International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-1, 2019.
ISSN: 2581-3404 (Online)

A Novel Approach to Security using Extended Asymmetric Based RSA Algorithm

Dr. Sunil Gupta [1], Pawan Tiwari [2], Dr. Deepak Choudhary 3

[1]**Head & Professor, Department of CSE, IET, Alwar (India)**

[2]**M. Tech Scholar, Department of CSE, IET, Alwar (India)**

[2]**Associate Professor, Department of CSE, IET, Alwar (India)**

[1]**sunilgupta8764@gmail.com**

ABSTRACT
The information over the network in the presence of the third party then it is very necessary to protect our data from the attacker's, in the series to protect the data we are using the cryptography algorithms. Day to day the new cryptography algorithms are found and there is modification in the previous algorithm also. According to the key the encryption algorithm are of two types. First is symmetric key algorithm and second is asymmetric key algorithms. This is the review work for searching the algorithms which are already derived and discovered, to find the working, advantage and disadvantage of those algorithm. How they algorithm are encrypt and decrypt the data.

Keywords:- RSA, Network, Cryptography, Diffie-Hellman.

INTRODUCTION
In cryptography we need to hide the data in such a way that no any third person or party can't hack the exact message. Even for static data, to prevent the misuse of data there should be some mechanism so that if a third party hack the data he will not be able to find out the right meaning of the data. Hence Cryptography plays an important role in data communication in today's digital world or in internet. Modern cryptography is part of mathematics and technology of computer science. Applications of cryptography include all computer passwords, ATM cards, and electronic commerce.

The present research focuses on the trying to being enhance the basic Playfair technique (5x5 matrix) to 16x16 size of rectangular matrix with the help of RSA algorithm (asymmetric key cryptography), attacks possible on information and tackle them with right types of counter measures. and to secure the key of the playfair technique is the need to ensure the security of a given message by some kind of mechanism and increase the security, confidentiality, integrity and availability.

Aftab Alam et al. in [1] this paper the original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair cipher. The symbols "*"and "#" are included in the matrix which create one-to-one correspondence between the plaintext and the cipher text. So the encryption and decryption process is unambiguous and easy. The text is more unreadable when these symbols appear in the resulting cipher text. Also this method can be extended to encrypt and decrypt the messages of any language by taking a proper size matrix. Ravindra babu et al. In [2] the existing playfair algorithm, its merits and demerits. The existing playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. For this in this paper an enhancement to the existing algorithm, that a 6 X 6

matrix can be constructed. There is total 36 character, where all the 10-decimal numbers (0-9) and 26-alphabets of English language in upper case. V. Umakanta Sastry et al in [3] this paper, it generalized and modified the Playfair cipher into a block cipher. The use of the ASCII values in playfair. The use of 7-bit ASCII values increases character support to 128 characters. In this paper uses a key matrix of size 8×8 in which the key K consists of 64 distinct numbers, denoted by K_i, where i = 1-64 and each number lies between the ASCII limit of the 0-127. It was found to be breakable with some amount of computation, as the structure of the plaintext is not that much dissipated in the corresponding cipher text. Lt. Ravindra Babu Kallam et al. In [4] this paper, it addresses the problem in a completely different way by generating a Block Cipher using Color Substitution. Binary values of the 7-bit ASCII codes are used along with corresponding colors of ARGB color model. In this paper "Play Color Cipher" substitutes each character of plaintext with a color block from an 18 decillions of colors. Color limit of the ARGB color model is N = 256×256×256×256 = 4294967296. With this we have the following problems: It is a time consuming process for both encryption and decryption, It is difficult for the crypt analyzer to analyze the problem. Also suffers with the problems in the existing system. Mohamed Hashem et al. in [5] this paper, it modifies the Playfair cipher significantly by introducing the DNA-based amino acid structures to core of ciphering process. A binary form of data, such as plaintext messages, or images are transformed into sequences of DNA nucleotides. Subsequently, these nucleotides pass through a Playfair encryption process based on amino-acids structure. The primary idea behind this encryption technique is to enforce other conventional cryptographic algorithms which proved to be broken, and also to open the door for applying the DNA and Amino Acids concepts to more conventional cryptographic algorithms to enhance their security features. But they were unable to clearly handle the problem of ambiguity as performed by our algorithm. Subhajit Bhattacharyya et al. [6] in this paper which includes a rectangular matrix having 10 columns and 9 rows and six iteration steps for encryption as well as decryption purpose. This 10 x 9 rectangular matrix includes all alphanumeric characters and some special characters. In this modified playfair cipher six different keys and six iteration steps used to make the encrypted message stronger than the traditional playfair cipher. Packirisamy Murali et al. [7] in this paper have attempted to implement modified Playfair cipher using Linear Feedback Shift Register. The classical Playfair cipher is not secure because it produces only 676 structures. With mapping of random sequences to classical Playfair cipher, increases the security of the transmission by many folds. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of cipher text are sufficient. Fauzan Saeed, Sriram Ramanujam, Shiv Shakti Srivastava et al. In [9-10] focused on the well known classical techniques the aim was to induce some strength to these classical encryptions for that purpose blended classical encryption with the structure of modern techniques like DES and SDES.

