Randomized Character based Secure Plaintext Cryptography (RCSPC) Algorithm

Meeta Gohel
Computer Engineering Dept.
Swaminarayan College of Engineering & Technology,
Saij, Kalol, Gujarat, India.

Abstract: Information Technology field has become ubiquitous in day-to-day life to deliver user-centric communication services. With the arrival of internet and explosive growth of social networking applications and cloud computing environments, corporations do generate a substantial amount of data. There exist security risks in places where resources are connected and accessible by any person. The progress of a sustainable, unfailing and trustworthy information infrastructure depends on the secure systems. Cryptography is the elemental tool for such security systems. The study of cryptography techniques is becoming vital as the world is moving towards digitalization. The increasing connectivity of internet users attracts a lot of cyber-attacks. Cybersecurity incidents are becoming severe to take over the control of systems. One of the types of cryptographic techniques is Symmetric key encryption technique. Symmetric key encryption approach is known to apply the same single key for enciphering and deciphering process. The merits of symmetric key approach are its simplicity and faster execution. The major problem with symmetric key encryption approach is its key sharing. This vulnerability is resolved by producing the random key every time. The random key generation can be implemented through the use of secure pseudo random number generator function. Random number generator functions generate a stream of random bits, which are entirely unpredictable. Random number generation approach relies on two types – true random number generator function and pseudo random number generator function. The keystone of pseudo random number generator approach is an initial value, called seed. True random number generator is not dependent on the seed value. In this work, the security breaches of symmetric key encryption approach are studied. The attempt is to devise an encryption algorithm in order to increase the security level of symmetric key encryption approach with the use of random number generator function.

Index Terms **- Information Security, Cryptography, Encryption, Symmetric encryption, Cipher, Random number, Random number generator, randomness.**

I. INTRODUCTION

Information Technology field has been ubiquitous as an exciting paradigm in order to provide computing and communication services. Information Technology benefits are realized in various computing environments such as cloud computing, autonomic computing, internet of things and so on. There exist security risks in resource sharing of all such user-centric environments. Information Security is referred to as a branch of protecting information from unauthorized access, disclosure or security violations. There are 5 types of Security Services: 1) Authentication 2) Access Control 3) Confidentiality 4) Integrity 5) Non-repudiation. The development of an unfailing and trustworthy data infrastructure requires secure systems. The key elemental tool for protecting computing environments is Cryptography. Cryptography is the art and science of keeping secrets. Cryptography is broadly applied to ensure data security, privacy and trust in computing environments. The data has been increasing in all the private and public sectors which require availability, data secrecy and data integrity. Encryption is defined as the process of converting the given message into the coded message, which is not understandable. Decryption is the reverse of the encryption, which takes the coded message as input and gives the original message as output. The protection of the confidential data from unauthorized access can be done through various encryption techniques.

.

II. CLASSIFICATION OF ENCRYPTION TECHNIQUES

A. Symmetric Key Encryption

Symmetric Key Encryption technique uses the same key for encryption and decryption process. Here there exists a common key for both encryption and decryption, therefore this technique is known as Secret Key Cryptography or Private Key Cryptography. There are different symmetric key encryption algorithms such as DES (Data Encryption Standard), TRIPLE DES, AES (Advanced Encryption Standard), RC4 (Rivest Cipher 4), RC6 and BLOWFISH.

B. Asymmetric Key Encryption

Asymmetric Key Encryption technique uses two different keys for encryption and decryption process. Therefore, this technique is known as Public Key Cryptography. Here two keys are used: a private key and a public key. Private key is kept secret and public key may be distributed. The message is encrypted with receiver's public key and the encrypted message is decrypted with receiver's private key. Examples of asymmetric key encryption algorithms are DSA (Digital Signature Algorithm), RSA (Rivest Shamir Adleman) and Diffie-Hellman algorithm.

2.1 TYPE OF ATTACKS

An attack is defined as an assault on system security that comes from an intelligent threat. Technology has been rapidly evolving in a world driven by social networking, online transactions, big data processing and cloud computing. The progress of cybercrime and the development of new attack types come with this evolution. There are basically two types of attacks: 1) Active Attack 2) Passive Attack.

A. Active Attack

An active attack is a network attack in which the attacker attempts to change the system resources or alter the system operations. The types of active attacks include: masquerading, replay attack, modification of messages, denial of service, distributed denial of service.

B. Passive Attack

A passive attack is a network attack in which the attacker attempts to gather information or make use of gathered information, but the system resources are not affected. The types of passive attacks include: release of message content, traffic analysis.

