Comparison of Symmetric Cryptographic Techniques

Akash Shitole[1], Siddharth Nanda[2], Rajeshwari Gundla[3]
[1]U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India
[2]Faculty - IT, iNurture, Bengaluru, India
[3]Senior Faculty - IT, iNurture, Bengaluru, India

Abstract- Prior, when computers hadn't progressed people use to transmit messages or information through letters or physical means. They were convenient for short distance communication but it wasn't possible to convey messages for longer distance. In addition, these messages were also less secure as they had a risk of being stolen in the middle.

Nowadays with the progress in technology and advancement in each field we can accurately and securely transmit data over the globe. Cryptography has a crucial hand in channeling data over network. Data is transferred in encrypted format and is also decrypted back to get the data. There are numerous ways to encrypt data to communicate securely. Various algorithms are used to make the encryption stronger. In this paper we will see the most used algorithms in cryptography.

Keywords- Computers, technology, cryptography, encryption, decryption, network, algorithms.

I. INTRODUCTION

Wikipedia explain cryptography as methods and practices used for securing communication over a channel in the existence of a third force. Cryptographic techniques take part in communicating with people. Not only communicating but cryptography also be a major part in creating a secure computing environment. There exist risks that affect an organization or a personal due to rapid advancement in technology, therefore, being updated with various new cryptographic security techniques can ensure your data to be secure and no third person can gain way in to the information.

Creating secure organizational environment is important through security point of view. Cryptography helps you in creating this environment by keeping your sensitive information and all the data accessible to authentic person.

There are number of cryptographic techniques which every organization needs to adapt. Here, we will see about the various techniques used in organizations and the most used technique amongst them to help us understand the most secure technique amongst others. This will also help us in adapting to this technique to keep our data safe.

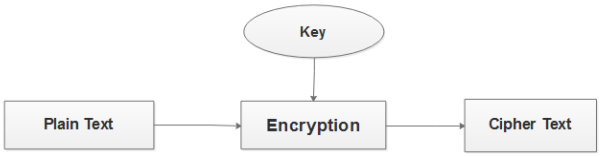

Fig.1: Basic Encryption method

II. LITERATURE SURVEY

a. Transposition Cipher

Transposition cipher works by categorizing information into static sized blocks and then arranging the characters within each block. A. Dimovski and D. Gligoroski [1] proposed an algorithm for breaking the transposition cipher in which they recover a key with ciphertext amount 13.25 out of 15. R. Toemeh and S. Arumugam [2] also proposed an algorithm in which for the same number of encrypted text, the key length obtained was 15 with an improvement of 13 percent. Therefore, the transposition cipher can be broken easily with an accurate key to get the data.

b. Substitution Cipher

According to Wikipedia [3], substitution cipher is a method of securing information by which parts of plaintext are replaced with cipher text. As stated by a fixed system, the parts can be any number of letters or methods. The receiver decrypts the data by executing the reverse substitution. Shmuel Peleg and Azriel Rosenfeld [4] demonstrated relaxation method and concluded that it is possible to break the encrypted text in which substitution method is used. This helps us to verify that substitution cipher can be broken as well to know about the messages passed over a network.

c. Vigenère Cipher

As mentioned in Wikipedia [5], In Vigenère cipher, alphabet text is encrypted by using sequence of various Caesar ciphers (Caesar cipher is cipher in which each alphabet is moved some amount of places) based on the alphabets of a keyword. It is a simple form of polyalphabetic substitution. Ragheb Toemeh and Subbanagounder Arumugam [6], implemented genetic algorithms for polyalphabetic substitution for recovering plaintext. They proved that genetic algorithms will be helpful in deciphering Vigenère cipher. Therefore, we can conclude that Vigenère cipher can also be cracked.

d. Block Cipher

A message is distributed into pack of data which are then encrypted. This process is known to be block cipher. It encrypts a whole block rather than encrypting letters. Referring to [1] block cipher can break using their algorithm. Block cipher comes under symmetric cipher; hence, genetic algorithms can also be used in cracking block ciphers. Marc Kaplan1, Ga¨etan Leurent, Anthony Leverrier, and Mar´ıa Naya-Plasencia [7] concluded that symmetric cryptosystems can be easily broken using quantum period findings. They provided the first known quantum speed-up of a classical attack which performed to break the encryption. Therefore, block ciphers are also vulnerable.

e. Feistel Cipher

As per Wikipedia [8], in cryptography, for construction of block cipher a symmetric structure is used which is the Feistel cipher. The cipher and decipher methods are very similar, at times even identical which leads to requirement of only a reversal key of key schedule in Feistel cipher. Dong. X. and Wang. X. [9] considered the first quantum key-recovery attack against Feistel structures. This attack was successful and the cipher was exploited.

f. Data Encryption Standard (DES)

Wikipedia [10] defines DES as encryption of electronic data using symmetric key algorithm. It has a short 56-bit key which makes it insecure for most of the current applications. The procedure used for DES is repeated twice or thrice to get a double or triple DES cipher. Sandeep Kumar [11] showed that the DES can be broken within 9 days. DES takes time to examine and decrypt. DES can keep your data safe for a longer period than rest as it takes time to break and also there isn't a 100 percent assured chance of getting it right.

