IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

ALO Based Robust Cryptographic Scheme

B. Hitesh Linganna[1], G. Dedeepya[2], Sk. Ayesha Sultana[3], T. V. V. Satyanarayana[4]

Student, 4/4 B.E., Department of ECE, Matrusri Engineering College, Hyderabad, India[1,2,3]

Associate Professor, Department of ECE, Matrusri Engineering College, Hyderabad, India[4]

Abstract: Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and it is important that communication be made secret. Cryptographic technique is one of the principal means to protect information security. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. As the technology for providing the data to be more secure has changing day by day by increasing the efficiency of the existing systems.In a very proportional way the number of triflers was also being increased day by day to hack the private data.Using public key encryption, it is possible for two users who do not know one another to send secret messages back and forth without having to agree upon and exchange a secret key over an untrusted network. A pair of keys is used to make this communication possible. One key, the public key, is used for encryption and is distributed freely to other users. The other key, the private key, is not shared with other users and can be used for decryption. The keys are different, and one key cannot be determined from the other. In this paper a novel algorithm based on Arithmetic Logic Operation (ALO) is proposed which gives a new logic to the existing systems. The complexity of the proposed algorithm is observed to be less compared to the traditional algorithms.

Keywords: cryptography, encryption, cipher text, ALO, security.

I. INTRODUCTION

Communicating in a secured environment is of major concern. In the recent past most of the researchers have been concentrating in this area. With the introduction of telegraph in mid 19th century, the art of communication started and has been rapidly growing. However, a high proportion of the disseminated over these communications is confidential in nature. Today's scenario in the world is posing a high threat due to the hackers who emulate the user to be the actual user. Hence, there is a need for techniques that are to be developed in this direction which prove to be hack proof. In many cases an unauthorised person who has access to the secured information will try to intercept and get benefited from this knowledge that he has gained by exploiting the communications. Cryptography is one such area which can provide security for communications.Cryptography is classified into two categories, Symmetric key based and Asymmetric key based, where in the former, if an attacker compromises the key of a group of users, then all the encrypted messages for that group will be exposed, and the later, can provide more functionalities than symmetric ones and are computationally expensive. In this paper we propose a novel technique based on asymmetric key based technique.

The basic concept that is followed in this technique is, both the sender and receiver are using their own individual key's for encryption and decryption. Initially the sender encrypts the data with his own key followed by receiver also encrypting with his own key (both key's are not similar) and re-transmitting it to sender. Now the sender decrypts the received cipher text with the private key which is known only to him/her this releases the key which he/she has used initially for encryption, and sends again to the receiver. Finally the receiver also decrypts the received data after which the receiver is left only with the required message that is interested by the transmitter in communicating to the receiver. This is discussed clearly in section V.

This paper is organised into seven sections. Section II details the previous work in this area. Section III details the problem faced in the presently used cryptography. Section IV defines the solution to the one of the problems described. Section V outlines the proposed algorithm. Section VI gives the results of the algorithm. Section VII concludes the cryptographic scheme.

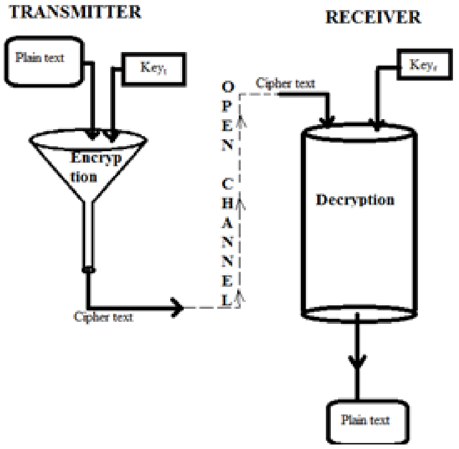

Fig. 1. Block Diagram of a system using Cryptography scheme.

