International Journal of Research in Engineering, Science and Management
Volume-2, Issue-12, December-2019
www.ijresm.com | ISSN (Online): 2581-5792

Design and Implementation of Text Cryptography for Multi-Languages and Resolving Type Cast Issues

Tarun Kumar Mishra[1], Nimish Arvind[2]
[1]*Student, Department of Computer Science and Engineering, Poornima College and Engineering, Jaipur, India*
[2]*Assistant Professor, Dept. of Computer Science and Engg., Poornima College and Engineering, Jaipur, India*

***Abstract*: In today's world of internet data communication is very important and the whole world is running over that only. If two countries need to share the information or if they have to discuss anything related to counter the terrorism around the globe, discussion about the trade these are very vital and important communication that goes on between the two countries or two bodies. Securing data techniques have always been the talking point for the scientists, detectives, bureaucrat and or any other person that is involved with the nations and is responsible for its security. The intelligence exchange could be turn out very destructive for the countries if they don't have the technology to secure their data, in this dissertation a methodology has been proposed to implement such an algorithm which can encrypt any language data without being constrained by the length.**

***Keywords*: Text Security, Data Encryption.**

1. Introduction

HE growth in Internet and smartphone use has had a major social and commercial impact on daily life. These new technologies benefit people all over the world, and allow information to be stored, processed, and accessed in an inexpensive and widely accessible manner. Since the text message has become a popular and easy form of communication, concerns about data leakage attacks, such as hacking, hijacking, and phishing, have emerged. Users such as detectives, journalists, judges, and election officials rely on short message service (SMS) or Social Media Applications (SMAPP) to communicate with each other. Smartphone users typically send confidential information such as banking credentials (e.g., account details, passwords, and transaction information), secret missions, confidential appointments, and private identities to family members via text messages using SMS or SMAPPs. However, the standard SMS service and social media amazingly do not provide security to this type of digital data being transmitted over networks. In this case, it is required to provide secure communication between smartphone users. Since text messages via SMS and SMAPPs on smartphones are so common, cyber-attacks such as man-in-the-middle (MITM), message disclosure, and manipulation by readers (MBR) are a concern. Functionally, text messages are sent as plaintext between smartphone users and service providers (the SMS service center, social media service provider, etc.) using an available network. Text message content is stored by service providers in servers that are easily accessed. Over the last two decades, many techniques have been proposed to improve the efficiency of text steganography in digital texts, but these methods have low embedding capacity and low robustness against distortion attacks. In other words, they are not able to embed a high capacity of secret information through a short message.

Cryptography is logic of mathematical manipulation of data (cipher text) with some text (Key). To convert plain text to cipher text encryption algorithm is applied on plain text using key. And to convert cipher text to plain text decryption algorithm is applied on cipher text using key. Previously encryption and decryption algorithm, some algorithms are compulsory to produce key at first. Throughout cryptography, there are 3 basic processes- Key Generation, Encryption and Decryption procedure.

In cryptography, we couldn't care less in the event that somebody is listening stealthily upon us however in certain circumstances classification winds up vital and we need to shield the data from untouchables. In these circumstances, the job of cryptography becomes possibly the most important factor. Cryptography is the system to move data safely between two gatherings without getting interceded by outer components. Cryptography includes a calculation and a key incentive to change over the data into an organization which isn't reasonable to anybody aside from the members. The calculation must be effective and simple to be figured by the members associated with correspondence. The key is utilized alongside the calculation so we can utilize the calculation over and over with various key an incentive as it is extremely hard to create another calculation each time we need to impart some data to somebody.

2. Literature survey

Data security can also play important role in national security as well, during the wars if two units of defense want to communicate their plans they need to be very sure that the data

they are exchanging is secure and safe and is intended for their counterparts only and not any other third party intruder [1].

As security is the major issue in today's world, it is just said that to secure the information, data hiding technologies are used to protect the data and any other information i.e. being transferred using communication channels. Security is though not new, it's unprecedented the way it had grown into a part of day-to-day life now a days. The codes people use for entering in their extremely secured homes, biometrics like scanning retina technology, finger printings, secure wearable devices etc. that recognizes as staff enter in workplace buildings, to scanners at railway stations or airports to maintain safety, security technique is just portion of day-to-day life as the cell phone or vehicle. Each and all people are surrounded by secret communication now a days, where different types of communication and transmitting data performed by many people like encrypted particulars of credit card to an online store and on disaster note it is a terrorist plot to hijackers [2].

Cryptography is the technique of encoding the secret facts in a manner by which other person cannot recite it, only the user holding the key i.e. the sender and the authorized receiver. More advanced cryptographic techniques ensure that the secret data which is communicated should remain unaltered in transmission. Cryptography can be understood by these basic but some very important terms [3].

Decryption is the process of decoding /deciphering or transforming an enciphered data to its original format. It means its opposite of encryption [4], [5]. Taking a cipher data and changing the data to plain text. It is necessary to not forgetting that there is a connection in the middle of the procedures called encryption and decryption. If a text is encrypted using a particular technique and decrypted by another technique than this process of decryption will going to result the trash text not the original data.