III. RANDOM NUMBER GENERATOR

Random number is a number selected from a set of numbers which occur without any definite pattern. It is a kind of number obtained by chances. Random number is one of a sequence of numbers which are appropriate for satisfying certain statistical tests. Random numbers are one of the most important numbers in cryptography. Random numbers are used in generating the data encryption keys, simulation of models, video games and gambling. Randomness refers to the degree of unpredictability of generating the random numbers at a time. Classic examples of randomness include - flipping a coin, rolling a dice, shuffling of playing cards.

Random number generator function is a mathematical function which is used to generate a sequence of random numbers. These random numbers cannot be predicted reasonably. Random number generator functions are used to construct a series of the required number of random bits on request. Random number generator function is used to produce a string of 0 and 1 bits that may be combined into the blocks of random numbers. Random number generator is also called as Random Bit Generator. These random number generator functions are believed to be statistically independent and unbiased. Random number generator function should be compatible with a general-purpose cryptographic library for encryption of keys. Random number generator functions are used in applications of cryptography, computer simulation, statistical sampling, gambling, randomized design and in security applications.

3.1 TYPES OF RANDOM NUMBER GENERATOR

There are main two types of random number generator function: -

1) True Hardware Random Number Generator functions (Non-deterministic RNG)
2) Pseudo Random Number Generator functions (Deterministic RNG)

A. True Hardware RNG

Randomness is derived from physical phenomena and based on this concept true random generator function has been developed. This type of function measures physical phenomenon which is expected to be random. Examples include atmospheric noise, thermal noise, cosmic radiation, and quantum phenomena. This function generates the random numbers from a physical process, rather than by means of any computational algorithm. That is why it is called Hardware Random Number Generator function. In this method, there is no base value used for calculation or generating process of random numbers. Therefore, this method is truly unpredictable. True random number generator functions consist of microscopic phenomena that can generate the low-level and statistically random noise signals. True random number generators are used for non-gambling purposes, such as in sampling for opinion polls, selecting jurors, military draft lotteries.

B. Pseudo RNG

The word ‘pseudo’ means kind of close to, but not in a real sense. Pseudo random number generator functions are mathematical functions that use a precalculated set of values to generate the random numbers. In this method, the numbers generated look like random but they might not be actually random. Pseudo random number generator function makes use of a seed value which is a fixed number used as a base of the algorithm. This seed is also known as an initial value. Pseudo random generator functions are like computational algorithms that can produce a sequence of random numbers, which are completely determined by an initial value, which is known as a seed value or key.

3.2 RCSPC (RANDOMIZED CHARACTER BASED SECURE PLAINTEXT CRYPTOGRAPHY) ALGORITHM

RCSPC Algorithm is based on random string generator function. During encryption process, the plain text is given as input and it is converted into the cipher text through 128 bits key, which is produced randomly by random number generator function.

RCSPC algorithm will encrypt both – plain text and key. The decryption process will produce the original plain text from the entered key and cipher text.

Following are the steps used in the encryption algorithm:

1. Plaintext is entered as input.
2. After entering the plaintext, the function of character optimization is applied, in which the characters of given plaintext are separated. The identification logic is implemented at this stage, which uses the identification buffer. The identification buffer stores the identity character for each character of a given plaintext according to the level of encryption.
3. Random String Generator function is applied at this stage, which is used to generate random length strings which are added to the plaintext as padding.
4. Random Position Generator function is applied, which is used to allocate random strings on random position by applying the mixture of substitution and transposition operations.
5. Key is generated according to the size of the plaintext and key is encrypted by the random generator function.
6. Depending on the level of encryption, the plaintext is converted into the ciphertext with the help of random generator functions.
7. The output of the encryption algorithm is the encrypted text and encrypted key.