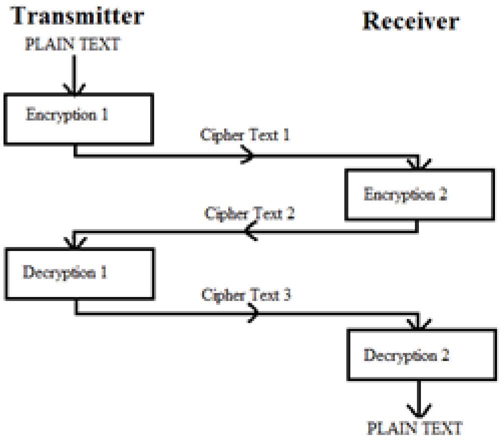

Fig. 2. Basic block diagram of the proposed technique

II. LITERATURE SURVEY

Cryptography aims to provide different scheme that provides the users to communicate over a secured channel that cannot be hacked. For this purpose various schemes or protocols are provided to execute authenticity and privacy of a person. [1]. In the recent past several researchers have developed various techniques in cryptography, Ching-Nung Yang et al. proposed a (k,n) VCS (Visual Cryptographic Scheme) which encodes a secret image into ‘n’ shadow images. These images are distributed among all the ‘n’ participants. The secret image is revealed by human visual system without the need for any computation by superimposing the ‘k’ participants on an overhead projection which in this case is an OR operation. As the OR operation degrades the visual quality of reconstructed image, a XOR- based VCS (XVCS), which uses XOR operation has developed for decoding to enhance the contrast[2].

In the current scenario information is transmitted in an open channel. The major problem with this channel is that the volume of the data that is transferred is not considered but how securely it is transferred is prime. Cryptography is one such technique which provides security for data transmission[3]. Symmetric key cryptography is a private key method that uses the same key for transmitting and receiving the data[4]. Identity Based Cryptography(IBC) is one property of a public key which relates the users with their identity. This technique suffers from having a key escrow problem which is overcome by using CL-PSK[5]. Visual cryptography encodes the secret image into binary shares of having a number 'n'. If these are photocopied, then the secret image can be visually decoded but there would be no visual meaning. Hence, an extended visual cryptographic technique is proposed for retrieving binary image whose image quality is poor but having better security[6]. Elliptical Curve Cryptography is another technique that is used to determine the complexity and area occupied by an algorithms when it is loaded into a FPGA[7]. Software updates, e-mail, online banking, and the entire realm of public-key cryptography and digital signatures rely on just two cryptography schemes to keep them secure—RSA and elliptic-curve cryptography (ECC)[8].The designed publick key cryptography must be secure enough to authenticate users. For performing this the complexity of the designed algorithm must be low enough to deployed on to a network where it exchanges the data[9]. Attacks on the designed algorithms gives the efficiency of the algorithm. Most of the cryptographic algorithms and the systems that are designed over these algorithms are not break free[10]. Combining biometrics with cryptographic techniques improve the efficiency of the algorithm. The problem of saving a file of large size on a server isa big problem where it can be corrupted by any hacker, hence, a new technique is proposed that this problem is overcome by the addition of fingerprint as one of the biometric [11].Deploying cryptography in wireless sensor networks that monitor people where integrity and privacy are most important. Various solutions have been proposed till date for acquiring privacy and integrity.

Hence, splitting schemes came into existence to provide integrity and security while computing SUM average[12]. Secure multiparty computation of a multivariate function is a central problem in cryptography It is well known that such a computation can be realized by a set of n parties if and only if the connectivity of the authenticated communication network is more than twice the number of corrupted parties[13-16]. A novel class of authentication systems "Infinite Alphabet Password Systems" (IAPs) are proposed which use a character set for the construction of the authentication token that is theoretically infinite, only bound by practical implementation restrictions. It is observed that the IAP architecture can be feasibly adapted for the use in many real world situations[17].

III. PROBLEM DEFINITION

Problem Statement: As it has become very important now-a-days in military and also for civilian applications to have a secured communication between two individuals or two organizations. Even though there are many algorithms proposed to perform this operation, they have high complexity and also the counter attacks are designed for tracking the data from the medium by brute forces.

IV. PROPOSED SOLUTION

Proposed method: So in order to make the communication more secured for civil and defence networks, the proposed algorithm plays a crucial role. The process of encryption and decryption are easy to perform and can be easily understood to users but the encrypted data is very hard to understand, and also it provides high security with the less complexity compared to other algorithms. The added advantage is with the use of private key the algorithm becomes unbreakable.

V. METHODOLOGY

The transmitter who is having information of alphanumerical data that is to be transmitted is represented in decimal digit’s. These decimal numbers are converted to binary data. Let this binary data be D. Now a key is prepared by the transmitter and represented in binary data as K1. This is the private key of the sender. Now BIT-XOR operation is performed on the binary data D and key K1.The result of this operation is converted to decimal numbers(T1) and is transmitted to receiver in open channel, after receiving the data by the target person(receiver). A private key K2 is prepared by the receiver and operated on the received data(T1) and the result(R) is retransmitted.

Now the sender after receiving data(R), an operation BIT-XOR is performed to remove the private key K1 so that only the information data as well as the private key K2(encrypted by the receiver) is left after removing the key K1 and the result after this operation which is in decimal data(T2) is again send to the receiver.

