Performance Evaluation of Symmetric Key Block Algorithm in RC5 over RC4

[1]Kritika Purohit and [2]Karmendra Singh Gehlot
[1]Asst. Professor, CSE Dpt Jodhpur National University
[2]Guest Faculty, MBM Engg. College, Jodhpur
kritika.purohit25@gmail.com karmendra.gehlot@gmail.com

Abstract—***In the internet era there are so many new threats and possible attacks on information, so security has become an important aspect of modern computing systems. With the global acceptance of the Internet, every computer is connected to every other in the world. This has created a wide range of opportunities in the world, but it has also created new risks for the users. Cryptography has been the most robust and potential tool available for se-curing communications over the Internet.***

Keywords : ***DES, 3DES, AES, RC4, RC5, MD5, Enc, Dec, RSA***

I. INTRODUCTION

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. As per the past researches cryptography has often been used to protect the wrong things, or used to protect them in the wrong way.

Unfortunately, the computer security and cryptology communities have drifted apart over the last 20 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems. There are a number of reasons for this, such as different professional backgrounds (computer science versus mathematics) and different research funding (governments have tried to promote computer security research while suppressing cryptography).

Computer security people often ask for non-mathematical definitions of crypto-graphic terms. The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the cipher text. Thereafter, things get somewhat more complicated. There are a number of cryptographic primitives—basic building blocks, such as block ciphers, stream ciphers, and hash functions.

Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric. A digital signature scheme is a special type of asymmetric crypto primitive.

The simplest example of cryptography is transformation of information to prevent other from observing its meaning. Here, we prevent information from reaching an enemy in usable form. Confidentiality is the viewed as the central issue in the field of information protection. Secure communication is the straightforward use of cryptography. The key management problem has prevented secure communication from becoming commonplace. The development of public-key cryptography creates a large-scale network of people who can communication securely with one another even if they had never communicated before.

Early cryptographers used three methods for information encryption:

- Substitution
- Transposition
- Codes

Most initial computer applications had no or at best, very little security. This continued for a number of years until the importance of data was truly realized. Until then, computer data was considered to be useful, but not something to be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt never before. Two typical examples of such security mechanism were as follows. [9]

- Provide a user id and password to every user and use that information to authenticate a user
- Encode information stored in the databases in some fashion so that it is not visible to users who do not have the right permissions.

Furthermore, the internet took the world by storm and there were many of examples what could happen if there was insufficient security built in applications developed for the internet. For example, an intruder can capture the credit card details as they travel from client to the server. Of course this was just one example. There are many other cases have been reported and the need for security is being felt increasingly with every such attack. [9]

Now, there were so many new threats and possible attacks on information. As the technologists found new ways to thwart these attacks, the attackers found new ways to beat the technologists. This continues even now, and in all probability, it will continue to happen in the future. Therefore, it is very important to know how we can make information exchange secure.

Cryptography has been the most robust and potential tool available for securing communications over the Internet. The organizations follow two widely accepted and used cryptographic methods in order to achieve security for e-business application. These methods use some algorithms to scramble data into unreadable text which can only be decrypted by the associated key.

Furthermore, the internet took the world by storm and there were many of examples what could happen if there was insufficient security built in applications developed for the internet. For example, an intruder can capture the credit card details as they travel from client to the server. Of course this was just one example. There are many other cases have been reported and the need for security is being felt increasingly with every such attack. [9]

Now, there were so many new threats and possible attacks on information. As the technologists found new ways to thwart these attacks, the attackers found new ways to beat the technologists. This continues even now, and in all probability, it will continue to happen in the future. Therefore, it is very important to know how we can make information exchange secure.

Cryptography has been the most robust and potential tool available for securing communications over the Internet. The organizations follow two widely accepted and used cryptographic methods in order to achieve security for e-business application. These methods use some algorithms to scramble data into unreadable text which can only be decrypted by the associated key.

