Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Encryption Using Affine and one Time Pad(AAOTP)

Kavit Maral Mehta, Saksham Sharma
IT, VIT University
Tamil nadu, India

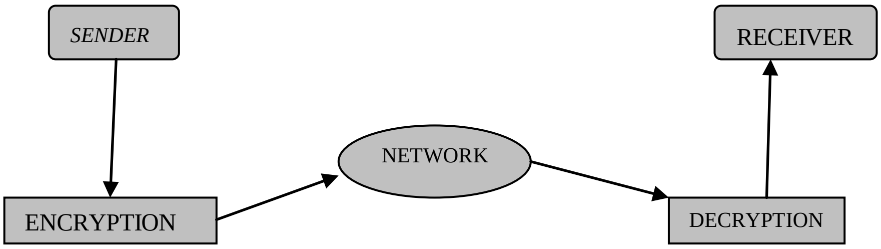
Abstract— ***The Explosive growth in computer systems and their interconnection via networks has increased the dependence of both organizations and individuals on the information stored and communicated. This in turn, has lead to a heightened awareness of the need to protect data and resources from disclosures, to guarantee the authenticity of data and messages and to protect the systems from network based attacks. Secondly, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security. So, looking at this scenario we have tried to contribute some of our knowledge and we have been successful in creating a simple hybrid cryptographic technique which involves the combination of Affine ciphers and OTP (One Time Pad). We have use java platform to program this cryptographic technique and we will be showing the snapshots taken from our computers to prove how this technique can be useful.***

Keywords— ***Cryptography, Affine ciphers, OTP, Java, CMD.***

I. Introduction

The word cryptography means "*secret writing*". However, the term today refers to the science and of transforming messages to make them secure and immune to attacks. *The original message before being transformed is called* plaintext. *After the message is transformed, it is called* cipher text. *An encryption algorithm transforms the plaintext to cipher; a decryption algorithm transforms the cipher text back to plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.*

.



These encryption and decryption algorithms are called as ciphers (categories of algorithm). One cipher can serve millions of communicating pairs.

A *Key* is value that the cipher, as an algorithm, operates on. To encrypt a message we need an encryption algorithm, an encryption key, and the plain text. These create the cipher text. To decrypt a message, we need a decryption algorithm, a decryption algorithm and the cipher text. So these reveal the original plaintext. In Cryptography, the encryption/decryption algorithms are public; anyone can access them. The keys are secret. So they need to be protected.

Cryptography algorithms can be divided into two groups.

- Symmetric-key cryptography (or secret key) algorithm
- Public-key cryptography (or asymmetric key) algorithm

Now in our project we have used the above two categories as our base as we have developed a cipher that is the combination of one cipher from each of the given above categories.

II. Symmetric Key Encryption

The symmetric-key cryptography algorithms are so named because the same key can be used in both directions. Here, the same key is used by both sender/receiver. The sender uses this key and an encryption algorithm to encrypt data. The receiver uses the same key and a decryption algorithm to decrypt data. In Symmetric-key cryptography, the algorithm used for decryption is the inverse of the algorithm used for encryption.

Advantages:

(i) Symmetric key algorithms are efficient.

(ii) It takes less time to encrypt a message using symmetric key algorithm than to encrypt a message using a public key algorithm.