Flowchart of RCSPC Algorithm

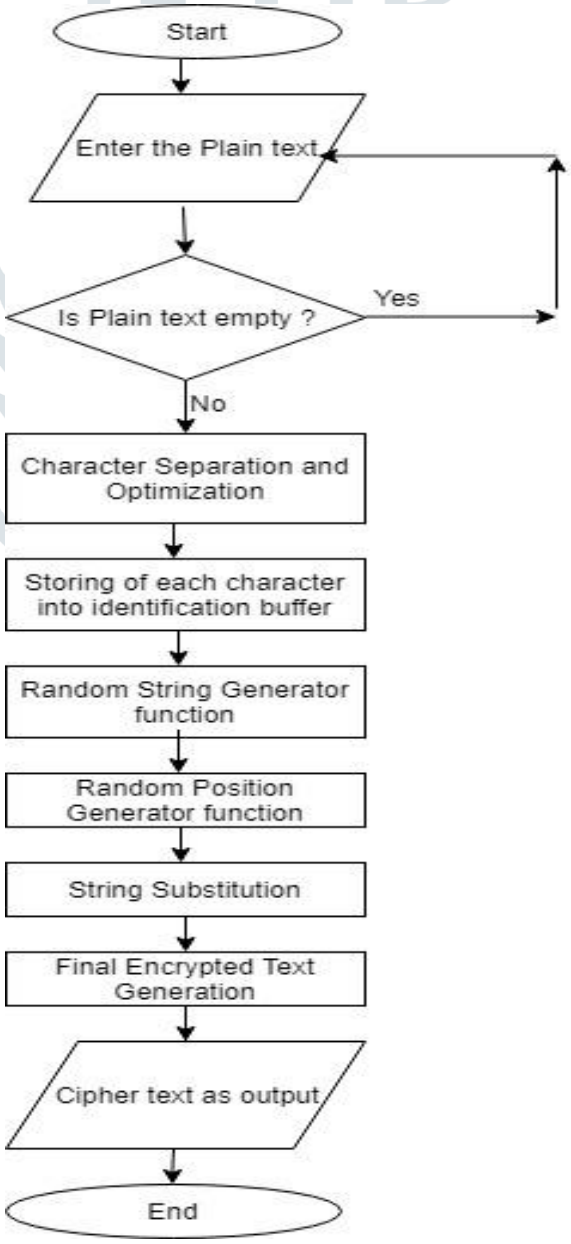

Fig 1 – Flowchart of RCSPC Algorithm

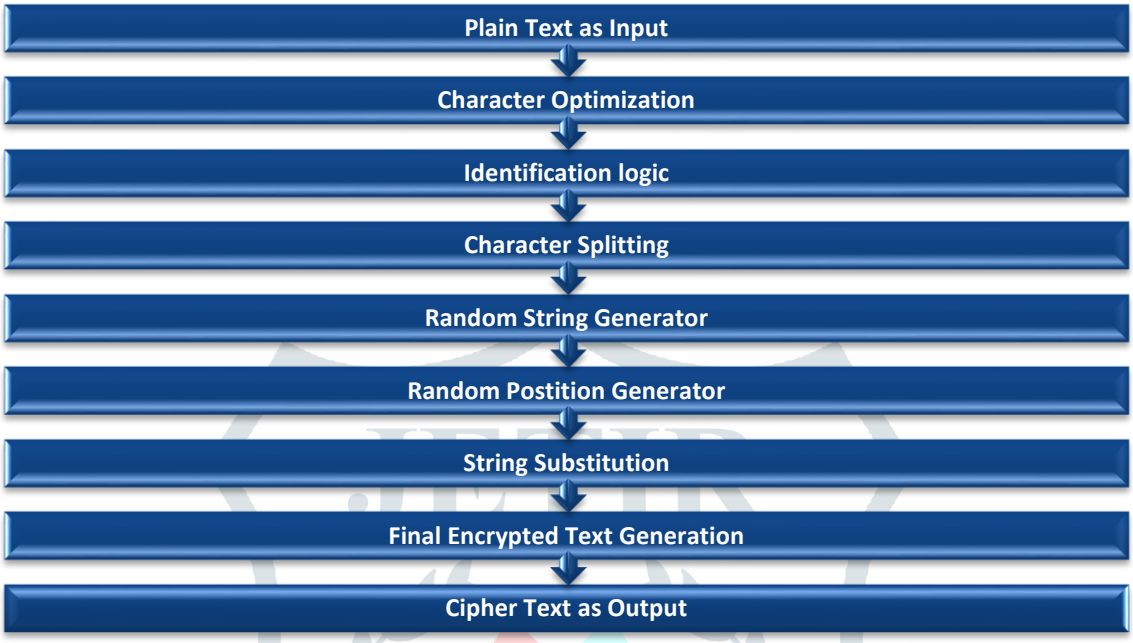

Fig 2 – RSCPC Algorithm Steps

3.3 Characteristics of RCSPC Algorithm:

1. RCSPC algorithm is based on the standard encryption algorithm Blowfish.
2. RCSPC algorithm is a stream cipher.
3. Algorithm accepts the input of 64 bits.
4. Key size is varying between 32 to 448 bits.
5. The output of the encryption algorithm is of the range of 256 bits.
6. RCSPC algorithm uses a random number generator function for generating the random key.
7. Algorithm also uses a random string generator function to generate the random characters which are used for padding during enciphering process.