Finally, the receiver who alone know the key K2, will decrypt by performing its counter that is initially performed. The data after removing K2 is only the information that the sender wants to transmit.

The operation to be performed need not be only the XOR, but it can also be XNOR, simple ADDITION, SUBSTRACTION, MULTIPLICATION, DIVISION,... which has a counter operation that makes the data retrievable.

As we know that

$$D \oplus K1 \oplus K1 = D.$$

Which is a simple operation

But as the key K1& K2 are known only to the sender and receiver respectively. The possibility by the intruders to get the data is less.

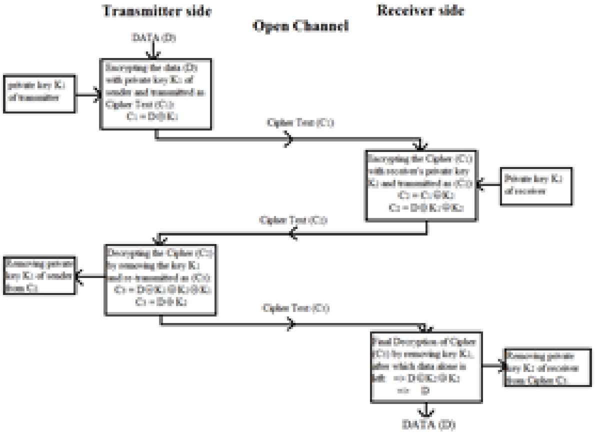
Transmitter side
Open Channel
Receiver side
DATA (D)
private key K1 of transmitter
Encrypting the data (D) with private key K1 of sender and transmitted as Cipher Text (C1)
C1 = D⊕K1
Cipher Text (C1)
Encrypting the Cipher (C1) with receiver's private key K2 and transmitted as (C2)
C2 = C1⊕K2
C2 = D⊕K1⊕K2
Private key K2 of receiver
Cipher Text (C2)
Decrypting the Cipher (C2) by removing the key K1 and re-transmitted as (C3)
C3 = D⊕K1⊕K1⊕K2
C3 = D⊕K2
Removing private key K1 of sender from C2
Cipher Text (C3)
Final Decryption of Cipher (C3) by removing key K2, after which data alone is left =&gt; D⊕K2⊕K2
=&gt; D
Removing private key K2 of receiver from Cipher C3
DATA (D)

Fig. 3. Detailed description of the algorithm

VI. RESULTS

The following results are taken for evaluation of this technique:

As we are transmitting the data “hai” which is having the ASCII values as:

h→ 104
a→ 97
i→ 105

But the sender transmits the data for the first time, in cipher text as:

312 2134 6195

The receiver after receiving this converts with his own logic and re-transmits to the sender as:

312 29876 204435

Now the sender again transmits this code as:

104 1358 3465

Finally the receiver decrypts the received data and is left with:

104 97 105

This is the required data which is transmitted by the sender.

Characteristics of proposed algorithm

The features/characteristics of algorithm are as follows

- It’s computational complexity is defined in terms of Big O functions and the complexity of this is given as O(N).
- The key used in this algorithm can be of variable length and minimum key length is ‘N’.

Where N is number of bits to be transmitted

The transmitter and the receiver are having their own logics (private keys).

TABLE I: Time taken by the proposed algorithm for execution

Length of the key (in bytes)	Time of execution (milliseconds)
1	0.24
2	1.367
3	1.424
4	1.62
5	2.21
6	3.14
7	3.57
8	3.74
9	4.05
10	4.71

Advantages

- It’s complexity is less compared to the presently used RSA algorithm.
- Less memory is occupied during it’s operation.
- The efficiency and speed are also high compared to RSA algorithm.

Disadvantages

- In this algorithm the data is transmitted twice by the sender, to the receiver.
- Minimum knowledge about the logics, should be maintained with both the user’s.

Comparative analysis with the existing systems

The computational complexity of proposed technique is very less compared to other algorithms which is Big O(N)

DOI 10.17148/IJARCCE.2016.55204

for XOR operations and varies with logics where as in popularly used RSA algorithm has :

- for public encryption it takes O(k^2) steps.
- for private key operation it takes O(k^3)steps.
- for key generation it takes O(k^4)steps.

Here K is number of bits in the modulus n.
And modulus n =p×q
Where, ‘p’ and ‘q’ are different prime factors.