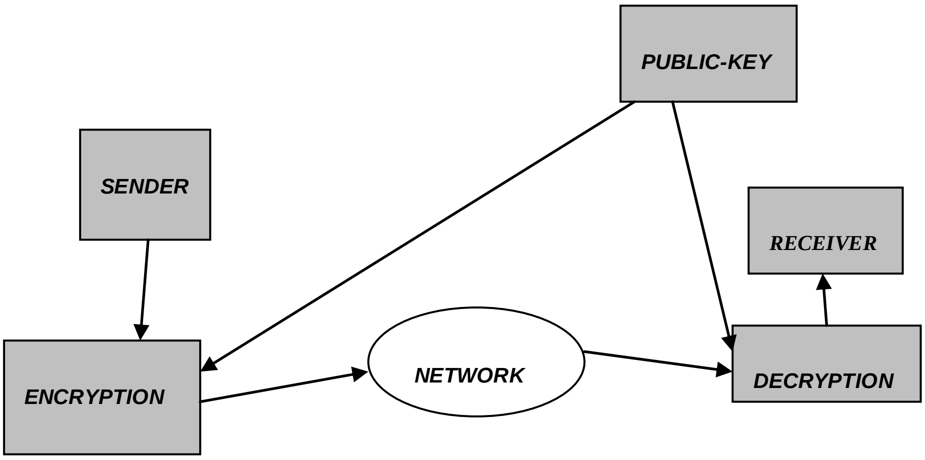
(iii) The key is usually small.
(iv) It is used to encrypt and decrypt long messages.

Disadvantages:

(i) Each pair of users must have a unique symmetric key.For n people, n*(n-1)/2 symmetric keys are used. Ex: For 1 million people to communicate, 500 billion symmetric keys are needed.
(ii) The distribution of keys between two can be difficult.

III. ASYMMETRIC KEY ENCRYPTION

In public key cryptography, there are two keys a private key and a public key. The public key is announced to the public and the private key is kept by the receiver. Here the public that is used for encryption is different from the private key that is used for decryption. The public key is available to the public and the private key is available only to an individual.



In public key encryption/decryption, each entity creates a pair of keys, private and public keys. Each entity is independent, and the pair of keys created can be used to communicate with any other entity where as a shared symmetric key is shared by the two parties and cannot be used when one of them wants to communicate with a third party.

Advantages:

(i) As discussed above, it removes the restriction of a shared symmetric key between two entities who need to communicate with each other.
(ii) The number of keys needed is reduced tremendously. For 1 million users to communicates, only 2 million keys are needed, not 500 billion, as was the case in symmetric key cryptography.

Disadvantages:

(i) Complexity of the algorithm
(ii) The association between an entity and its public key must be verified.

IV. TRADITIONAL CIPHERS

Ciphers that involved either substitution or transposition are referred to as traditional ciphers.

Substitution Cipher:- A cipher using the substitution method substitutes one symbol with another. If the symbols in the plain text are alphanumeric characters, we replace one character with another.

Ex: we replace characters A with D, B with E and so on. If symbols are digits (0 to 9), we can replace 1 with 5, 2 with 6 and so on.

VI.**Proposed Technique**

Our technique makes use of combination of symmetric key algorithm(Affine cipher) and an asymmetric key algorithm (OTP). This technique is giving extra layered proctection and is very easy to implement. The Encryption and Decryption algorithms are as followed.

A. Encryption Algorithm

1. Take the plain text as the user input.
2. Now store the input into an character array.
3. Now pick out one by one each letter from the array and then take out it's equivalent place value between 0 to 25 as a=0,b=1 and so on till z=25 and store it in a array[].
4. Now select two co-prime numbers and store them into variables p and q.
5. Now perform following operation on each of the extracted letter :- ((p*array[i])+q) mod 26
6. After performing Affine encryption on this store the encrypted letters in another character array.
7. Now produce an array of random numbers of same length as the length of the text.
8. Now perform addition of letter in the encrypted array with the corresponding element in the random array.
9. Now our message has been doubly encrypted and is more secure than a single encryption techniques.

Character	p	q	OTP-key	cipher
H	5	8	23	O
E	5	8	12	O
L	5	8	17	C
L	5	8	16	B
O	5	8	6	J

B. *Decryption Algorithm*

1. Now for decryption follow the reverse procedure.
2. First subtract the final encrypted character array with the random number array.
3. The result is stored inside another array arr[].
4. Now find p^{-1} and perform following operation on the above array :- p^{-1}*(arr[i]-q) mod 26
5. Now we get the original message.

Cipher	OTP-key	p	q	Original Text
O	6	5	8	H
O	16	5	8	E
C	17	5	8	L
B	12	5	8	L
J	23	5	8	O

VII.**ANALYSIS**

A.Simulation Results

The above algorithm AAOTP encryption technique is implemented using a C program running on a 2.27 GHz I5 processor and 4 GB RAM. Total execution time is compared with the RSA algorithm for different lengths of messages.

