STUDY FOR LOCKING SCRIPT FACTS PROGRAM TO DEVICE VIGENERE CIPHER AS CRYPTOGRAPHIC PROCESS

[1]Name of 1st Mr Manoj Patel
[1]Designation of 1st Assistant Professor
[1]Name of Department of 1st Faculty of Computer Science & Applications
[1]Name of organization of 1st Gokul Global University, Sidhpur, Patan, Gujarat – India

Abstract: In this paper, the security goals were described for complex encrypting and decrypting data which maintains the security on the communication channels by making it difficult for attacker to. Data can be in the form of mediocre information or information that is very important where other people may not know the contents of the data. Asymmetric encryption also known as Public-Key encryption, uses two different keys - a public key to encrypt the message, and a private key to decrypt it.

Keywords - Data, Cryptography, Vigenere Cipher, Encryption, Decryption.

INTRODUCTION

Data can be in the form of mediocre information or information that is very important where other people may not know the contents of the data [1]. Data is parts of digital information. It is usually formed in certain ways and can be in various ways, such as numbers or text. It is information in binary digital format
[2]. Data is a kind of technological information. It identifies the information from its source and splits into a separate small information
[3]. In network security, cryptography has a long history by provides a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient, where the cryptosystem is a set of algorithms combined with keys to convert the original message (Plain-text) to encrypted message (Ciphertext) and convert it back in the intended recipient side to the original message (Plain-text) [4].

If the information is stolen and falls into the hands of people who are not responsible, then this information can be misused or used as a source of illegal money search
[6]. To secure that information, good techniques are needed in turning that information into string words that cannot be understood by others. In the computer world, the tools to do this are called cryptography. Cryptography is the art of turning an original message into an unread message so that the message cannot be understood when taken by an irresponsible person. Cryptography is not easy in general
[7]. Cryptographic methods are safe enough to be used and can be a defence to avoid attacks
[8]. This method is one of the substitution methods in which the plaintext character will be replaced by the characters in the ASCII table by shifting the character's position with a key.

Encryption algorithms are functions that are used to perform encryption and decryption functions. However, some of encryption and decryption algorithms use the same key (i.e. sender, and receiver). And in other encryption and decryption algorithms they use different keys but these keys must be related.

MOST POPULAR ENCRYPTION ALGORITHMS

Asymmetric encryption also known as Public-Key encryption, uses two different keys - a public key to encrypt the message, and a private key to decrypt it [9]. Their complexity and ability to resist attack varies from one algorithm to another [10]. The main component of encryption process is the algorithms that serve basic purpose in different ways. Popularly used algorithms include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Rivest, Adi Shamir & Leonard Adleman (RSA) and Digital Signature (DSA) [11].

Data Encryption Standard (DES)

government that it was restricted from exportation to other countries.

Advanced Encryption Standard (AES)

The National Security Agency has approved 128-bit AES for use up to SECRET level and 192-bit AES for use up to TOP SECRET level. AES specifies three approved key lengths: 128-bits, 192-bits and 256-bits.

Blowfish

The Blowfish algorithm was first introduced in 1993. It is one of the most common public domain encryption algorithms provided by [14], one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security.

Rivest, Adi Shamir, and Leonard Adleman (RSA)

It's also part of Lotus Notes, Intuit's Quicken, and many other products. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

Digital Signature (DSA)

VIGENERE CIPHER

Vigenere cipher is a method of encoding the alphabet text by using a series of Caesar passwords based on the letters on the keywords. The advantage of this password compared to Caesar and other monoalphabetic codes are that they are not so vulnerable to a decoding method called frequency analysis [18]. The Vigenere code is a polyalphabetic substitution cipher. It was published by a French diplomat (and also a cryptologist), Blaise de Vigenere, in the 16th century, 1586. Giovan Batista Belasco described it for the first time in 1533, as written in the book La Cifra del Sig. Vigenere was the trigger for civil war in America, and the Confederate Army used the Vigenere code in the American Civil War. Babbage and Kasiski successfully broke the Vigenere code in the mid-19th century [19]. This type of encryption algorithm is very well known because it is easy to understand and implement. The technique to produce ciphertext can be done using number substitution or rectilinear square. The technique of substituting Vigenere by using numbers is done by exchanging letters for numbers, almost the same as a sliding code.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

Vigenere Table

RESULT & DISCUSSION

In the context of information technology, software or hardware implementation includes all post-sale processes involved in something that operates well in its environment, including analyzing requirements, installation, configuration, adjustments, running, testing, system integration, user training, delivery, and manufacturing that is required. Calculation examinations are designed to estimate the ability of an application program to add, subtract, divide, and multiply numbers quickly and accurately. In the example that will be presented, plaintext and key will be given to be processed to get the ciphertext. This test is carried out to see how accurate the application program is created and whether it is by calculations performed manually [20]. The process consists of two processes, such as the encryption process and the decryption process. The following calculation is a complete explanation and calculation of the encryption and decryption process in the Vigenere Cipher algorithm by providing two plaintext and keys.

explains the plaintext will be changed to ciphertext. Key characters must meet the length of the plaintext so that all characters in the plaintext have key pairs. The plaintext and key characters will be changed according to the values in the ASCII table. Both will be added and produce ciphertext

The ciphertext generated in the previous Table will be returned so that it produces a plaintext. Table is the result of the decryption process from the ciphertext obtained in Table. These results did not change so that the Vigenere Cipher calculation did not experience errors and failures.