Caesar's cipher

Caesar's cipher was invented by Julius Caesar around 100 B.C. - 44 B.C., and used during his military campaigns. This cipher is one of the earliest and simplest substitutions. The message (or plaintext) is encrypted by changing each letter into a fixed number and then replacing each number with a new letter which is also in the alphabet. The problem with this method is that Caesar's ciphers are very easy to break. Caesar's cipher is an instance of a substitution cipher. In Caesar's cipher each letter is substituted with a different letter (three letter down) from the alphabet. By using the frequency of occurrence of letters in the languages (i.e. English or others), these substitution ciphers are very easy to break.

RSA cryptosystem

RSA cryptosystem was developed by these three, Ronald Rivest, Adi Shamir and Leonard Adleman in 1978. It has become a standard public- key cryptography used to encrypt private data, and it was the first published public key system. The

high level of security of RSA algorithm depends on the difficulty of factoring the large numbers which are products of two large primes. Around the 1980s, scientists noticed that even though this difficulty occurred, it still did not achieve sufficient security. Therefore, they developed a strong method for security which created a hypothesis about the weaknesses of an adversary. This method is used with specific computational algorithms to meet the requirements of security. In 1984 the ElGamal public-key encryption appeared. It was based on the discrete logarithm problem and competed with the RSA cryptosystem.

Process in RSA algorithm

The RSA algorithm is a public key cryptographic algorithm that is used to help ensure data (information) communication security. It is simply based on the two main cryptographic processes. First, using a public key it converts an input data or file called PT into an unrecognizable encrypted output called CT (EP), such that it is impossible to recover original PT without the encryption password or key in a reasonable amount of time. Second, using a private key, RSA algorithm then converts the encrypted data back to its original form DP. Today it is used in email programs, web browsers, virtual private networks, mobile phones and secure shells. Until recently, use of the RSA algorithm was very much restricted by patent and export laws. However, patent has now expired and US export laws have been relaxed. The challenges of RSA are to develop an algorithm in which it is impossible to determine private key and two prime numbers.

1. Choose two prime numbers which are very large, P and Q Calculate N=P*Q.
2. Select the public key E (encryption key, which is known to every one) such that it is not a factor of the (P-1) and (Q-1).
3. Select private key D (decryption key) such that following equation fulfill this condition; (D*E) mod (P-1)*(Q-1)=1
4. For encryption , calculate the cipher text (CT) as, CT =PT ^{E} mod N
5. Send CT as the cipher text to receiver.
6. For decryption, calculate the plain text PT from the received cipher text CT as follows: PT=CT^{D} mod N.

Diffie-Hellman cryptosystem

This is the first public-key cryptosystem that was invented by Whit-field Diffie andMartin Hellman, working in collaboration with Ralph Merkle in 1976. This cryptosystem uses two different keys, but they are related: a public key and a private key. Both keys are secretly generated. Basically, the public key is used for encryption part while the private key is used for decryption. The Diffie-Hellman algorithm is based on the difficulty of the discrete logarithm problem. Even though Diffie achieved the concept of an asymmetric cipher, he did not really get the precise function that met his requirements. This only solved the key distribution. However, he inspired other mathematicians and scientists to discover another cipher, the RSA cryptosystem which is discussed next.

