THEORETICAL BIOLOGY FORUM
ISSN: 2283-7175 | https://tbfpeerjournal.org/

A Comprehensive Review on Cipher Design Using Reverse String Techniques

Neha Jain*, Abhinav Tiwari, Kritika Goyal
* Medi-Caps University, Department of Computer Science & Engineering, Indore, India
Medi-Caps University, Department of Computer Science & Engineering, Indore, India
Medi-Caps University, Department of Computer Science & Engineering, Indore, India

ABSTRACT
There are many Crypto-system are define in today's world. There are some private key and public key Crypto-system. These Crypto-systems are all mathematical calculations So, each can be broken by computation machine. Computer can check all the possibilities of keys, a Crypto-system have in minutes or hours of time which depends on the speed of the computer and computation power. Computer applies keys to a cipher text and then checks the string matching with a dictionary. There are many techniques which are being used to increase the key space and secrecy of the Crypto-system but still the computer can find the solution by applying all possible combinations. Reverse String Cipher is a modification in all cipher techniques to increase the security.
General Terms
Reverse String, Modern Cipher.

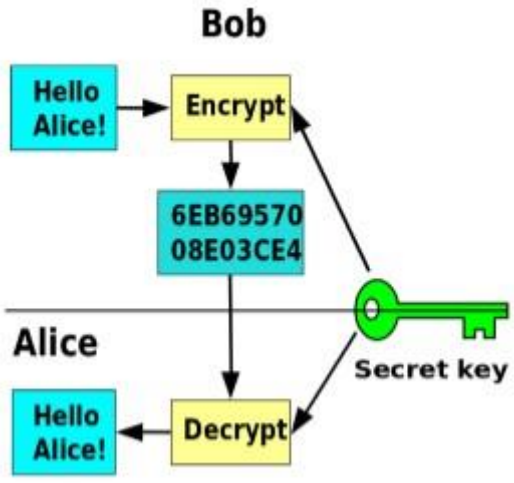
KEYWORDS: Reverse String, Technique, Key, Cipher, Formulas, Secrecy.

INTRODUCTION
Crypto-system is a set of keys, cipher text, plain text, encryption, and decryption. Cryptography was used in World War I and World War II. In WW-II most famous encryption device was being made named Enigma design by Germany [1] to communicate with their army. This kind of machine with better quality ciphers are being created after cryptanalytic difficult in WW-I[8]. There are two types of Crypto-system:

- Symmetric Crypto-system
- Asymmetric Crypto-system

Symmetric Crypto-systems are the system in which both the users have equal knowledge about the keys and functions used. In this kind of Crypto-system the user needed a secret channel to send the key on which the functions are being design. That are functions are design by the use of mathematical formulas. This are also knowns as private key cryptography. Symmetric crypto-system is the only method known to public to apply encryption before 1976.

There are many types of symmetric Crypto-systems which are being used to transfer their information with secrecy but finding a function or mathematical technique is not a big problem for analysing programs or softwares and so as finding a key for other program by checking each possible key on that function they just have extract form the given ciphered text.



This makes the Crypto-system less secure nowadays since there are many software can decipher the given text. Symmetric model use AES which also replaced DES[2].

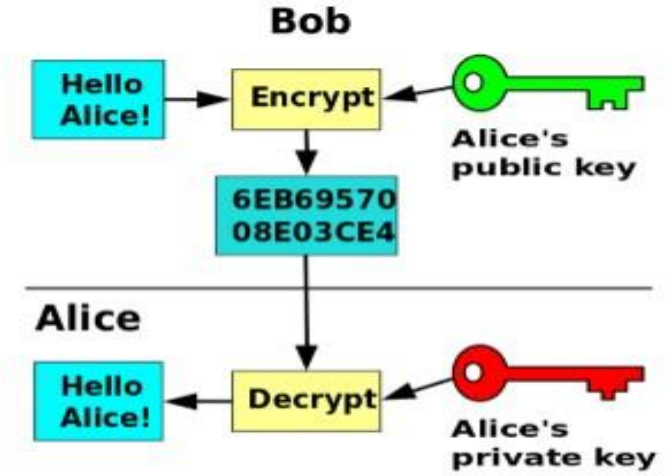
There are some general symmetric cryptosystem:

1. Classical Cipher
    1. Shift Cipher
    2. Affine Cipher
    3. Vingenere Cipher
2. Block Cipher
3. Stream Cipher

Block cipher are divide the plain text into blocked which is a input to Stream Cipher. Stream cipher create a stream of keys to cipher a plain text.