Cryptography is the art and science of study of designing or generating the secret message i.e. code or ciphers of the original message for the secure communication between sender and the receiver. Cryptanalysis is the art and science of breaking the generated code or the secret message by finding weakness within it. This process takes the encrypted data and tries to decode the secret message without using the key (which is used to generate the secret message). This process cracks the code, decode the secrets and violate authentication schemes. It is the antonym of cryptography. It makes the secret data confused so that it becomes less clear and more di cult to understand. Cryptology is the study of both cryptography and cryptanalysis and it is the science of encoding and decoding messages.

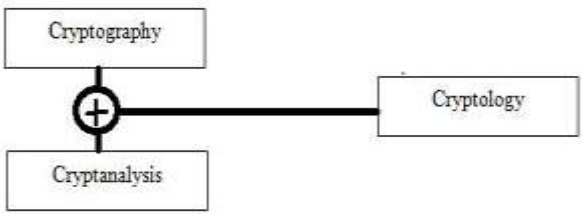

Figure 1: Conversation of Cryptography, Cryptology and cryptanalysis

The main goals of cryptography are as follows:-

1) **Authentication-** This is the process of proving ones identity in which the correctness of an identity can be identified because it is very necessary so that receiver will not receive any false data from unauthorized person or user or the secret message will not receive by a false or unauthenticated user.
2) **Privacy-** Also referred as Confidentiality. Information that is sent over the network or to the receiver can only be read by the intended user or authorized person. This goal is very necessary because it is very necessary for the organization to keep their secret data unhidden from the unauthorized users who intended to steal it and make wrong use of it.

Integrity- This goal helps us to ensure that only authorized person or par-ties are able to modify the contents of the secret data and also the received message is not altered in between by any unauthorized parties.

Non-repudiation- This goal helps to ensure that the sender send the message In other words, neither the sender nor receiver can deny the sending and receiving of the message.[3]

Access Control- This helps to control the accessing of the data so that no other person other than the intended one can use it. This helps in malfunctioning of the data.

Security Approaches

Trusted Systems is a computer system that can be trusted to a specific extent to enforce a specified security policy. Security Models: An organization can take several approaches to implement its security model.

- No security in this simplest case, the approach could be a decision to implement no security at all.
- Security through obscurity In this model, a system is a secure simply because nobody knows about its existence and contents. This approach can-not work for too long, as there are many ways an attacker can come to know about it.
- Host security, In this scheme, the security for each host is enforced individually. This is a very safe approach, but trouble is that it cannot scale well. The complexity and diversity of modern sites organization makes the task even harder
- Network security Host security is tough to achieve as organization grows and become more diverse. In this technique, the focus is to control network.

Access to various hosts and their services, rather than individual host security. This is very e client and scalable model.

II. CRYPTOGRAPHIC ALGORITHM

A cryptographic algorithm is a mathematical functions and unchanging set of steps to perform encryption and decryption of the original data. These algorithms work in combination with a secret key which can be a combination of alphabets, numbers, words or phrases. For the purpose of encryption, the algorithm combines the original data or the text to be encoded (plain-text which is input to the encryption process) with the secret key supplied for the encryption. This combination will yield a cipher text (which is our desired code or we can say output). Similarly, for the purpose of decryption,

The algorithm combines the encrypted data or cipher text with may or may not be the same secret key and this combination will yield again the same plaintext. If there is any modification takes place in any of the secret key or the plaintext, the algorithm will yield a different result than

before. The main objective of every cryptographic algorithm is to make it as di cult as possible to decrypt the generated cipher text without using the key. If a really good cryptographic algorithm is used, then there is no technique significantly better than methodically trying every possible combination of key.