Steganography is the skill of concealing secret data by embedding it into covered passages so that its secrecy is maintained inside the carrier message. The denotation of word Steganography in Greek is "concealed script". Now day, Steganography means hiding secret data in any file like sound, image, video file. The idea has come about a thousand years ago, but is applied to digital data where safety of data transmission is a must. It is a technique of transmitting encrypted information deprived of knowing message's existence [6].

In ancient Greece when people have to send some secret information then they used images and messages carved on wooden planks than wrapper them with the wax, and tattoos were done on shaved head of trusted messenger, and then wait till the hair grow back on messenger's head, and then to read the message head shaving was done again, this was commonly practiced. In World War II, some other technologies for steganography were developed that completely made of invisible inks. Invisible inks that used earlier can contain fruit juices, milk, urine and vinegar that blacken when heated. The following message was led during the World War II by the German scout [5]. When to translate through invisible inks became easy, null ciphers were practiced.

Microdots are text as well as images that are photographic and compacted to the dimension and form of a point or the 'i' & 'j' dots. Microdots were generally directed by texting a letter encompassing gaps of i's, or j's, the letters could read by the use of a microscope by determined receiver [7]. As of the extremely minor dimension of the microdots the letters characteristically went unobserved by supervisors.

The September 11 attacks (denoted as 9/11), a sequence of four synchronized terrorist attacks by the Islamic terrorist group al-Qaeda held on September 11 in the year 2001 on New York City (United States) and the Washington, D.C. metropolitan area. Along with 19 hijackers overall 2,977 victims were dead in those attacks [8].

Al-Qaeda hijackers captured 4 passenger flights to be crashed on buildings in suicide attack. Two among 4 flights blasted into the World Trade Center complex in New York City [9]. The third airplane was down into the Pentagon (the command center of the United States Department of Defense). The fourth plane was besieged at Washington, D.C. [10] but gone down into a ground nearby Shanks Ville, Pennsylvania.

Image steganography have become prevalent technique in current years than further types of steganography, maybe due to the abundance of electric image data presented with the coming of cameras and internet spreading. Image steganography usually includes concealing data in the logically arising noise inside the picture, and delivers good scheme for such methods.

Maximum types of data comprise certain type of unwanted bits termed as noise. Inside an auditory data, the idea of unwanted bits is understandable. For pictures, in the process of interpreting an analog image as digital image however, noise generally indicates to the flawed characteristics [11].

When concealing information in Audio files the procedure generally in use is lower bit encrypting that is a bit similar to technique of inserting least bits that is usually worked in pictures. This is quite chancy technique for users to utilize because to disguise data within a sound object the trouble with lower bit encrypting which is generally perceptible to the ear of humans. Other technique performed to hide data within a sound file is Spread Spectrum. Noises are extra up to the signal in this process. The frequency spectrum hidden inside a carrier is used to spread the information across. Obscuring echo data is other practice of wrapping up data into sound file is. To attempt and conceal data this process echoes used in audio files. Just by adding an extra bit of sound to an echo into audio file info can be hidden. Its skill to perk up the sound bit of the audio into an audio file makes this process of hiding information inside audio files better than others [12].

3. Proposed work

Text cryptography allows you to transmit data from one end to another end securely. Though the text cryptography can be

very complex at a time and it may result in loosing data completely and permanently as well. An algorithm has been postulated here in this dissertation which deals with the complex programming for text cryptography encryption and its decryption.

Step 1: Plain input text:

This is the beginning of the algorithm and this deals with the text input from the user. The applied algorithm deals with the text input from the user. The implemented algorithm gives you the liberty to enter text in any language and of any length as well.

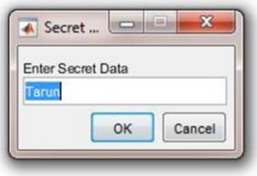

Fig. 1. Text data input dialogue box

MATLAB pops up the dialogue box to fetch the user input data which can be of any language and any length, entered data is of length 5 and is of English alphabets.

Step 2: Length Identifier:

This section of the algorithm deals with the calculation of the length of the secret data entered so that the forthcoming steps of the algorithm can perform accordingly and it will be required for making all the applicable calculations for further encrypting the secret data.

Step 3: Rotation Coefficient:

This section of the algorithm selects the rotation coefficient to rotate the entered text. The text entered is first converted to the binary dataset and then the length gets calculated which becomes the range of the rotation coefficient. The implemented code works in such a way that the range of the rotation lies in between 1 to length of the string or 1 to total characters present in the string entered.

Step 4: Validation:

The code performs a check over the validation of the users, where the user is authenticated or no to execute the developed algorithm. This can be done using the MATLAB pcode files where the editing of the credentials will not be possible and the visibility of the credentials is hidden.

Step 5: Rotated Matrix:

Rotation coefficient is now being used for rotating the matrix by the received coefficient. In order to rotate and change the original position of the matrix this block performs the loop to rotate the 1-D matrix according to the rotation coefficient.

