International Journal For Technological Research In Engineering
Volume 6, Issue 6, February-2019 *ISSN (Online): 2347 - 4718*

DIFFERENT POSSIBLE ATTACKS ON CRYPTOGRAPHY: A REVIEW

Chhotu Ram Jat[1], Shalini[2]
[2]AP, [1,2]Jaipur Institute of Technology Group of Institution, Jaipur

Abstract: In the era of digital world, security of 'information' has extremely important to both organization as well as individuals. When information is stored or transmit by a message or packets of messages by some channel there, be supposed to be some system or method to protect the information from interruption and hacking. If information hacked by the wrong one there might occur various problems. Therefore, we need to secrete data in such a way that no any third person or party can't hack that exact communication. The present research focuses on the annoying to being enhance the basic Playfair technique (5x5 matrix) to two matrix of size 12x18 size of rectangular matrix, attacks probable on data and tackle these attacks by means of right types of contradict measures. In addition, to secure the key of the playfair technique is need to make sure the safety measures of a given data by some kind of mechanism and increase the security, confidentiality, integrity as well as availability.

The cryptography algorithms are those algorithms that can convert the data readable form to unreadable form as well as unreadable from to readable form. According to key, cryptography algorithms are of two types first is symmetric key algorithm and other is asymmetric key algorithm. If the encryption and decryption both are done using the same key then it is called the private key or Symmetric cryptography. Symmetric-key cryptography is where senders and receivers share the same keys. So those keys are used for encryption and decryption. They are used mainly with block ciphers and stream ciphers.

I. CRYPTANALYSIS

Cryptanalysis means "decrypted the code or code breaking". It is the art of defeating cryptographic systems, and gaining access to the process of encrypted messages, without being given the key. In this goal are the same, methods and the techniques of cryptanalysis have a big change from first to last history of cryptography, and increase complexity of cryptographic algorithm, ranging from paper as well as pen methods of past to mathematically advanced programmed schemes of present. [4], [5]

II. BRUTE FORCE ATTACK

An attack on a cipher text message, wherein the attacker attempts to use all possible permutation and combinations, it is called Brute force attack. [4]

In this type of attack attacker tries to enter every possible key to get the original text. It is like if we have bunch of several keys and don't know the exact key to open the lock then we are try for every key in the available bunch until the lock is going to open. So in this case attackers try at least half of possible key to get the data. So this is time consuming for attacker as every time he has to try new key if the entered key is not work until original text is not visible.

And while performing this attack if that person got the success then the system will be compromised and he will get the exact key and possibly he come to know the all past and future message sent with the help of that key.

In the above we see the cryptanalysis and brute force attack by the person who try to find the secret key. Attacker normally have cipher text when he interfere between the two authorized persons so it is just consideration that he know the cipher text only but we always assume that he have an idea about the algorithm used for encryption. So if this information is available to attackers then he can go for the brute force attack in which he try all possible combination of secret keys. As we discussed previously if we used the larger key space then it is practically impossible to try all the keys because range is very large. So attacker depend on the cipher text for every operation of encoding process, try to apply various mathematical test to get the original output. To do these entire things attacker must have some knowledge about the type of plaintext he is searching for. This type can be anything like English sentences, exe files, and financial transaction file of any accounting organization or any type of file which is sensitive for that person. [4]

When attacker only attack on the cipher text then it is very easy to defend against this type of attack because in this attack attacker has minimum information about this and so it is not much easy to workout with it. In some of the cases attacker have more information about these things possible he is capable to get the plaintext messages and its encryption process. Also there is a chance of getting some idea about the original text patterns which regularly visible in the message. For example if we consider the C program in that it always start with some common code which can be easily guess or if we are dealing with the electronic fund transfer then this also have some specific pattern which is guessable. So in this way attacker is able to assume the key and go for the further operation to find all things which is required to harm or damage any one. [4]

Plain text attack is also referred as word attack. If attacker is operating with encryption process of some particular type message then by experience or by working with that environment style he will get some knowledge about that message means which type of it is. Also id attacker get specific information about that message then some portion of the message may know by some processing and guessing too. For example if one user transmitted one C program code to another user and this code is critical or sensitive for both these person. And while transmitting this code, if attacker got that code and he make some research and work for hours to decode then after some work he get the knowledge that this code contain some specific header, some comment line, some specific special character and many such things which are normally available in the program code then he will come to know that this is some program code.

Also if while transmitting the message between sender and receiver, sender uses the same technique, same style for encryption and similarity between the keys then structure of message will be same and attacker will see that there is same structure in generating messages. It means if pattern of message is repeated then the security will be compromised as attacker will not find more problem while decoding it. [4]

The above case is never happened as only weak algorithm fail when cipher text attack happen and in general all the encryption algorithm are designed in such a way that they must stand whenever such attack take place.