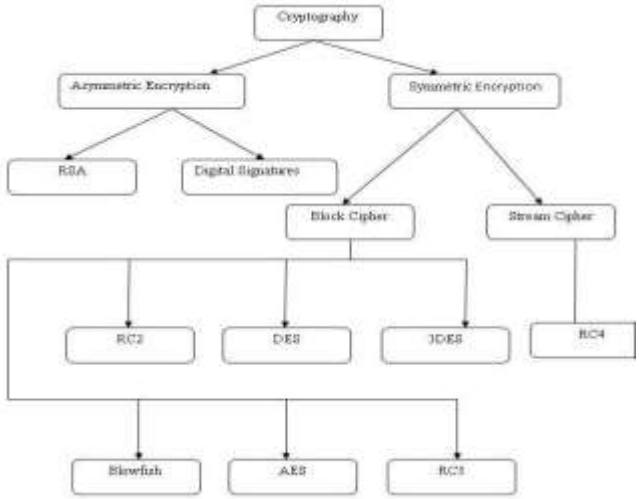

Figure 2: Overview of Cryptography Algorithm

Encryption Algorithms are categorized into 2 categories as follows:-

1. Symmetric Key Encryption
2. Asymmetric Key Encryption

Symmetric Algorithm

In symmetric encryption algorithm, only one key is used for both encryption and decryption process. The key is transmitted to both the sender and receiver before. The key is transmitted to both the sender and receiver before the process of encryption and decryption. So, the secret key plays an important role and its strength depends on the length of key (in bits). The longer the length of key is, it is harder to break it and shorter the length of key is it is even easier to break it. [1] Thus it violates the security purpose of encryption. Symmetric key encryption algorithms are RC2, DES,3DES, RC5, AES, Blowfish

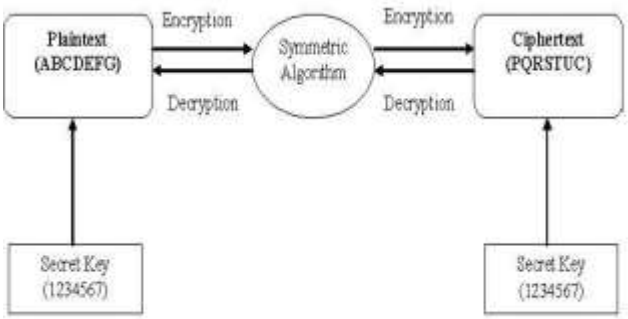

Figure 3: Symmetric Algorithm

Symmetric Encryption algorithms are traditionally divided into two categories:-

a) Block Cipher

A block ciphers divides the plaintext into separate blocks of fixed size (64 bits or 128 bits) and encrypts each of them independently using the same key-dependent transformations.

A block encryption scheme is an encryption scheme whose state, if it has one, can be kept fixed without significantly reducing its security, provided that the plaintext symbols are independent and uniformly distributed.

A block cipher, aims to make its output depend in an unpredictable way on the value of the plaintext block.

b) Stream Cipher-

A stream ciphers takes as input a continuous stream of plaintext symbols, typically bits, and encrypts them according to an internal state which evolves during the process.

A stream encryption scheme is an encryption scheme whose state cannot be kept fixed without severely reducing its security, even if the plaintext symbols are independent and uniformly distributed.

A stream cipher tries to defeat the adversary by making the encryption of a plaintext symbol depend in an unpredictable way on the position in the stream.

III. PREVIOUS WORK ON RC5

The RC5 Algorithm is perceived as one of the strongest cryptographic algorithms. Professor Ron Rivest, author of the earlier RC2 and RC4 algorithms, published a proposed algorithm, RC5, on the Internet. This algorithm uses data-dependent rotation as its non-linear operation and is parameterized so that the user can vary the block size, number of rounds and key length. [5]

The main features of RC5 are that it is quite fast as it uses only the primitive computer operations (such as addition, XOR, shift, etc.). It allows for a variable number of rounds and a variable bit -size key to add to the flexibility. Different applications that demands varying security needs can set these values accordingly.

RC5 are the heavy use of data-dependent rotations and the exceptionally simple encryption. The former feature has been shown to be useful in pre-venting certain advanced types of attack, while the latter feature makes RC5 both easy to implement, and very importantly, more amenable to analysis than many other block ciphers. In particular, the use of data-dependent rotations helps defeat differential and linear cryptanalysis.