CONCLUSION

This research paper carries out the work related to the Vigenere Cipher algorithm and does the encryption and decryption of data. Many researchers have worked on cryptography, but most of the algorithms have several weaknesses either caused by low security level or increase the delay time due the design of the algorithm itself. The result of the proposed algorithm of Vigenere Cipher works by shifting characters. Vigenere Cipher has a key that can be determined according to the desired number of keys. Also it can be consider as a good alternative to some applications because of the high level of security and average time needed to encrypt and decrypt a data using the same.

REFERENCES

[1] M. den Hengst and M. Warnier, “Cyber Crime in Privately Held Information Systems: Personal Data at Stake,” in 2013 European Intelligence and Security Informatics Conference, 2013, pp. 117–120.
[2] Iswanto, “Avoiding local minima for path planning quadrotor based on modified potential field,” Int. Rev. Aerosp. Eng., vol. 11, no. 4, pp. 146–154, Aug. 2017.
[3] Iswanto, O. Wahyunggoro, and A. I. Cahyadi, “3D object modeling using data fusion from laser sensor on quadrotor,” in AIP Conference Proceedings, 2016, vol. 1755.
[4] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.
[5] Ali Mir Arif Mir Asif, Shaikh Abdul Hannan, Yusuf Perwej, Mane Arjun Vithalrao, “An Overview And Applications Of Optical Character Recognition”, International Journal of Advance Research In Science And Engineering (IJARSE), July (Vol.3, No.7), 2014, Pages 261-274, ISSN 2319–8354(E) & ISSN 2319–8346(P).
[6] W. Stallings, Cryptography and Network Security: Principles and Practice. New Jersey: Prentice Hall Press, 2013.
[7] A. A. Bruen and M. A. Forcinito, Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. New Jersey: John Wiley & Sons, 2005.
[8] F. H. Khan, R. Shams, F. Qazi, and D.-E.-S. Agha, “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix,” Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, pp. 5–7, 2015.
[9] Ali Mir Arif Mir Asif, Shaikh Abdul Hannan, “A Review on Classical and Modern Encryption Techniques”, International Journal of Engineering Trends and Technology (IJETT), June (Vol.12, No.4), 2014, Pages 199-203, ISSN 2231–5381(E) & ISSN 2349–0918(P). [10] Deepak K. D. and Pawan D., “Performance Comparison of Symmetric Data Encryption Techniques”, ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4 June 2012.
[11] Frank K. G., “Channel Attack secure Cryptographic Acceleration”, 2006.
[12] Coppersmith D., "The Data Encryption Standard (DES) Its Strength Against Attacks”, IBM Journal of Research and Development, May 1994, pp. 243 -250.
[13] Chen J., Li X., Li W., Wan, W., “An improved AES Encryption Algorithm”, IET International Communication Conference on Wireless Mobile and Computing (CCWMC 2009).
[14] Bruce S., “The Blowfish Encryption Algorithm Retrieved”, http://www.schneier.com/blowfish.html, 2008.
[15] Shaikh Abdul Hannan and Ali Mir Arif Mir Asif, “Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption” International Journal of Computer Science and Software Engineering (IJCSSE), February (Volume 6, Issue 2), 2017, Pages 41-46, ISSN (Online): 2409-4285.
[16] Iana G. V., Anghelescu P., Serban G., “RSA Encryption Algorithm Implemented on FPGA”, International Conference on Applied Electronics, pp. 1-4, 2011.
[17] Rivest, R. L., Shamir, A., & Adleman, L., “Methods for Obtaining Digital Signatures and Public key cryptosystems”, communication Of the ACM Vol. 21. pp. 120—126.1978.
[18] A. Hidayat, “Algoritma Kriptografi Vigenere Cipher,” 2012.
[19] Dony Ariyus, Pengantar Ilmu Kriptografi. Yogyakarta: Andi Offset, 2008.
[20] Andini Dani Achmad, Ayu Aryista Dewi, Muhammad Roy Purwanto, Phong Thanh Nguyen, Imam Sujono, “Implementation of Vigenere Cipher as Cryptographic Algorithm in Securing Text Data Transmission”, Journal of Critical Reviews, VOL. 7, No. 1, 2017, Pages 76-79, ISSN- 2394-5125