The encryption method we are using will be totally secure if and only if the generated output in the form of cipher text does not contain the sufficient information to define the original plaintext in any possible way. In this case size and how much is the output text does not matter. Also there is no meaning how much span attacker has for the decryption; it is not possible to decode the information as required information is not present at that instance. There is some exception of the above method called as one time pad (OTP), no algorithm is totally secure in today’s world. So every user who is using the algorithm for encryption process attempt to match the following principal:

- The price of decoding the cipher beats the value of the encrypted information.
- The span needed to decode the cipher surpasses the beneficial lifetime of the information.

When algorithms apply both the above principals then that algorithm is called as sufficiently secure. But in fact it is not easy to follow the above completely and difficult to calculate the effort required finding the correct solution.

Everyone who worked in the security system accept the fact that if attacker identify for the specific pattern then there is more possibility that all secret information will be exposed to attacker and this will affect the past and future operation of that user. As user will never know that attacker cracked the secret key and he is getting all the information in original form. And the original user will transmitting his critical information to the sender continuously, sender will always thought that his information is secure and method is sufficient strong enough to protect all his important work. [4]

The brute force attack try for every possible combination of the key by which the coded information will be decoded and in this process the attacker who is using this attack nearly half of the possible combination for getting success. Data encryption standard usually called as DES use 56 key size and on the other hand triple DES uses 168 bit key size. And at later stage in the case of advanced encryption standard called as AES uses minimum 128 bit key size which may vary as per the user. This all are the key size only but in the operation of internal part there are various permutation and substitution process are available which make the encryption process more and more complex. Many times some encryption technique uses multiple key with proper combination. After getting everything it is not easy to decrypt the data as after some time span the knowledge of such information become meaningless. But now many people uses parallel microprocessor so there may be a possibility of getting success. [4]

The size of key area in this dissertation the modified two 12X8 playfair cipher is 96!X96! (Factorial 96X Factorial 96). As the key area is very large it will be very hard for modified cipher. Thus the modified two 12x8 play fair cipher algorithm is stronger than traditional cipher.

III. MAN-IN-THE-MIDDLE ATTACK

It occurs, where the mugger furtively relays and probably alters the communiqué between two parties who suppose they are in a straight line communicate with each other. Example of this attack is active eavesdropping, in which mugger makes self-regulating links with fatalities as well as relays communication between them to make them assume that they are talking directly to each other over a secret link, when in fact the mugger controls the complete conversation. The mugger must be capable to interrupt all proper messages passing between the two victims and inject new ones. This is easy in many conditions. [29]

IV. CIPHER TEXT ONLY ATTACK

In this, attacker does not have any clue about PT. She has some or all CT. The mugger analyzes CT at spare time to try and figure out unique PT. Based on frequency of characters attacker attempts to guess PT. Apparently, more CT available to mugger, more are changes of a thriving attack.[4] The cryptanalyst can start on a CT only attack. However number of two 12X8 PF matrix diagrams to be search would be 96X96X96X96 = 84934656 which is much larger than 26 X 26 = 676. Thus the Thus the modified 16X16 Play fair matrix algorithm is stronger than the traditional cipher.

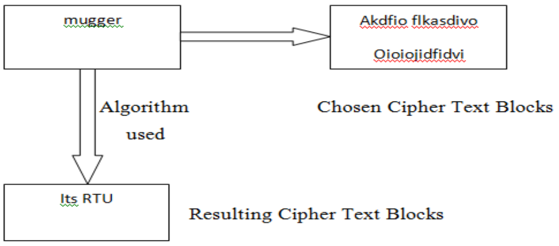

Fig.3 Chosen Cipher Text Attack [4]

Known Plain Text Attack

In this attack, attacker has some pairs of PT and related CT for those associated pairs, with this data, attacker try to discover other pairs and then, know more PT. [4]

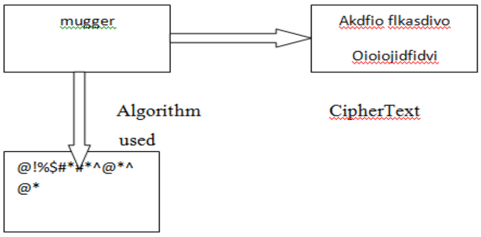

Fig 1 Cipher Text Only Attack [4]

V. CHOSEN PLAINTEXT ATTACK

In chosen plain text, attacker selects a PT block and try to discover encryption of same in CT. At this time, attacker is capable to choose data to encrypt. Like this, attacker calculatedly choose the patterns of CT that result in obtaining more data about key.[4]

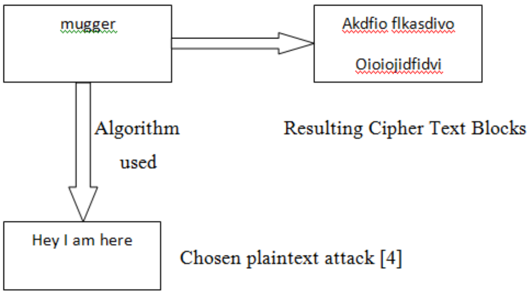

Fig 2 Chosen Plaintext Attack [4]