Basic Principles

In RC5, the word size (i.e. input plain text block size) number of rounds and number of 8-bit bytes (octets) of the key, all can be of variable length. These are variable in the sense that before the execution of a particular instance of RC5, these values can be chosen from those allowed. This is unlike DES, for instance, where the block size must be of 64

bits and the key size must always be of 56 bits; or unlike IDEA, which uses 64-bit blocks and 128-bit keys.
The following conclusions for RC5 algorithm:
a) The plain text block size can be of 32, 64 or 128 bits (since 2-word blocks are used).
b) The key length can be 0 to 2040 bits (since we have specified the al-lowed values for 8 bit keys).
The output resulting from RC5 is the cipher text, which has the same size as the input plain text. Since RC5 allows for variable values in three parameters, as specified, a particular instance of the RC5 algorithm is denoted as RC5-w/r/b, where w=word size in bits, r=number of rounds, b=number of 8-bit bytes in the key. Thus, if we have RC5-32/16/16, it means that we are using RC5 with a block size of 64 bits (remember that RC5 uses 2-word blocks), 16 rounds of encryption and 16 bytes (i.e. 128 bits) in the key. Rivest has suggested RC5-32/12/16 as the minimum safety version.

Principles of Operations

At first, RC5 appears to be complicated because of the notations used. How-ever, it is actually quite simple to understand. Rather than getting into notations, we shall first illustrate the working of RC5 using g.3.1. As shown in the figure, there is one initial operation consisting of two steps (shown shaded), then a number of rounds. The number of rounds(r) can vary from 0 to 255.
For simplicity, it is assumed that input is plain block with size 64 bits. The same principle operation will apply to other block sizes, in general. In the first two steps of the one-time initial operation, the input plain text is divided into two 32-bit blocks A and B. The first two sub keys S[0] and S[1] are added to A and B, respectively. This produces C and D respectively and marks the end of the one-time operation.
Then, the rounds begin. In each round, there are following operations:

1) Bit-wise XOR
2) Left circular-shift

Addition with the next sub-key, for both C and D- This is the addition operation first and then the result of the addition mod2w (since w=32 here, we have S 32) is performed.
As per the observations the operations the output of one block is fed back to as the input to another block, making the whole logic quite complicated to decipher.

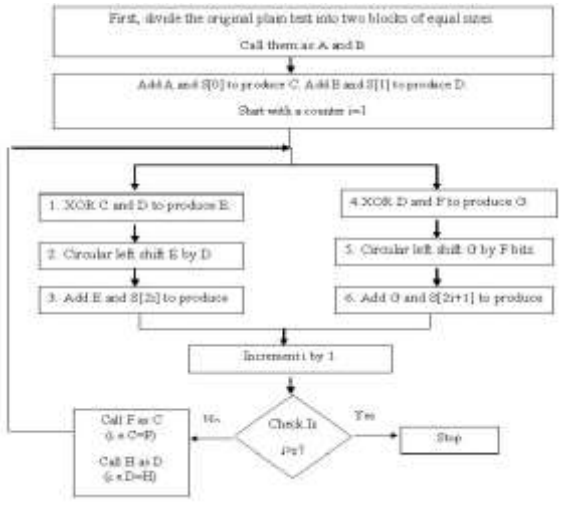

Figure 3 : Encryption using RC5

IV. Comparision of RC5 and RC4

RC4-

RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The data stream is simply XORed with the series of generated keys. The key stream does not depend on plaintext used at all. A variable length key from 1 to 256 bit is used to initialize a 256-bit state table. Vernam stream cipher is the most widely used stream cipher based on a variable key-size. It is popular due to its simplicity. It is often used in file encryption products and secure communications, such as within SSL. The WEP (Wireless Equivalent Privacy) protocol also used the RC4 algorithm for confidentiality. It was also used by many other email encryption products. The cipher can be expected to run very quickly in software. It was considered secure until it was vulnerable to the BEAST attack.

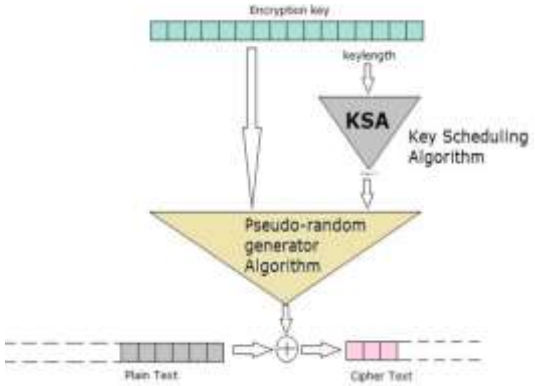

Figure. Schematic representation of RC4 [15]