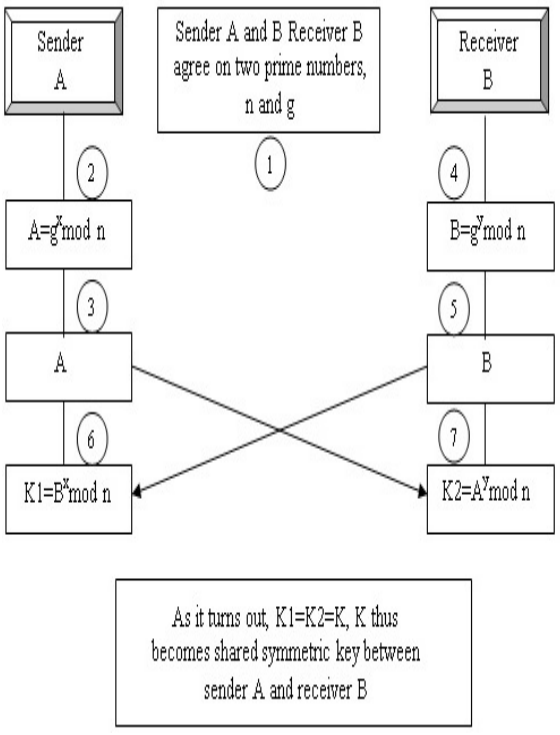

Fig. 1: Diffie-Hellman key exchange method

This algorithm is based on the one-way function. As the name implies, the function is only one-way i.e. there given some input values it is relatively easy to compute result. However, it is extremely difficult, nearly impossible to determine the input values given result .In mathematical terms, given x, computing the function f(x) is relatively easy, but given the function f (x), computing the value of x is very-very difficult. The one-way function used by RSA is the multiplication of the two very large prime numbers. It is easy to multiply them but extremely difficult, a little impossible and time consuming to factorize them.

2. DIFFERENT POSSIBLE TYPES OF ATTACKS

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 through the history of cryptography, and increasing complexity of the cryptographic algorithm, ranging from the paper and pen methods of the past to the mathematically advanced computerized schemes of the present. [4], [5]

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]

The size of the key domain in this thesis the modified 16X16 playfair cipher is 256! (Factorial 256). As the key domain is very large brute force attack will be very difficult for the modified cipher. Thus the modified 16X6 play fair cipher algorithm is stronger than the traditional cipher.

Cipher text only attack

In this type of attack, the attacker does not have any clue about PT. She has some or all CT. The attacker analyzes CT at leisure to try and figure out original PT. Based on frequency of letters attacker makes an attempt to guess PT. Obviously, the more CT available to attacker, more are the changes of a successful attack. [4]

The cryptanalyst attacker can launch a CT only attack. However the number of 16X16 PF matrix diagrams to be searched would be 256 X 256 = 65536 which is much larger than 26 X 26 = 676. Thus the modified 16X16 Play fair matrix algorithm is stronger than the traditional cipher.

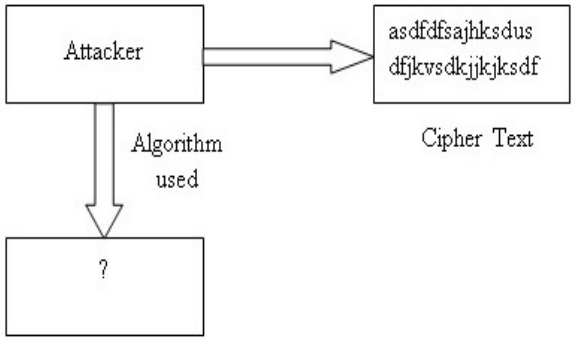

Fig 2: Cipher text only attack [4]

Chosen plaintext attack

In chosen plain text, the attacker selects a PT block and tries to look for encryption of same in the CT. Here, the attacker is able to choose the message to messages to encrypt. Based on this, attacker intentionally picks of patterns of CT that result in obtaining more information about key.[4]

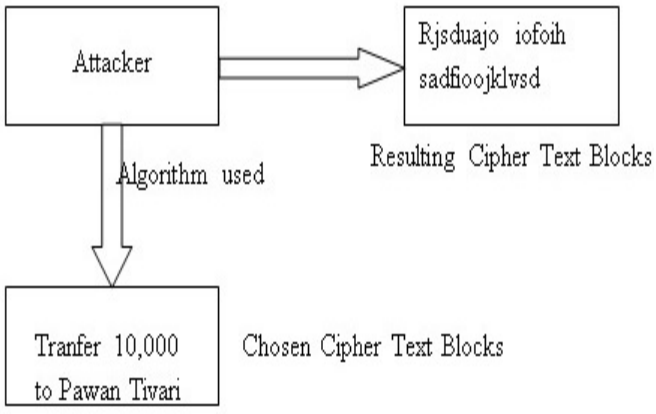

Fig 3: Chosen plaintext attack [4]

