An Effective Approach towards Encryption of Limited Data

Ruchi Kawatra*
Sapna Arora Saini**

Abstract

Processed information from a network is very difficult to maintain. As the data travels from one point to another, there are different threats / obstacles through which a programmed data has to go through. In the modern world, it is necessary to secure data and maintain its features like confidentiality, integrity, privacy and security. For the same, cryptographic techniques are used. These techniques are the base on which these features sustain. Cryptography is art of writing secret code from a plain code so that the privacy of data gets sustained. Generally, we deal with the type of data algorithms which works with extensible data.

Our approach is towards encryption of limited amount of data.

Keywords: Encryption, Decryption, SDEA (Short Data Encryption Algorithm), Cryptography

I. Introduction

The word cryptography comes from a Greek words means hidden or secret writing. Cryptography is the art of secret writing. Generally, people think of cryptography as the art of managing information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Cryptography provides services such as

- Integrity checking – reassuring the recipient of a message that the message has not been altered since it was generated by legitimate source.
- Authentication - verifying someone's or something's identity.

In simple words we can explain that a message in its original form is known as **plain text** or **clear text**. The mangled information is known as **cipher text**. The process for producing cipher text from plain text is known as **encryption**. The reverse of encryption is called **decryption** [1].

Ruchi Kawatra*
Department of IT
Institute of Information Technology and Management, GGSIPU, Delhi, India

Sapna Arora Saini**
Department of IT
Institute of Information Technology and Management, GGSIPU, Delhi, India

Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you like to start the communication secretly.

Sometimes a cryptographic algorithm has a variable-length key. It can be made more secure by increasing the length of the key.

Sometimes, Steganography and cryptography are used interchangeably assuming that both are used for protecting confidential information. However there is a big difference between the two. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver knows the existence of message, if it exists[2]. Steganography prevents discovery of the very existence of the communication. In cryptography, encryption prevents any unauthorized user from detecting the contents of communication. In Cryptography the structure of the secret message is changed, no such thing in steganography.

II. Type of Cryptography

There are three types of cryptographic techniques:

1. Symmetric Key Cryptography: It is also known as **secret key** cryptography. In this only a single

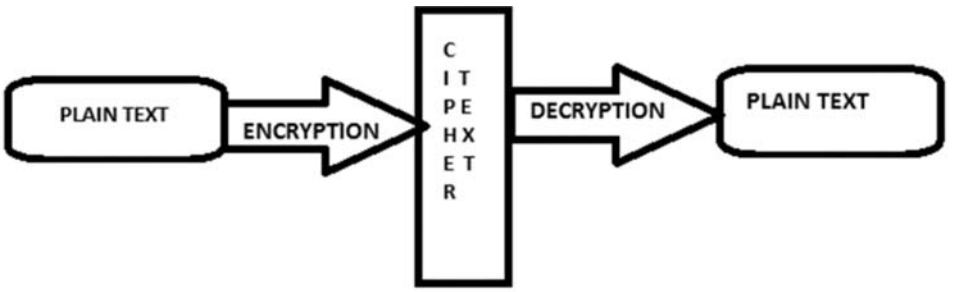


Fig. 1: Encryption-Decryption process

key is used. Here same key is shared by both the parties communicating. It is simple and faster. Given a message and the key, encryption produces unintelligible data, also known as cipher text, which is about the same length as the plain text. Decryption is the reverse process of encryption and involves the use of same key as that of encryption. The Captain Midnight code and the mono-alphabetic cipher are both examples of secret key cryptography.

2. Asymmetric Key Cryptography: It is also known as **public key** cryptography. Unlike secret key cryptography, the keys are not shared. In this two different keys are used. A private key that is not shared with anyone and a public key that is preferably known to the entire world. The users get the keys from an authorized Certificate Authority.[5][6]

3. Hash Function: They are also known as message digests or one-way transformations. It is a one way encryption. A cryptographic hash function [4] is a mathematical transformation that takes a message of arbitrary length and computes from it a fixed length number. No key is used for encryption or decryption process.

III. Existing Techniques

A number of image based encryption algorithms is available like Baker's Transformation, in this Baker's map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc. But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

As mentioned in Introduction section, there are two main types of cryptography in use today - symmetric or secret key cryptography and asymmetric or public key cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's.