Step 6: Concatenation of Rotation Coefficient:

The selected rotation coefficient is needed to be transferred to the receiver for the retrieval of the transcript code. The concatenation process is to add the rotation coefficient as a suffix or prefix to the augmented matrix for reducing the execution time as adding complexity will add more execution time.

Step 7: Addition of Coefficient to the Augmented Matrix:

The above section concatenates the rotation coefficient however this won't be enough and the rotation coefficient will be added to individual bits of the whole augmented matrix to add the more security to the encrypted text.

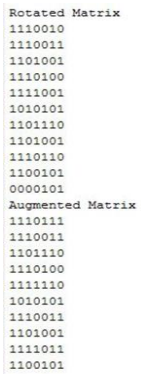

Fig. 2. Augmented additive matrix

Table 1
Algorithm and Result Comparison

Factors	DES	3DES	AES	IDEA	RSA	Our Work
Developed By	IBM in 1975	IBM in 1978	Vincent Rijen Joan Daemen	James Massey of ETH Zurich and Xuejia Lai in 1991	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978	Tarun Kumar Mishra
Key Length	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192 or 256 bits	0 to 256 bits	Depends on number of bits in the modulus n where n=p*q	Plus one what has been entered
Round (s)	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key	8.5 rounds	1	1
Block Size	64 bits	64 bits	128	64 or 128 bits	variable	Variable (minimum 8 bits)
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher	No Cipher Required only Rotation Coefficient
Speed	Slow	Very Slow	Fast	High Speed	Slowest	Elapsed time is 0.019974 seconds.
Security	Not Secure	Adequate Security	Excellent Security	High level of security	Least Secure	Adequate Security with Typecast Resolved
Languages	Singular	Singular	Singular	Singular	Singular	Multi-Language

The addition of the rotation coefficient to the augmented matrix is a mandatory task as it will help in covering up the rotation coefficient to make it more secure and safe.

Data typecasting is a big major issue of any transmission or data transformation based applications, when a variable enters any process the output generated should be of the same data type as the conversion of it back to the normal should be smooth and accurate. The resultants of the implemented code is valid for all the language and for any data length.

4. Results

The proposed work is not restricted to any single language it is valid for multiple languages and can be used or tested thoroughly.

5. Conclusion and future scope

Cryptography can be a technology that develops, but as long as security is made by man, cryptography is as good as the practice of people who uses it. This paper is focused on the different security issues for providing a secure and effective cryptography technique over the block cipher.

Most of these issues occurred when users leave keys unattended, keys that were chosen were easy to remember or maintain the same keys for years. This can be resolved by the suggested model, using the encrypting key that existed independently as an external tool by managing keys sequentially. The major issues for any cryptographic algorithms has been revoked here, majorly the length constraint and the language constraint.

The text cryptography can be enhanced for the dynamic algorithm which can evolve itself regularly and the database connectivity can help in saving a lot of time for repeating keywords randomly so that the system can never be out of the keys and will keep itself updated.

References

[1] K. Rabah, “Steganography-The art of hiding data,” Information Technology Journal, vol. 3, pp. 245-269, 2004.
[2] Gupta, Chhavi, and Prateek Thakral. "ASCII conversion based two keys V4S scheme for encryption and decryption—A four step approach." In Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on, pp. 1-6. IEEE, 2017.
[3] Jammi Ashok et. al. “Steganography: An Overview”, International Journal of Engineering Science and Technology Vol. 2(10), pp. 5985-5992, 2010.
[4] Arvind Kumar, Km. Pooja “Steganography- A Data Hiding Technique” International Journal of Computer Applications, Vol. 9, No.7, November 2010.
[5] T. Sharp, “An implementation of key-based digital signal steganography,” Lecture Notes in Computer Science, Science Direct vol. 2137, pp. 13–26, 2001.
[6] Shivani, Virendra Kumar Yadav, Saumya Batham, “A Novel Approach of Bulk Data Hiding using Text Steganography”, 3rd International Conference on Recent Trends in Computing (ICRTC), Procedia Computer Science vol. 57, pp. 1401 – 1410, 2015.
[7] F.L. Bauer, “Decrypted Secrets Methods and maxims cryptology, 4th Edition”, springer Education pvt. Ltd, 2010.
[8] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O. Gorman, “Electronic marking and identification techniques to discourage document copying,” IEEE Journal on Selected Areas in Communication, vol.1, pp. 1495-1504, 1995.
[9] Banerjee, S. Bhattacharyya, and G. Sanyal, “Novel text steganography through special code”, International Conference on Systemics, Cybernetics and Informatics.
[10] S. Changder, D. Ghosh, and N. C. Debnath, “Linguistic approach for text steganography through Indian text”, 2nd International Conference on Computer Technology and Development, pp. 318-322, 2010.
[11] Casualties of the September 11 attacks, “Nine facts about terrorism in the United States since 9/11”. The Washington Post, September 11, 2013. Retrieved November 26, 2015.
[12] Pravin R. Kamble, Prakash S. Waghamode, Vilas S Gaikwad, Ganesh B. Hogade, “Steganography Techniques: A Review”, International Journal of Engineering Research & Technology, Vol. 2 Issue 10, October 2013.