g. Advance Encryption Standard (AES)

Wikipedia [12] describes AES to be built on a theory known as substitution-permutation network, and is effective in both software as well as hardware. AES is not based on Feistel network like its precursor DES. AES is a version of Rijndael that has a static block size of 128 bits with a key size of 128 bits, 192 bits or 256 bits. Amir Moradi, Mohammad T. Manzuri Shalmani, and Mahmoud Salmasizadeh [13] concluded that by using Differential Fault attack, AES can be broken. Therefore, we can conclude that AES is also vulnerable to fault attacks and is not secure completely.

Table of Comparison

Ciphers	Symmetry (Symmetric or Asymmetric)	Key-size	Level of Cipher (Easy, Medium, Hard)	Level of breakability (Easy, Medium, Hard)	Issues with the Cipher
Transposition	Symmetric	Variable	Easy	Easy	Easily detected by cryptanalysis
Substitution	Symmetric	Variable	Easy	Easy	Cypher is weak and cryptanalyst can easily deduce the meaning of the ciphertext
Vigenère	Symmetric	Variable	Easy	Easy	It is a polyalphabetic cipher, therefore is weak to frequency analysis
Block	Symmetric	Variable	Easy	Easy	Allows you to encrypt message the same size as the block size
Feistel	Symmetric	Variable	Medium	Medium	Limited parallelism compared to other ciphers
DES	Symmetric	56-bit	Medium	Medium	Fails with linear cryptanalysis, has a small 56-bit key
AES	Symmetric	128, 192, 256-bit	Hard	Hard	Simple algebraic structure, every block encrypts in same way

III. FUTURE SCOPE AND DISCUSSION

The cryptographic techniques play a vital part in securing our data over the network. In this paper, we conducted a literature survey to differentiate various cryptographic methods and practices to find out which one would be the most secure to communicate over network. This study will help users in choosing the right technique to apply to their network to secure their data. This paper is a gathered place of various techniques and how they are unprotected to various attacks. This study will also prove to be of use for various researches in order to overcome the faults in these techniques and secure our data over greater extent. Referring this paper one can choose an encryption technique or combine multiple techniques most suited for their purpose to transfer their data over their network.

IV. CONCLUSION

We have conducted a survey to compare various cryptographic techniques. We compared transposition, substitution, Vigenere, block, Feistel, DES, and AES ciphers. We concluded that no cipher is absolute and is vulnerable to in some way or other. We also concluded that the AES holds an upper hand over the rest as it contains a 128-bit key which is tough to break. It also contains 192 and 256-bit key depending on how secure the user wants the data transmission to be. This study has helped us know about how various cipher techniques can be broken and how can we make them better.

V. REFERENCES

[1]. Dimovski A., Gligoroski D. Attacks on the Transposition Ciphers Using Optimization Heuristics // International Scientific Conference on Information, Communication & Energy Systems & Technologies ICEST 2003, Sofia, Bulgaria, October 2003.

[2]. R. Toemeh, S. Arumugam. Breaking Transposition Cipher with Genetic Algorithm // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 7(79). – P. 75–78.

[3]. https://en.wikipedia.org/wiki/Substitution_cipher - Accessed on 7th April 2019.

[4]. Peleg, S., & Rosenfeld, A. (1979). Breaking substitution ciphers using a relaxation algorithm. Communications of the ACM, 22(11), 598–605.doi:10.1145/359168.359174.

[5]. https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher - Accessed on 7th April 2019.

[6]. Ragheb Toemeh and Subbanagounder Arumugam Applying Genetic Algorithms for Searching KeySpace of Polyalphabetic Substitution Ciphers, The International Arab Journal of Information Technology, Vol. 5, No. 1, January 2008.

[7]. Kaplan, M., Leurent, G., Leverrier, A., & Naya-Plasencia, M. (2016). Breaking Symmetric Cryptosystems Using Quantum Period Finding. Lecture Notes in Computer Science, 207–237. doi:10.1007/978-3-662-53008-5_8.

[8]. https://simple.wikipedia.org/wiki/Feistel_cipher - Accessed on 7th April 2019.

[9]. Dong, X., & Wang, X. (2018). Quantum key-recovery attack on Feistel structures. Science China Information Sciences, 61(10).doi:10.1007/s11432-017-9468-y

[10]. https://en.wikipedia.org/wiki/Data_Encryption_Standard - Accessed on 7th April 2019.

[11]. Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer, Andy Rupp, Manfred Schimmler. How to Break DES for Euro 8,980.

[12]. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard - Accessed on 7th April 2019.

[13]. Moradi, A., Shalmani, M. T. M., & Salmasizadeh, M. (2006). A Generalized Method of Differential Fault Attack Against AES Cryptosystem. Cryptographic Hardware and Embedded Systems - CHES 2006, 91–100.doi:10.1007/11894063_8