1.**Data Encryption Standard (DES):**The main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES).[2][3] However, this has now been replaced by a

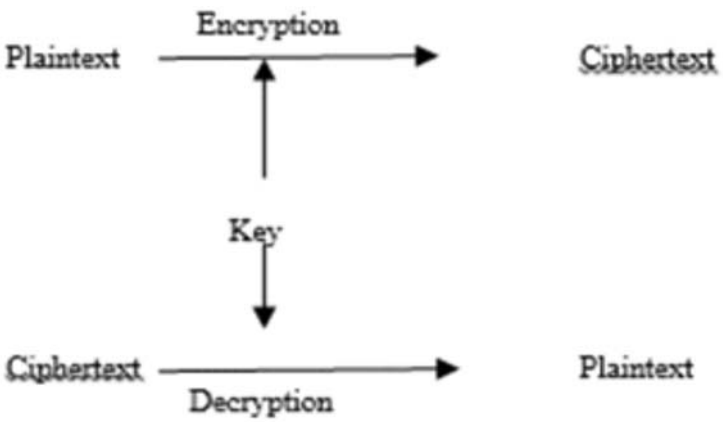


Fig. 2: Symmetric-key cryptography

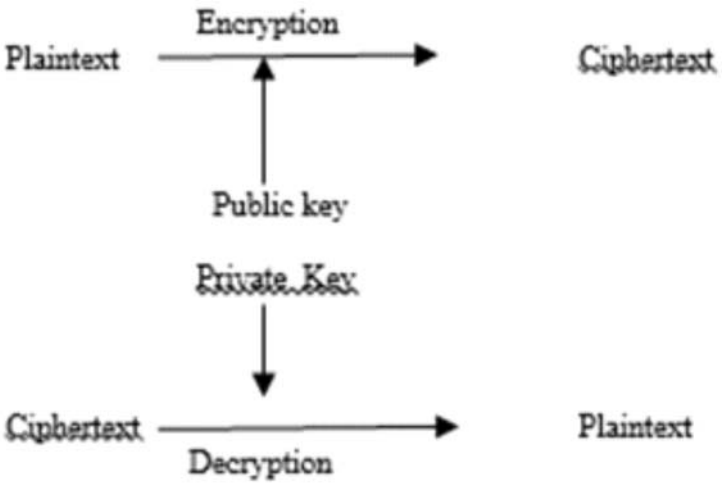


Fig. 3: Public-key cryptography

new standard known as the Advanced Encryption Standard (AES) which we will look at later. DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time.

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. However, DES is widely used algorithm in different domains like Education, military & others, but some of the design considerations are under controversy.

2**. Triple Des (TDES):** As a replacement to DES, TDES was a better solution to make possible changes. However its encryption algorithm status is too strong (i.e difficulty in breaking the cipher text) sue to advances in key searching.[10]The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming.

3. Advanced Encryption Standard (AES): AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds. But for the case of limited data, it would be quite difficult to work with.

4. **BLOWFISH:** Blowfish [9] was one of the fastest & better options for existing encryption algorithm (in case of data on 32 bit microprocessors). It is efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES.

IV. Implementation

A **transposition cipher [10][11]**is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

The Proposed algorithm is used to encrypt data by using ASCII values of plain text or the data to be encrypted. The secret key is used to make modification in another string and that new modified string is used

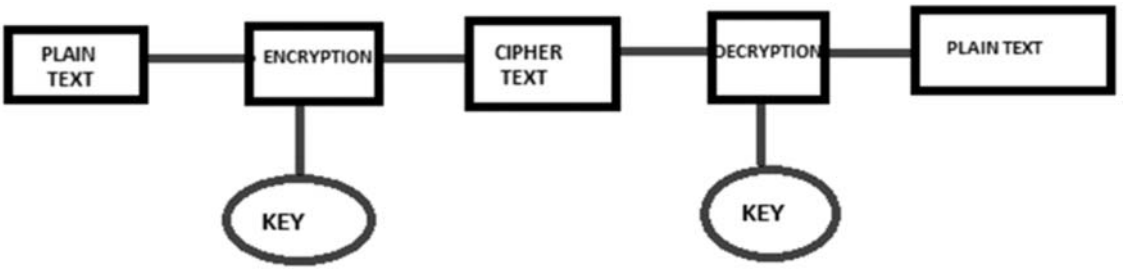


Fig. 4: Symmetric Key Cryptography

to encrypt or decrypt data. Therefore, it is assumed that it is a type of symmetric key algorithm because it uses same key for encryption and decryption purposes.

