm approach to use. However, it will be better to carry out the necessary steps into finalizing the RC6 algorithm as an official AES algorithm which can extend this research in terms of comparing it against Rijndael algorithm as RC6 algorithm could be a perfect replacement for the RC2 alogrithm.

References

[1]. Kessler, G. An Overview of Cryptography. 2017 [cited 2017 26th March]; Available from: http://www.garykessler.net/library/crypto.html#skc

[2]. Menezes, A., S. Vanstone, and P. Van Oorschot, Handbook of applied cryptograph. 1st ed. 2001, Boca Ratón: CRC Press.

[3]. Stallings, W., Network security essentials. 4th ed. 2011, Upper Saddle River, NJ 07458: Pearson Education, Inc.

[4]. Rivest, R., Cryptography. JElsevier, 1990. In J. Van Leeuwen: Handbook of Theoretical Computer Science(1st).

[5]. www.cryptool.org. Cryptool. 2017 [cited 2017 27th March]; Available from: https://www.cryptool.org/en/home.

[6]. Elminaam, D., H. Kader, and M. Hadhoud, Evaluating The Performance of Symmetric Encryption Algorithms. International Journal of Network Security, 2010. 10(3): p. 213-219.

[7]. Rivest, R., A Description of the RC2(r) Encryption Algorithm. . MIT Laboratory for Computer Science and RSA Data Security, Inc. , 1998.

[8]. Daemen, J. and V. Rijmen, The design of Rijndael. Vol. 1st. 2011, Berlin: Springer.

[9]. Rudra, A., et al., Efficient Rijndael Encryption Implementation with Composite Field Arithmetic, in Cryptographic Hardware and Embedded Systems Third sInternational Workshop Paris, France.