3.4 Benefits of RCSPC Algorithm:

1. Algorithm consumes less memory space.
2. Encrypted text length is different every time.
3. Random key is generated at every iteration.
4. Algorithm execution flow is unpredictable.
5. Algorithm is fast in execution.
6. Encryption algorithm is very difficult to hack.
7. RCSPC algorithm is less complex as compared to other standard algorithms.
8. Decryption is not possible without key.

3.5 Limitations of RCSPC Algorithm:

1. Key transportation can become problematic.
2. Digital signatures cannot be generated using this algorithm.
3. Risk of symmetric key storing.
4. If the symmetric key is compromised or damaged, user's data will be lost.

5. The range of random number generator function is 0 to 9999. It is limited to 9999 only.

IV. RESULTS AND GRAPHS

4.1 Results of Different Input Categories

Table 1: Input Type vs. Output Variation

Sr. No.	Category	Input Type	Output Length (bits)	Key Size	Encryption Time (mins)
1	A – Short Length (1 to 25)	Alphabets (Small)	2600	Moderate Strong	~1.5
		Alphabets (Capital)			
		Alphanumeric			
		Digits only	3200		
		Special Characters only			
		Digits + Special Characters			
		Alphabets + Special Characters			
2	B – Moderate Length (25 to 35)	Alphabets (Small)	3700	Moderate Strong	~2
		Alphabets (Capital)			
		Alphanumeric			
		Digits only	4200		~2.5
		Special Characters only			
		Digits + Special Characters			
		Alphabets + Special Characters			
3	C – Highest Length (>35)	Alphabets (Small)	6000	Strong	~3.6
		Alphabets (Capital)			
		Alphanumeric			
		Digits only	9999		~4
		Special Characters only			
		Digits + Special Characters			
		Alphabets + Special Characters			