DES and AES are the standards design by block cipher for private key crypto system designed by US government by with cryptographic standards. This are still in use in worldwide in ATM encryption [3], remote secure access [4], e-mail [5].

Asymmetric Crypto-systems are much popular in day to day world e-mails, messages anything is be ciphered by using asymmetric Crypto-system. The concept of asymmetric crypto-system was proposed by Whitfield Diffie and Martin Hellman in year 1976 the introduce a method with 2 mathematical key generation public and private key public key[6] is used to design encryption function and private key for decryption function after 2



year a working crypto system was design using public key concept named RSA. In this technique the sender doesn't have full knowledge of keys and decryption function. This are also called as public key cryptography. As by the name public key cryptography in this the encryption function is known to all which are going to communicate with end user or not and they can use that encryption function to analysis the function and find the solution to decrypt it. The calculations are pretty big for a human to calculate and find the right solution but with a correct software or program and computer can calculate it faster.

There are some asymmetric cryptosystem:

1. RSA
2. DSA

RSA and DSA are the modern algorithms for public key cryptosystem. RSA algorithm was design by Ronald Rivest, Adi Shamir, and Len Adleman in year 1978[7].

Cryptanalysis is a technique to break the code or cipher text by hacker or attacker on the given information. It is used to analysis the cipher text and decrypt by finding flaw in the algorithms and hijack the information. Cryptanalysis is used to find the hidden aspect in system [9]. In World War I vingenere cipher was1st time broken by Friedrich Kasiski [10] before this vingenere cipher was used for 2 centuries to communicate securely.

Now after time changes asymmetric cipher are being introduced in that the private key and public key are different as the time increased the key space of asymmetric cipher are being increased as in 1980 the key space was 150 digits then in entering 21st century the key space was increased to seven hundred. And the difference between private and public key is that the attacker have knowledge of public key. After world war each government agency have their own team of cryptographers to decode the cipher text by using cryptanalysis[11].

PREVIOUS WORK

Sonal Sharma, Jitender Singh Yadav, Prashant Sharma, "Modified RSA crypto system Using Short Range Natural Number Algorithm" In this paper the author proposed a method for public key crypto-system which is modification in RSA named as SRNN(Short Range Natural Number). In SRNN they generate small range of random natural number u to a session to session which will be better for the solution for balance between security and speed. In their method they established a secure communication where the couriers doesn't carry keys with it. They also mention the differences between the RSA and SRNN but the main differences mention are SRNN increase the security but the process is slow[12].

Hardik Gandhi, Vinit Gupta, Indra Rajput, "A Research on enhancing Public Key Cryptography by the use of MRGA with RSA and N-Prime RSA" In this paper the author suggested another method named magic rectangle to increase the security. Magic rectangle is constructed by min start max start seed values and column sum. If any hacker get initial value it will be hard for him to find rest of the column and row values because of the randomness created by magic rectangle. The only issue in this method is magic rectangle takes time to be constructed[17].

Jeffrey Sorrentino, "Information Security: Introduction to Cryptography" In this paper the author told about the problems faced by government and private sector on the attacks on digital communication. The author discussed cryptography algorithms and the recent public algorithms such as-Data Encryption Standard and Advanced Encryption Standard. The development of cryptography is never ending process when we develop any new algorithms somehow there will be a way we'll find out later to hack it[16].

Shyam Nandan Kumar, "Review on Network Security and Cryptography" In the paper the author reviewed various cryptographic concepts. the author explain some basic cipher techniques such as-shift cipher, block cipher, RSA. the author also suggested to increase the security on internet to protect the data we upload on clouds. It also says that there are many mathematical formulas and cryptographic techniques which are increasing day by day [15]. He also said that Model for Cryptosystem Using Neural Network supports high security [18].