Chosen cipher text attack

In chosen cipher text attack, the attacker knows cipher text to be decrypted, the encryption

algorithm that was used to produce this CT and the related PT block. The job of attacker is to discover the key used for encryption. [4]

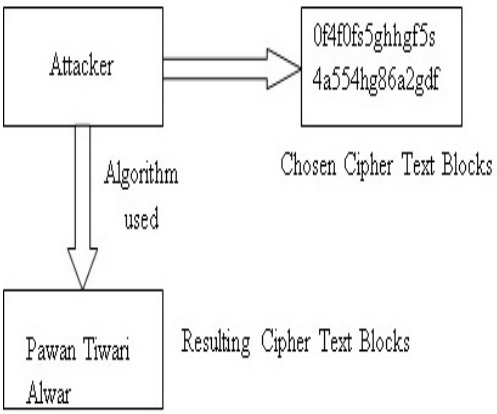

Fig 4: Chosen cipher text attack [4]

Known Plain text attack

In the plain text attack, the attacker has some pairs of PT and related CT for those pairs. Using this information, attacker tries to find the other pairs and therefore, know more and more of the PT. [4]

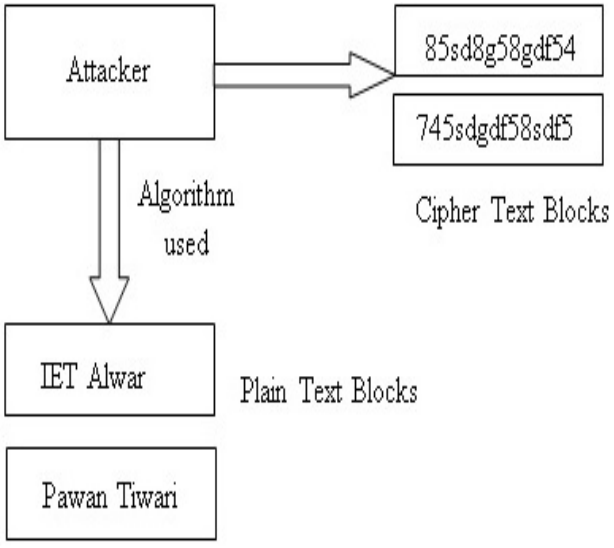

Fig 5: Known plain text attack [4]

LITERATURE REVIEW

The main limitation of the playfair algorithm is that it supports only 25-alphabets of English language. Over years several attempts have been made to increase character limit of its dataset some of these are discussed here.

According to **Aftab Alam, Shah Khalid, and Muhammad Salam, et al** [1] has discussed in this paper, a keyword is used to construct the 7x4 playfair matrix using letters and symbols, "#" and "*" two special symbols and upper case letters are the base for this Playfair Algorithm. The 7x4 playfiar matrix is constructed by filling keyword with no repeating (duplicate) letters. There is I and J are in different cells.

According to **Ravindra babu, Udaya Kumar, Vinaya babu, et al** [2] has discussed in this paper proposed a 6×6 size of matrix use of a larger key. There is total 36 character, where all the 10-decimal numbers (0-9) and 26-alphabets of English language in upper case. But it needs more characters support in order to be able to work over a large range of text file. They also proposed use of transposition ciphers to preserve frequency distribution of the single letters to destroy the diagram and higher order distribution.

