ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on an Enhanced Cryptographic Technique for Messages Encryption and Decryption

Darshana Patil[1], Prof. P. M. Chawan[2]

M. Tech Student, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India [1]

Associate Professor, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India [2]

ABSTRACT: Currently, security has become one of the important factors in our day to day life. Like banks, shops and everywhere else we require security. An attacker can use the password to access the private information. To avoid this is one of the goals of the data security. As we know that we require security in our daily life then what about the security of our security system such as our national security i.e. defense. Mainly, at the time of war the terrorists, spies or an attacker tries to leak information and capture the important information which may useful to win the war. To overcome the problem the proposed technique can be used. The plain-text is treated at the bit level for encryption/decryption which provides more security than compound and intermix characters. Moreover, the advantage of the technique is that both the algorithm uses the same key generation algorithm. Here the key is generated from the plain-text bit stream and same key is used for both encryption and decryption.

KEYWORDS: Encryption key, decryption, symmetric key cryptography, asymmetric key cryptography.

I. INTRODUCTION

Number of algorithm is used in order to perform the encryption and decryption, but as compare to others only few algorithms had a best result among themselves. The algorithm gives the best result use a key. A key is used to configure a cryptosystem and used as a parameter for encryption and decryption. There are many algorithms and cryptographic techniques which uses key to encrypt and decrypt the data. They are mainly divided into two classes: asymmetric key and symmetric key cryptography. In the symmetric key cryptography, a similar secret key is used for both encryption and decryption and shared between sender and receiver. While, in the asymmetric key cryptography there are two keys instead of one, they are public and private keys. To encrypt data user use public key of sender and for decryption private key of its own.

Even though the symmetric key cryptography is very efficient, but it has its own drawbacks and weakness. As, we used the same key for encryption and decryption we should keep that key more secure. If an antagonist or an attacker knows the key, then the message can be decrypted very easily. Simultaneously, the key must be available to the sender as well as to the receiver. Here transmitting the message securely is not the problem, whereas transmitting keys securely is the problem, which is not the purpose of our security system. To overcome the problem, as we know keys are much smaller than the messages and can be generated in advanced. Although, here sender and receiver are using same key or symmetric key but here key transmission is no more a challenge. Hence key management problem is solved within the message.

II. LITRATURE REVIEW

Cryptography is the art and science which provides method of storing and transmitting data in a particular form to introduce secrecy in information security. It is an important element of any technique which provides message transmission security. Here message is conceal in such form so that authenticated recipients can only decrypt and read the message. Authenticated and intended user can access the data as they possess the secrete key, no-one can read them

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

without having access to the 'key'. Cryptographic systems are generically classified along three independent dimensions.

1. Methodology to transform plain-text to cipher text.

Generally two principles are used for encryption algorithms: First, substitution cipher is a method of encoding by which each units of plain-text are replaced with cipher-text. The "units" may contain single letter or combination of two or many letters. Transposition cipher is a method in which elements in the plain-text are rearranged.

2. Methodology in order to use the number of keys.

Secret key, public key, digital signature and hash function those are some methods which is used with cryptography.

- Secret Key: In secret key cryptography, a symmetric and single key is used for both encryption and decryption.
- Public Key: Public key cryptography is a two-key crypto system where two parties could have a secure communication over an insecure communications channel but no need to share a secret key.
- Digital Signature: In order to ensure the authenticity of the sender there is a need of digital signature. The digital signature is nothing but the stamp or signature of the sender which is embedded together with the data. Here, the signature ensures the senders identity and any changes made in the data that has been signed. Hence, it is very easier for receiver to identify correct data.
- Hash Function: A small size of bits is generated by using a well-defined mathematical formula or procedure from a large sized file is called a hash function which is one of the ways of encryption. The result is called s hashes or hash code.
  There are three main properties of ideal hash function:
  - For any given data it is extremely easy to calculate a hash.
  - It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
  - It is extremely difficult and impossible that two different messages will have a same hash function.

3. Methodology in order to process plain text.

Here an output block is produced for each input block which is processed by a block cipher one at a time.

Different Cryptographic Algorithms

1. AES

One of the example symmetric key block cipher is Advanced Encryption Standard. AES has substitution, shift and bit mixing as encryption primitives whereas confusion and diffusion are the cryptographic primitives. It is implemented in software as well as in hardware all across the world in order to encrypt sensitive data.