Aayushi Shukla, Prof. Pradeep Kumar, "An approach for Information Hiding using Inverse Z-Transform and Genetic Algorithm" In this paper the author describes steganography which is a method that involves a carrier which help a communication of secret data. There are various steganographic techniques present nowadays. In this paper they proposed inverse Z-Transform to modify the pixel location and genetic algorithms to increase secrecy. They combine one of the best cryptographic technique with some message hiding algorithms which will further increase the visual quality of image the cryptographic technique used in it is blowfish and the message hiding algorithms are IZT and genetic algorithms[14].
Ajay Kr. Phogat, Archana Das, "A Symmetric Cryptography Based on Extended Genetic Algorithm" In this paper the author suggested genetic algorithms for cryptanalysis he said genetic algorithms has been used to solve many problems. In this paper it shows how genetic algorithms can be used to decrypt the ciphered text. Genetic algorithms been tested on some basic ciphers such as-classical ciphers, verman cipher, knapsack, permutation, substitution, transposition[13].

METHOD

Encryption with reverse string

In this method the plain text will first being reversed and then we apply the encryption function of that reversed plain text and get a cipher text. This will increase the work of the ciphering but the result will be increased as the number of words increased in the information it makes difficult for computer to find the key in the normal process as the words are being increased the possibility increases for the computer to find the right key. The more the data computer have to compute the easier it becomes to find the right key for the crypto-system.

Decryption with reverse string

In this method after applying decryption function on the cipher text the output of the function will be reversed string. So,after decrypting reverse the output and get the plain text.This decryption can be done as normal decryption as well as after getting the data we just have to apply the reverse string to get the actual information. As i said earlier it will increase the secrecy with the no. of words increased so the bigger the information is the greater time the system will take to find the key and after finding the key the system still needs to inverse the string.

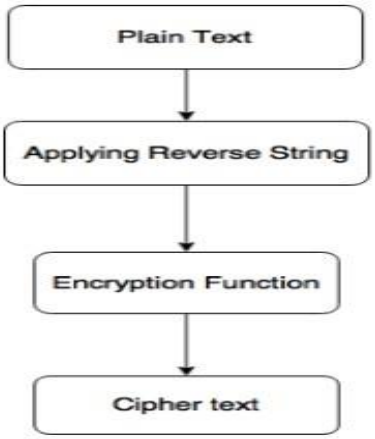


Fig 1. Encryption with Reverse String

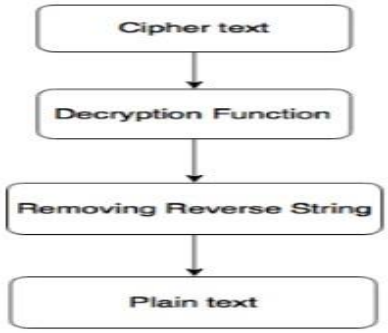
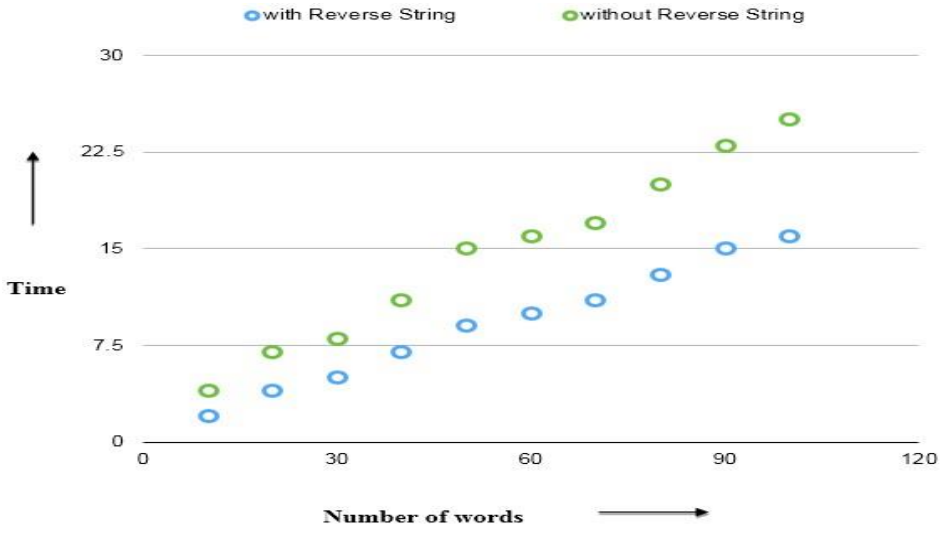


Fig 2. Decryption with Reverse String

COMPARISON

As we seen above that all Crypto-systems are design by using mainly keys and mathematical functions and there are computers fast enough to check all the possible keys with different type of functions and find a solution and there are plenty of software design to find the solution of ciphered text. That software analysis the pattern in that cipher text then start applying the possible keys and then check the words matching with dictionary or not.