According to **V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani, et al** [3] has discussed in this paper, it generalized and modified the Playfair cipher into a block cipher. The proposed work focuses on the use of the ASCII values in playfair. The use of 7-bit ASCII values increases character support to 128 characters. The work uses a key matrix of size 8×8 in which the key K consists of 64 distinct numbers, denoted by Ki, where i = 1-64 and each number lies between the ASCII limit of the 0-127. The remaining locations of matrix are filled by remaining numbers Ri, where i = 1-64. Initially, and every plaintext P is read 2n characters at a time, and using ASCII code, P is represented in form of a matrix given by- P = Pij , i = 1-n and j = 1-2. This extended playfair key matrix is used to encrypt / decrypt the plaintext matrix row wise, using the same rules of Playfair cipher and the cipher text P1 is obtained. In addition to this extended matrix, the concept of interweaving is introduced, which actually jumbles binary values of the ASCII codes of a set of characters. The matrix P1 ij is converted

into the binary form and every odd column are rotated upward following left rotation of each even numbered row. The steps of substitution and interweaving are iterated for the N number of times for each 2n characters. This algorithm uses a block of size 112-bits for n=8. So, a computation is to be carryout with an enormously huge 2112 (≈1033.6) alternatives, which actually ruled out possibilities of cipher text only attack. The key contain 64-distict numbers in a range of 1-127, allowing a 128P64 number of possible keys. Again the remaining 64numbers can also be arranged in a 128P64 possible ways. Now, the formidable task of finding substitution in all cases makes brute force attack almost impossible. Use of the numerous iterative substitution and interweaving steps also makes it resistance of known plaintext attacks. The time requirement of proposed algorithm is quite high for its complex iterative procedures. And thus can be proven less effective in the case of encryption / decryption of large files.

According to **Subhajit Bhattacharyya, Nisarga Chand & Subham Chakraborty, et al** [6] has propos the effective way to show the 90 characters. This extended play fair algorithm is based on use of a 10 by 9 matrix of letters constructed using a keyword. This 10 x 9 matrix contains almost all printable characters. This includes lowercase, uppercase alphabets, punctuation marks, numbers and special characters. The playfair matrix is constructed by filling in letters, numbers or special characters of keyword from the left side to right side and from top side to bottom side, and filling in the remainder of the matrix with remaining letters in the alphabetic order and the digits in ascending order form 0 to 9 and special characters .In this algorithm upper case alphabets are placed first then lower case alphabets following the digits 0 to 9 can be placed next cells of lower case alphabet a to z in an ascending order. And finally special characters which are arranged in an order .In this algorithm we have not counted alphabet I and alphabet J as one letter instead we are placing both alphabet I and alphabet J in two different cells in order to avoid the ambiguity to the user at time of decipherment. This algorithm can allow plain text containing of alpha numeric values; hence user can easily encrypt alpha numeric values efficiently. Plain text containing contact numbers, house numbers date of birth and other numerical values can be efficiently and easily encrypted using this algorithm.

Problem Statement

The problem statement of this algorithm is to ensuring three main goals of security, confidentiality, integrity and availability and secure the key of playfair matrix cipher technique (symmetric key cryptography) and provide the secure channel to send the key of Playfair cipher to the receiver end with the help of RSA algorithm (asymmetric key cryptography), attacks possible on information and tackle them with right types of counter measures and look at the various variations proposed by different authors and then to come up with a new modified cipher which will be stronger than the traditional Playfair cipher.

There are some limitations of the 5X5 playfair matrix.

1. The 5×5 PF Matrix considers the alphabet ‘I’ and alphabet ‘J’ as one character.
2. Only 26 letters of upper case in English can take as the key without duplicates.
3. The Space between two words in the plain text (PT) is not considered as one character.
4. The special characters can’t use as and numbers.
5. In 5X5 playfair matrix only uppercase alphabets are only used in 5x5 Matrix.
6. An extra alphabet ‘X’ is added when the PT word consists of the odd number of characters. In the DP this ‘X’ is ignored. ‘X’ is a valid character and it creates confusion because ‘X’ could be a part of PT, so we cannot simply remove X in DP.
7. The ‘X’ is used a filler letter while repeating letter falls in the same pair are separated.

To design an efficient algorithm by such type of method to overcome these limitation of the 5X5 playfair matrix and provide the secure method to send the key.

CONCLUSION AND FUTURE WORK

In this paper we discussed many extension in the playfair algorithm. We discussed the advantage of those particular algorithms. By studding's all these papers, we find out that there are need have the extension in the previous play fair algorithm is required to overcome the disadvantage of the algorithm. We also feel that in this time there is much requirement to secure the key of the playfair algorithm.

REFERENCES

[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, December, 2009 1793-8201

[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", ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28

[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", 2009 International Conference on Information Management and Engineering, 2009, Page 488-490.

[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, May 2010, Page 280-285.

[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, January 2011, Page 106-111.

[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 [2011]10-16

[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.