Advantages:

- AES gives more security than other algorithms..
- Larger key sizes supported by AES than 3DES's such as 128, 192, 25 bit length.
- AES is faster and has same performance in both hardware and software.

2. DES

The DES stands for Data Encryption Standard which is a symmetric key block cipher, takes an input as plaintext of 64-bit and key of size 56-bit and produces an output, cipher text of 64-bit. It is developed in 1976 much before

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

AES.DES has substitution and permutation as encryption primitives whereas confusion and diffusion are the cryptographic primitives. In encryption primitives P and S boxes are used for substitution and permutation respectively.

Advantages:

- As 56 bit of key is used for the encryption hence 256 keys are possible. It is impractical for brute force attack on such large number of keys.

Disadvantage:

- Same output can be created by S-box for two chosen input.
- Initial and final permutation is performed in DES but the purpose of both is not clear.

3. Cryptographic Hash Functions

Two particular hash functions are the most popular today.

I. MD5

- Ron Rivest is the one who developed Several hash algorithm. Those are nothing but MD2, MD4 and MD5, in this MD stands for Message Digest. And the latest version is MD5.
- MD5 is one of the fastest method and which produces 128-bit message digests.
- As the initial processing is done, the input is first divided into 512-bit blocks and each block is processed further.
- Four 32-bit blocks are produced as an output of the algorithm, from that the 128-bit message digest is produced.

II. SHA

- The secure hash algorithm is devolved by NIST along with NSA.
- SHA has a design which closely matches with MD5 moreover it is a modified version of MD5.
- SHA requires an input message which is in size less than 2^{64} bits in length.
- The output of the SHA is a message digest of 160 bits in length.
- In SHA word secure was decided based on two features of SHA.
  - Obtain the original message, given its message digest
  - Find two messages producing the same message digest

4. RSA

RSA is the most popular and proven asymmetric key cryptography algorithm. It is one of the public-key cryptosystems and most popularly used. In this algorithm, the encryption key is public whereas decryption key is kept secret. In RSA, two large numbers are multiplied then the factoring of that product is done. The asymmetry is based on the practical difficulty of factoring the product.
RSA is implemented by using two important ideas:

1. Public-key encryption.
   In this technique encryption keys are public and decryption keys are private, hence only the person who knows the decryption key can decrypt the encrypted message.

2. Digital signatures.
   Here the receiver may need to verify that a received message is actually originated from the sender by using signature. Message is decrypted by using decryption key, and the signature is verified by using the public encryption key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

5. IDEA

IDEA stands for International Data Encryption Algorithm which is one of the strongest cryptographic algorithms. Although it is quite strong, IDEA is less popular than DES for two main reasons:

- It is patented whereas DES is not and for that reason before it can be used in any commercial applications is licensed.
- DES has a long history as compared to IDEA.

III. THE PROPOSED ENCRYPTION/DECRYPTION TECHNIQUE

The first step of the decryption algorithm consists in reading the encrypted text blocks. In the second step, the text block is converted to the binary format by generating the binary code for every character. Thus, the key is extracted in the third step by selecting the same specific bits already selected. During the extraction of the key, some bits may be missing and a key cannot be completed because text blocks are too short or small. In this case, a missing bit can be replaced either by 0 or with 1. XOR operation is used with two inputs. The first input is the key extracted and the second input is taken from the binary format to restore the original binary format. In order to send an email or private instant messaging The proposed technique is used.

It can be applied to text blocks travelling between two computers through a network. It is based on the generation of a key in a symmetric Key Cryptography (SKC). The similar shared key is used for encryption and for decryption, which is incorporated in the encryption as well as in the decryption algorithm. Neither the sender nor the receiver knows in advance the key used. The key is generated from the text block to be encrypted or decrypted and depends on the nature and size of the text block. The final stage of this algorithm will convert the binary format of the decrypted text block to characters.

The major advantage of this technique is that the used key is generated at the encryption and extracted at the decryption time using an algorithm. This technique is simple, easy to implement and will be applicable to any language. On other words, every message, email or text block will have its own and unique key. This will guarantee a very-high secure connection between two recipients in case messages are intercepted. Another advantage of this technique is that neither the sender nor the receiver needs to memories the key. The similar shared used key is generated at the encryption time and it extracted at the decryption n time.