We can use reverse string technique to solve this problem in reverse string before ciphering an information at first we'll reverse whole information by using and reverse string program design in any language that will create a chaos for computer when computer decipher a given text and check the words in the dictionary it will find very less words are matching and hence the software will conclude that is not a right key for that Crypto-system.



Graph 1. Time vs Number of Words

CONCLUSION

Reverse string technique can be used with any cipher technique. It will increase strength of the encryption.It can help the crypto-system to put the computer in an ambiguous situation in which the computer will solve the problem which is given to it but can't reach at the solution of the encrypted solution. There are many techniques been suggested to increase the key space of a Crypto-system or new techniques to cipher but no one ever try to enhance the old methods with some kind of changes within the plain text. No computer will find any words matching with the dictionary words and reach at a certain solution.

FUTURE SCOPE

This technique can be used with other cryptography method to increase the secrecy of any information. It can design software with reverse string cipher in them. An add-on feature in old software to encrypt with reverse string with a simple program added in the software. It can be further designed a new type of cipher method with more mathematical formulas and methods used in it.

ACKNOWLEDGEMENT

Our thanks to Deepak Agarwal who have contributed towards development of the research.

REFERENCES

[1] Hakim, Joy (1995). A History of US: War, Peace and all that Jazz. New York: Oxford University Press. ISBN 0-19-509514-6.
[2] Sharbaf, M.S. (2011-11-01). "Quantum cryptography: An emerging technology in network security". 2011 IEEE International Conference on Technologies for Homeland Security (HST): 13–19. doi:10.1109/THS.2011.6107841
[3] "NCUA letter to credit unions"(PDF). National Credit Union Administration. July 2004. Retrieved 26 March 2015.
[4] Golen, Pawel (19 July 2002). "SSH". WindowSecurity. Retrieved 26 March 2015.
[5] "RFC 2440 - Open PGP Message Format". Internet Engineering Task Force. November 1998. Retrieved 26 March 2015.
[6] Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques". AFIPS Proceedings. 45: 109–112.
[7] Rivest, Ronald L.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. Association for Computing Machinery. Archived November 16, 2001,
[8] Gannon, James (2001). Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century. Washington, D.C.: Brassey's. ISBN 1-57488-367-4.
[9] "Cryptanalysis/Signals Analysis". Nsa.gov. 2009-01-15. Retrieved 2013-04-15.
[10] Singh 1999, pp. 63–78.
[11] Stallings, William (2010). Cryptography and Network Security: Principles and Practice. Prentice Hall. ISBN 0136097049.
[12] Sharma,Sonal,Yadav,Jitendra Singh ,Sharma Prashant,"Modified RSA Public Key Cryptosystem using Short Range Natural Number Algorithm", International Journal Of Advanced Research in Computer Science and Engineering, Volume 2, Issue 8, August 2012.
[13] Phogat, Ajay Kr., Das,Archana,"A Symmetric Cryptography Based on Extended Generic Algorithm". International Journal of Current Trends in Engineering and Research, Volume 22, Issue 4, April 2016.
[14] Shukla, Aayushi, Kumar, Prof.Pradeep,"An Approach for Information Hiding using Inverse Z-transform and Genetic Algorithm", International Journal Of Advanced Research in Computer Science and Engineering, Volume 5, Issue 1, January 2015.
[15] Kumar, Shyam Nandan ,"Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3
[16] Sorrentino, Jeffrey, "Information Security: An Introduction to Cryptography"
[17] Gandhi, Hardik, Gupta, Vinit, Rajput, Indra, " A research on Enhancing Public Key Cryptography by the use of MRGA and N-prime RSA", –International Journal for Innovative Research in Science & Technology, Volume 1, Issue 12, May 2015
[18] Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