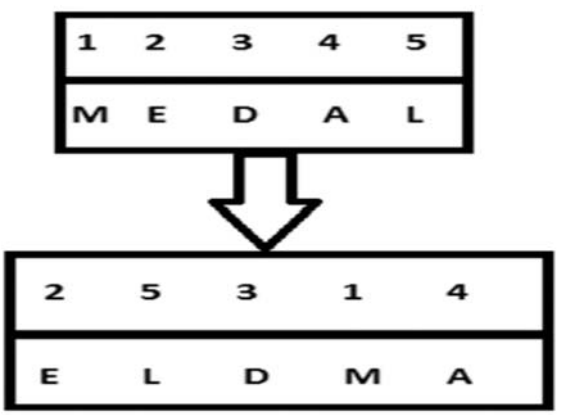
The proposed **algorithm** is –

1. The plain text is selected.
2. Fetch a string in order to encrypt it in a secure manner (say medal).
3. Convert it into ASCII code.
4. DECIMAL/ASCII:77 69 68 65 76
5. 8 BIT BINARY VALUE OF STRING-"MEDAL":01001101 01000101 01000100 01000001 01001100
6. ADD BINARY VALUE OF 1 IN EACH BYTE : 01001110 01000110 01000101 01000010 01001101
7. Perform Shift left operation 2 times: 00111001 100011001 00010101 00001001 00110101
8. Choose 1 symbol from queue: (say 5)
9. ASCII VALUE OF SYMBOL GENERATED: (5) 00110101
10. 8 BIT BINARY VALUE SYMBOL GENERATED & STORED AS KEY: 01101110 0101001110 01001010 0111110 01101010
11. CIPHER TEXT ACHIEVED THROUGH BINARY ADDITION: n s J > j

Decryption is the reverse process and performed in the following manner:

1. The cipher text is selected.
2. Fetch the ASCII value of the data.
3. Convert it into ASCII code.
4. Perform Shift right operation 2 times.
5. Subtract binary value 1 from each byte.
6. Convert the upcoming value into decimal number
7. Now, find out the string associated with decimal number i.e, MEDAL.

Encryption process example for our approach:



1 2 3 4 5	2 5 3 1 4
MED AL	E L D M A

V. Conclusion

Encoding & decoding is not at all much difficult task if suitable & precise algorithms are used but problem arises when we have to work out encryption of less amount of data with current & traditional algorithms which generally doesn't seems to be much cost effective. TO keep the same goal in mind with the integration of CIA (Confidentiality, Integrity & Authenticity), we designed an effective approach.

As a future work, we can merge the concept with

- Different data formats (Audio, Video & MM)
- Analysis of New information in an updated media file
- Working the same algorithm to partial secret key algorithm to make it more secure & confidential.
- Educational concepts.

References

1. SANS Security Essentials, (volume 1.4, chapter 4) Encryption and Exploits, 2001.
2. Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking", 2000.
3. Monisha Sharma, Chandrashekhar Kamargaonkar, Amit Gupta, "A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7, September- 2012.
4. The International Civil aviation Organizationn, http://www.icao.int ,The MRTD site pp:1-4.
5. MohitVirendra ,ShambhuUpadhyaya, Securing information through trust management in Wireless network,IEEE,2004.
6. Knut magnerisvik and Rolf michelsen,"Search engines and web Synamics" Computer networks volume 39 Issue3,21 June,P.289-302,2002,
7. Ahmed Ghoziaet. Al, "Improved Focused Crawling Using Bayesian Object based approach" A radio Science conference.National 18-20 March 2008.p.1-8,2008.
8. I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004
9. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications', IEEE Transactions on Consumer Electronics, voI.46,no.3,pp.395-403, Aug.2000.
10. M. Ali BaniYounes and A. Jantan, 2008,Image encryption using block-based transformation algorithm,in IAENG International Journal of Computer Science, Volume 35, Issue 1.
11. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229-234.