Algorithm	RC 4	RC 5
Year	1987	1994
Cipher	Stream	Block
Block Size	2064	32, 64, 128
Key Size	1-256	0-2048
Rounds	256	0-255
Possible Attacks	BEAST	Differential
Security	Vulnerable	Vulnerable
Possible Keys	……	…….
Operations Used	+, mod, Xor	+, -, <<<, >>>, xor, Mod

Table 1 : Comparisons between RC4 and RC5 Algorithms [15]

RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The key stream does not depend on plain text

used at all where as in RC5 is a symmetric block cipher having a variable number of rounds, word size and a secret key [15].

Algorithm	RC5			RC4	
Size	16				
Action	Init	Enc	Dec	Init	Dec
StrongARM	41	3	3	155	10
Xscale(400)	45	3	3	66.8	5
Xscale(200)	91	6	7	216	9
Sparc(440)	28	2	2	96	4

Table 2: Execution times [µS] for algorithms, platforms and plaintext sizes [bytes][14]

After performing simulation of these algorithms summarizes the result in table. Comparing the RC4 and RC5 on various processors it shows that the encryption time for both algorithms are close to each other, in fact, RC4 is slightly faster. But, however, by comparing them on Strong ARM, it shows that RC5 is 3 times faster than RC4 algorithm although RC4 operates on 8 bits while RC5 operates on 32 bits. [14]

V. Conclusion

The encryption algorithm is very pact, and can be coded in assembly language on most processors. An important feature of RC5 is its use of data-dependent rotations and the amount of rotation performed is dependent on the input data, and is not pre-determined. The encryption/decryption routines are very simple. The objective here is to focus on the data-dependent rotations as a source of cryptographic strength. [4]

Nowadays, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. It has been surveyed that the existing works on the encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. [8]

Acknowledgment

Thanks to the people who support me in any way, also I owe special thanks to **Mr. Rajendra Purohit**, Supervisor for giving me his precious time, his priceless guidance and suggestions for choosing and shaping this Research.

References

[1] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha, Throughput Analysis of Various Encryption Algorithms, International Journal of Computer Science and Technology, Vol. 2, Issue 3, September 2011.

[2] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, Evaluating the Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.216222, May 2010.

[3] Norman D. Jorstad, CRYPTOGRAPHIC ALGORITHM METRICS, Directorate for Freedom of Information and Security Review (OASD-PA), Department of Defense.

[4] Limor Elbaz and Hagai Bar-El,Strength Assessment of Encryption Algorithm, White paper, October 2000, Discretix Technologies Ltd.

[5] History of Encryption, SANS Institute Reading Room site.

[6] Ronald L. Rivest, MIT Laboratory for Computer Science.

[7] Gary C. Kessler, An Overview of Cryptography, May 1998.

[8] E.Thambiraja, G.Ramesh, R.Umarani, A Survey on Various Most Common Encryption Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[9] Atul Kahate, Cryptography and Network Security, ISBN-10: 0-07-064823-9, Tata McGraw Hill Education Private Limited, 2008.

[10] William Stallings, Cryptography and Network Security, ISBN 978-81-7758-774-6, Dorling Kindersley (India) Ptv. Ltd., Licensees of Pearson Education in South Asia.

[11] Omar Elkeelany, Adegoke Olabisi, Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Recon-gurable Hardware, JOURNAL OF COMPUTERS, VOL. 3, NO. 3, MARCH 2008.

[12] Diana Maimut, Khaled Oua , ghtweight Cryptography for RFID Tags, Copublished by the IEEE Computer and Reliability Societies, March/April 2012.

[13] Joan Daemen, Vincent Rijmen, The First 10 Years of Advanced Encryption, COPUBLISHED BY THE IEEE COMPUTER AND RELI-ABILITY SOCIETIES, NOVEMBER/DECEMBER 2010.

[14] Comparison Based Analysis of Differential Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN) (IJCSI Journal, January 2012)

[15] A comparative Study of Rivest Cipher Algorithms by Sheetal Charbathia (International Journal of Information & Computation, 2014)