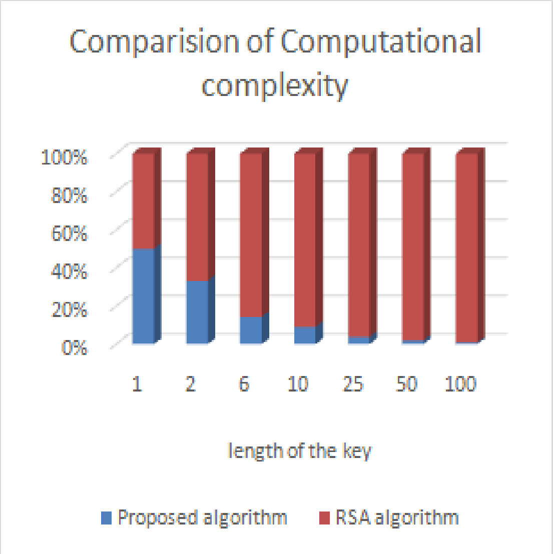

Fig. 4. Graphical representation of Complexity

- The key (carrier) size of this algorithm is of variable length which is given manually and minimum is ‘N’, whereas in RSA the key size is fixed to modulus(n).
- In this length of the key is not changed periodically as key is not fixed but in RSA algorithm key length is being doubled or tripled atleast for every 2 years.

VII. CONCLUSION

Cryptography isparticularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to thegoodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well- tested and well studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one.

The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

Hence the proposed approach provides the high security and protects from the crypto attacks.so, it is not possible to damage the data by the unauthorised personnel.

As a future scope, to make data more secure a private key can be used along with the public key cryptography.

REFERENCES

[1]. J. S. Coron, “What is cryptography”, IEEE Security &Privacy,Vol. 4, No. 1, Jan.-Feb. 2006, pp 70-73.

[2]. Ching-Nung Yang, Dao-Shun Wang, “Property Analysis of XOR-Based Visual Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology ,Vol. 24, No. 2, August 2013,pp. 189-197.

[3]. S. Chandra ; S. Paira ; S. S. Alam ; G. Sanyal, “A comparative survey of Symmetric and Asymmetric Key Cryptography”, International Conference onElectronics,Communication and Computational Engineering (ICECCE), 2014, pp.83-93.

[4]. O. O. Khalifa , M. D. R. Islam , S. Khan , M. S. Shebanig, “Communications cryptography”, RF and Microwave Conference, Oct. 2004, pp. 220 – 223.

[5]. A.Ahmad , A. Biri , H. Afifi , D. Zeghlache, “TIBC: Trade-off between Identity-Based and Certificateless Cryptography for future internet”, Sept. 2009, pp. 2866 – 2870.

[6]. ZhiZhou ,G. R. Arce ; G. Di Crescenzo, “Halftone visual cryptography”, IEEE Transactions on Image Processing”, Vol:15 No: 8 , Aug. 2006,pp. 2441 – 2453.

[7]. Junhyung Um, Sangwoo Lee, Youngsoo Park, SungikJun ;ThewhanKimU, “An efficient inverse multiplier/divider architecture for cryptography systems”, Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on, Vol:5, May 2003, pp. 149-152.

[8]. Monica Heger, “Cryptographers Take On Quantum Computers”, jan 1 2009.

[9]. Mike Burmester, YvoDesmedt “A secure and efficient conference key distribution system“,Volume 950 of the series Lecture Notes in Computer Science pp 275-286.

[10]. E. F. Brickell, A. M. Odlyzko “Cryptanalysis: a survey of recent results”, in Proceedings of the IEEE Vol:76 , no: 5 on May 1988,pp. 578 – 593.

[11]. M. Naor, G. N. Rothblum” The complexity of online memory checking”, in 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05) on Oct. 2005, pp. 573 – 582.

[12]. [12]K. B. Frikken and Y. Zhang, "Confidentiality and integrity for SUM aggregation in sensor networks," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, Greece, 2010, pp. 1-10.

[13]. C. Guyeuxand . M. ahi, "A new chaos-based watermarking algorithm," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, 2010, pp. 1-4.

[14]. S. Vaya, "Realizing secure multiparty computation on incomplete networks," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, Greece, 2010, pp. 1-8.

[15]. N. Papanikolaou, S. Creese, M. Goldsmith, M. C. Mont and S. Pearson, "EnCoRe: Towards a holistic approach to privacy," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, 2010, pp. 1-6.

[16]. N. Zannone, M. Petković and S. Etalle, "Towards data protection compliance," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, 2010, pp. 1-4.

[17]. M. Gibson, M. Conrad and C. Maple, "Infinite alphabet passwords: A unified model for a class of authentication systems," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, Athens, 2010, pp. 1-6.

DOI 10.17148/IJARCCE.2016.55204