1] Encryption Technique

Following are the 4 steps in order to perform encryption
1) Reading the text block
Plaintext: An Enhanced Cryptographic Technique for Messages Traveling between Computers

2) Converting the text block to binary format
00010100111110010010110110010001110010001101100 10
00101011101101100011110111100110001100000101110100
00110100001101001011000110010000001010100011001010 11
00011011010000110111001101001011100010111010101100 10

3) Generate the key:
000110100011000010111001

4) Logical operation such as XOR is used to perform encryption

The main stages of the proposed encryption technique are illustrated in Figure 1. The first step of the algorithm consists in reading a plaintext to be encrypted. In the second step, the whole text block is converted into a binary format that represents the binary code for every character. It is very easy and convenient to get streams of bits by converting these types of data, then encrypt the stream, and finally send the encrypted stream. Here, the text is treated

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

at the bit level it means each character is replaced by 8 or 16 bits n hence the number of bits. Intermixing and compounding of bits provides more security than that of the characters. Finally, the key is generated in the third stage by selecting specific bits at specific positions (prime number).

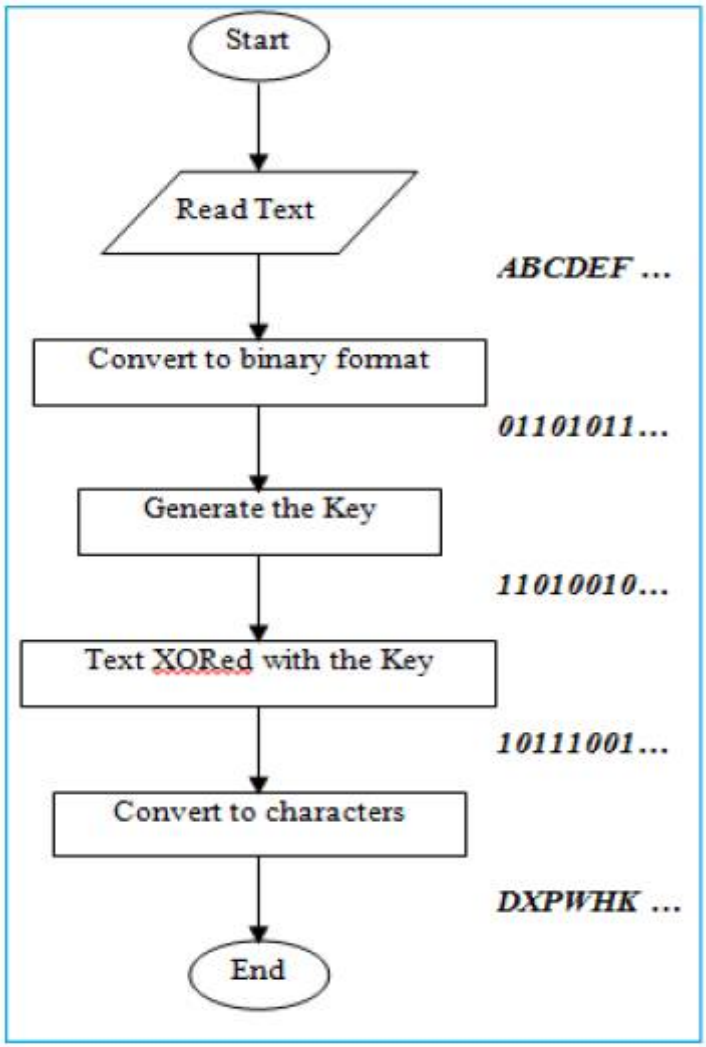

Figure 1.Flowchart representing the main stages of the encryption algorithm.

2] Decryption Technique

Following are the 4 steps in order to perform decryption
1) Read cipher text in binary format:
00010100111110010010110110010001110010001101100 10
00101011101101100011110111100110001100000101110100
00110100001101001011000110010000001010100011001010 11
00011011010000110111001101001011100010111010101100 10

2) Selecting the same specific bit to extract the key:
000110100011000010111001

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

3) Logical operation such as XOR is used to perform decryption

4) Converting the stream of bits into characters
01000001011011100010000001000101011011101100100001
10000101101110011000110110010101100100001000000100
00110111001001111001011100000111010001101111011001111
01110010011000010111000001101000011010010110001100010