The table below shows the simulation result for both the algorithms.

AAOTP		**RSA**	
Message Length	**Execution Time**	**Message Length**	**Execution Time**
5	0.018	5	0.092
10	0.025	10	0.121
15	0.028	15	0.129
20	0.055	20	0.142

B.Changing the message length

Changing the message length affects other parameters of the algorithm. With increase in size of the message the time taken to retrieve the acii value increases. In other words the time taken is directly proportional to the message length. So the time complexity is increased. The length of the key increases at the same as the increase in message size. With the larger key the security is increased. Hence increasing the message size increases security but decreases the speed of encryption and decryption.

C. Security Analysis

AAOTP is a hybrid key encryption scheme. The same key is used for encryption and decryption. This makes it less secure than the public key encryption schemes like RSA. If the key is obtained, then the encryption scheme can be cracked. The use of random numbers make it difficult to crack. This provides better security than simple private key encryption schemes. However the encryption/decryption speed of a private key encryption schemes is higher than the public key encryption schemes. Therefore AAOTP provides faster encryption or decryption than RSA.

VII. **Conclusion**

AAOTP algorithm successfully encrypts and decrypts all 256 ASCII values. The time complexity of this algorithm for a 11 letter message is 0.027 seconds. Even when the key is leaked or hacked this scheme remains secure. This security is provided by the random numbers. The hackers can figure out the encryption method, but different random numbers used for different letters makes it difficult for hackers to crack. Need for random numbers is growing. Most encryption algorithms require a source of random data, even some symmetric ciphers (where the secret is shared), either to generate new private/public key pairs, ie for session keys, padding, or for other reasons. With the growth in e-commerce, more and more random numbers and data are used to establish session keys for enhancing security. However the real area where hardware Random Number Generators will be needed is for IPSec (IP Security), especially for high security environments where connections are rekeyed often and there are many connections (like 300 remote users telecommuting to work). The possibility of an attacker intercepting the data stream and decrypting it - as opposed to just breaking in to your server, are slim, the possibility exists (and will grow in future).

Acknowledgement

We would like to thank our parents for giving us such a support in our research. And we hope that through your publication we may be able to bring our work in front of the whole world. As a student and lack of resources we have implemented this technique only at the basic level.

References

[1] James E.Gentle, “Random Number Generation and Monte Carlo Methods: Statistics and Computing”, Springer, 2003.

[2] William Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall,1999 .

[3] I.Deak , “Random Number Generators and Simulation: Mathematical methods of operations research” , Akademiai Kiado, 1990 .

[4] William Stallings, “Network Security Essentials: Applications And Standards”, Pearson Education, 2008 .

[5] N.Koblitz, “A Course in Number Theory and Cryptography”, Springer-Verlag, New York, Inc., 1994 .

[6] Kwok T.Fung, “Network Security Technologies”, CRC Press LLC, 2005.

[7] A.J.Bagnall, “Communication Theory of Security System”, Bell , System Technical Journal, 28, 1949.

[8] Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, John Wiley & Sons, 2007.

[9] Nalini Niranjan, “A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithm and Cryptography”, NIITCCS, 2004 .

[10] Mutsuo Saito and Makoto Matsumoto ,“A PRNG Specialized in Double Precision Floating Point Number Using an Affine Transition”, Springer, 2008 .

[11] EOTP – Static Key Transfer. Defuse.ca (2012-07-13). Retrieved on 2012-12-21.

[12] Barkan, Elad; Eli Biham; Nathan Keller (2003). "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication". Cryptome 2003: 600–16.

[13] Pelzl & Paar (2010). Understanding Cryptography. Berlin: Springer-Verlag. p. 30.

[14] Mullen, Gary & Mummert, Carl (2007). Finite fields and applications. American Mathematical Society. p. 112. ISBN 9780821844182.

[15] Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.