Example Differential Cryptanalysis

In this, a chosen plaintext attack to seeks to find out a connection between cipher texts produced by two correlated plaintext. It focuses on arithmetical analysis of two inputs as well as two outputs of the cryptographic algorithm system. [21]

Chosen Cipher Text Attack

In this attack, attacker knows about cipher text (CT) to be decrypted, encryption method that was used to create this CT as well as the related PT block. There is job of attackers, to find out key used for the encryption process. [4]

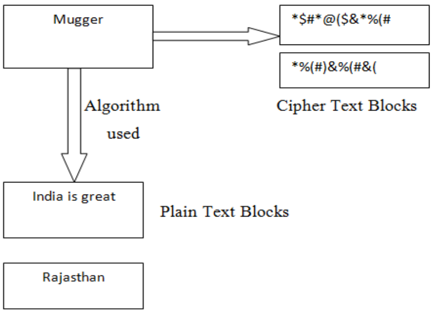

Fig 5 Known Plain Text Attack [4]

VI. CONCLUSION

In the era of digital world, security of 'information' has extremely important to both organization as well as individuals. When information is stored or transmit by a message or packets of messages by some channel there, be supposed to be some system or method to protect the information from interruption and hacking. If information hacked by the wrong one there might occur various problems. Therefore, we need to secrete data in such a way that no any third person or party can't hack that exact communication. The present research focuses on the annoying to being enhance the basic Playfair technique (5x5 matrix) to two matrix of size 12x18 size of rectangular matrix, attacks probable on data and tackle these attacks by means of right types of contradict measures. In addition, to secure the key of the playfair technique is need to make sure the safety measures of a given data by some kind of mechanism and increase the security, confidentiality, integrity as well as availability.

REFRENCES

[1] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix". International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[2] Ravindra babu, Udaya Kumar, Vinaya babu, "An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method", IJCA,0975-8887, Vol. 17, No 5, March 2011.

[3] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani," A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, 1793-8201 December, 2009.

[4] Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar, Dr. A.Vinaya Babu3 and Dr. M. Thirupathi Reddy, "A Block Cipher Generation Using Color Substitution", © International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28 2010.

[5] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa, "A DNA and Amino Acids-Based Implementation of Playfair Cipher" , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 3, 2010.

[6] Subhajit Bhattacharyya, Nisarga Chand & Subham Chakraborty, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps" International Journal of Advanced Research in Computer Engineering & Technology Volume 3, Issue 2, February 2014.

[7] Packirisamy Murali and Gandhidoss Senthil kumar, "Modified Version of Playfair Cipher using Linear Feedback Shift Register", International Conference on Information Management and Engineering, , Page 488-490 2009.

[8] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique", IJCSNS International Journal of Computer 280 Science and Network Security, Vol.10, No.5, , Page 280-285 May 2010.

[9] Sriram Ramanujam and Marimuthu Karuppiaj, "Designing an algorithm with High Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No. 1, Page 106-111 January 2011.

[10] Shiv Shakti Srivastava, Nitin Gupta, "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[11] Gaurav Agrawal, Saurabh Singh, Manu Agarwal, "An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text", Journal of Current Computer Science and Technology Vol. 1 Issue 3 10-16 2011.

[12] Packirisamy Murali and Gandhidoss Senthilkumar, "Modified Version of Playfair Cipher using Linear Feedback Shift Register", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[13] Harinandan Tunga, Soumen Mukherjee, "A New Modified Playfair Algorithm Based On Frequency Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

[14] Monika Arora, Anish Sandiliya, and Jawad Ahmad Dar," Modified Encryption Technique by Triple Substitution on Playfair Square Cipher Using 6 By 6 Matrix with Five Iteration Steps" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 4, 2015.

[15] S.S.Dhenakaran, and M. Ilayaraja," Extension of Playfair Cipher using 16X16 Matrix", International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012.

[16] Sanjay Basu, and Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012.

[17] Sagar Gurnani, Nitish Mhalgi, Samyukta Iyer, and Deepika Dixit," Modified 3-D Playfair Stream Cipher", International Journal of Computer Applications (0975 – 8887) Volume 84 – No 15, December 2013.

[18] Ali Mir Arif Mir Asif, and Shaikh Abdul Hannan," A Review on Classical and Modern Encryption Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 12 Number 4 - Jun 2014.

[19] Ayushi Kansal, Shruti Sneha, and Manish Kumar Patel," Modifying Playfair Cipher by Using DNA and Amino Acids", International Journal of Education and Science Research Review , E-ISSN 2348-6457, Volume-3, Issue-2,. www.ijesrr.org April- 2016.

[20] Nisarga Chand, and Subhajit Bhattacharyya, "A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1, January 2014.

[21] Cryptography, Cryptography portal, http://en.wikipedia.org/wiki/Cryptography.