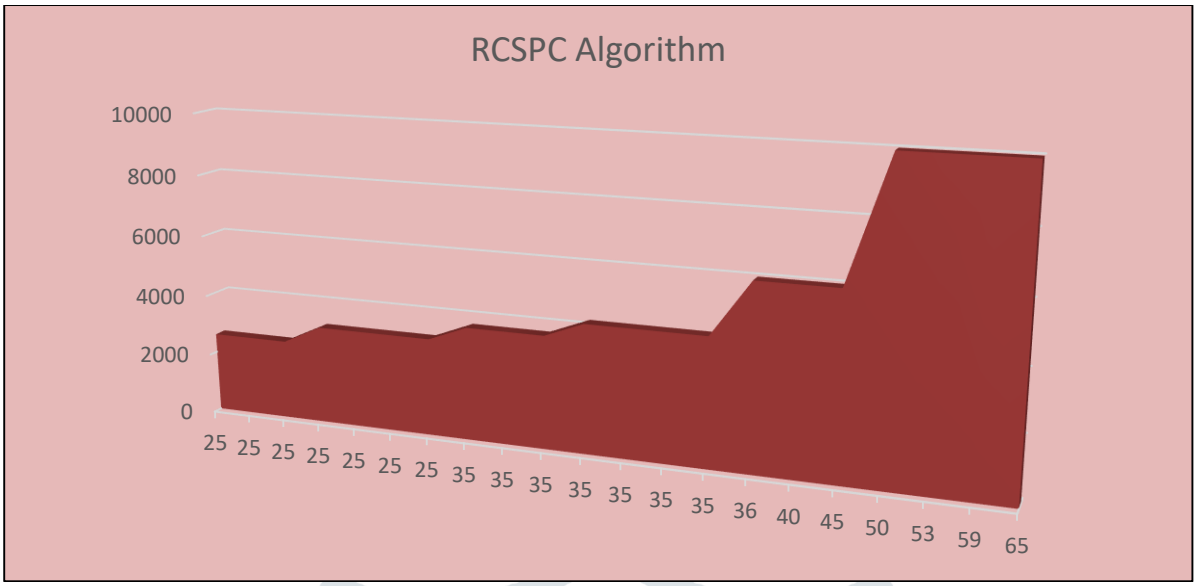

Fig 3 – Input Length vs. Output Strength in RSCPC Algorithm

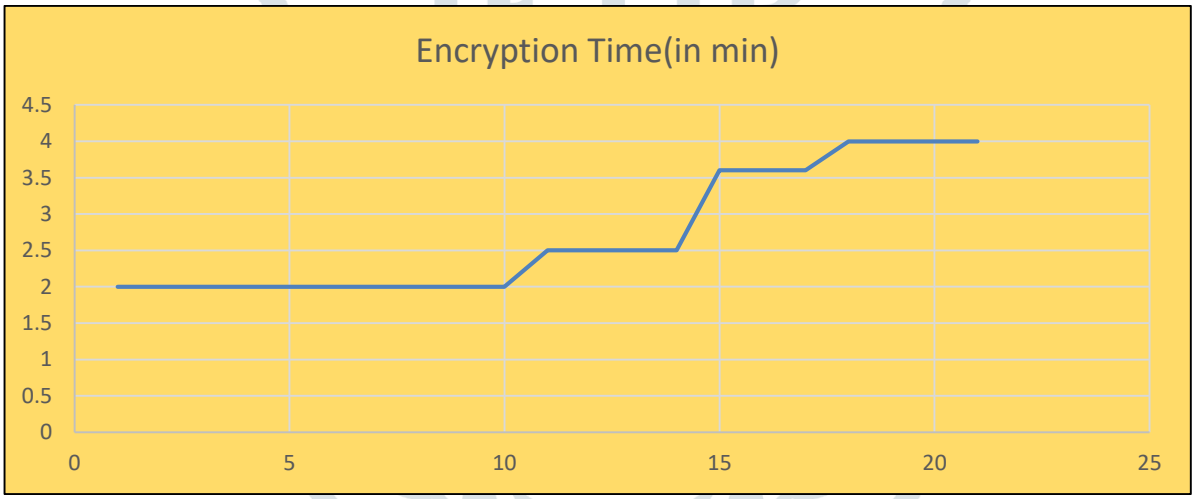

Fig 4 – Input Length vs. Output Time (in mins)

V. Conclusion

The benefits and security exploits of symmetric key cryptographic algorithms have been studied thoroughly and efforts have been put to resolve the limitations of symmetric encryption approach. With the implementation of random number generator function, the symmetric approach has been strengthened. The random number generator function is extended to the creation of random string generator function, which is used to produce the random key for the enciphering process. The RCSPC encryption algorithm has been devised using random number generator function. The encryption algorithm has been created by following the standard symmetric encryption algorithm – Blowfish. The key distribution in the RCSPC encryption approach is implemented through the Kerberos authentication protocol. Using the standard symmetric encryption algorithm and standard authentication protocol, the security level has been raised and successful results have been achieved.

VI. Acknowledgment

I would like to thank my parents, friends, internal guide, mentor and my GOD for their consistent and unconditional support.

References

[1] Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M, (2015). "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish.*"* BVBCET, Hubli 5800031, India.

[2] Ashoke Nath, Saima Gosh Meheboob Allam Mallick, (2010). "Symmetric Key Cryptography using Random key generator", St. Xavier's College, Kolkata, West Bengal, India.

[3] Mina Mishra, V.H. Mankar, (2015). "Text Encryption Algorithms based on Pseudo Random Number Generator", Nagpur University, Nagpur, Maharashtra, India.

[4] K.M. Uma Maheshwari, Rajdeep Kundu, Harsh Saxena, (2018). "Pseudo Random Number Generators Algorithms and Applications", SRM Institute of Science and Technology.

[5] Christophe Dutang, Diethelm Wuertz, (2009). "Overview of Random Generation Algorithms"

[6] J. B. Awotunde, A. O. Ameen, I. D. Oladipo, A. R. Tomori, M. Abdulraheem, (2016). "Evaluation of Four Encryption Algorithms for Viability, Reliability and Performance Estimation", Department of Computer Science, University of Ilorin, Ilorin, Nigeria.

[7] Diaa Salama Abdul Elminaam, Hatem Mohamed Abdul Kader, Mohie Mohamed Hadhoud, (2008). "Performance Evaluation of Symmetric Encryption Algorithms", Minufiya University, Egypt.

[8] Nentawe Y. Goshwe, (2013). "Data Encryption and Decryption using RSA Algorithm in a Network Environment", Department of Electrical/Electronic Engineering, University of Agriculture, Makurdi.

[9] Fausto Meneses, Walter Fuertes, José Sancho, Santiago Salvador, Daniela Flores, Hernán Aules, Fidel Castro, Jenny Torres, Alba Miranda, Danilo Nuela, (2016). "RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8.

[10] Sarita Kumari, Research Scholar, (2015). "A Research Paper on Cryptography Encryption and Compression Techniques", International Journal of Engineering and Computer Science ISSN:2319-7242.