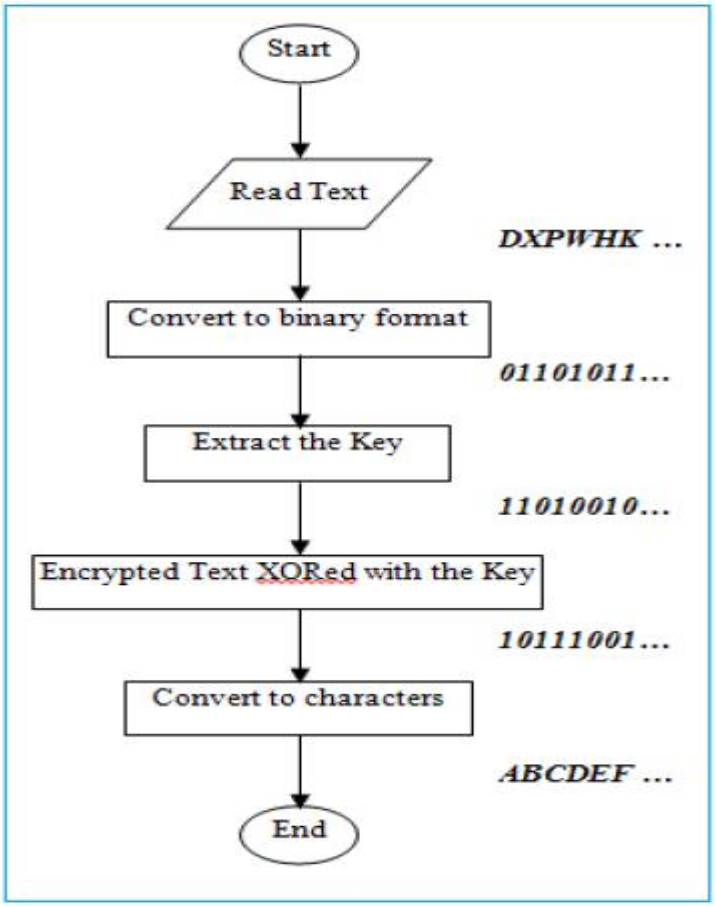

Figure 2. Flowchart representing the main stages of the decryption algorithm

Encryption/decryption key with 24 bits is taken from the above selected two first line plaintext stream bits. 000110100011000010111001

At the decryption time, the algorithm will reverse the process to decrypt the text block already encrypted. The main stages of the proposed decryption technique are illustrated in Figure 2. The first step of the decryption algorithm consists in reading the encrypted binary block. In the next step, by selecting the same specific bits that are already selected the key is extracted. The encryption key is removed in the third stage from the binary block. Finally, in the fourth step, the original binary format is restored after applying a logical operation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

IV. CONCLUSION

In this paper, an enhanced algorithm is proposed to encrypt/decrypt text blocks using a generated key without password. The proposed technique has been implemented with Java language and tested with English characters. This technique is simple, easy to implement, and can be applicable to many languages. Additionally, the similar key is used for encryption and decryption algorithm in order to prevent user or machine from holding, memorizing or recalling passwords.

REFERENCES

1. Dipti, K. S. and Neha, B.,"Proposed System for Data Hiding Using Cryptography and Steganography", International Journal of Computer Applications, 8(9), pp. 7-10, 2010.
2. Omar Kassem Khalil,AissaBoudjella, "An Enhanced Cryptographic Technique for Messages Traveling between Computers",Sixth International Conference on Developments in E-Systems Engineering, 2013.
3. Alan Siper, Roger Farley and Craig Lombardo, "The Rise of Steganography", Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005.
4. Niels, P. and Peter,"Hide and Seek: An Introduction to Steganography", IEEE Computer Society, IEEE Security and Privacy, pp. 32-44, H 2003.
5. Raphael, A. J., and Sundaram, V,"Cryptography and Steganography - A Survey", International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630,2011.
6. Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, "An Encrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh.
7. Sridevi, R., Damodaram, A., and Narasimham, S.,"Efficient Method of Image Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security",Journal of Theoretical and Applied Information Technology, pp. 768-771, 2009. Retrieved 21st August, 2012 from http://www.jatit.org.
8. http://en.wikipedia.org/wiki/Autokey_cipher
9. Helen Fouché Gaines, "Cryptanalysis", Dover, ISBN 0-486-20097-3, 1939.
10. Ibrahim A. Al-Kadi, "The origins of cryptology: The Arab contributions", Cryptologia, 16(2), pp. 97–126, April 1992.
11. David A. King, "The ciphers of the monks - A forgotten number notation of the Middle Ages", Stuttgart: Franz Steiner, (ISBN 3-515-07640-9)2001.