An Exquisite Cryptographic Algorithm for Lesser Amount of Data

Akhil Kaushik[1], Satvika[2], Manoj Barnela[3], Om Parkash[4]

Asstt. Prof. CSE Department[1,2]
Asstt. Prof. Electronics Department[3], Programmer CSE Department[4]
T.I.T&S College
Bhiwani, Haryana, India-127021

ABSTRACT

Once an application steps out of the bounds of a single-computer box, its external communication is immediately exposed to a multitude of outside observers with various intentions, good or bad. In order to protect sensitive data while these are en route, applications invoke different methods. In today's world, most of the means of secure data and code storage and distribution rely on using cryptographic schemes, such as certificates or encryption keys. Thus, cryptography mechanisms form a foundation upon which many important aspects of a solid security system are built. Cryptography is the science of writing in secret code and is an ancient art. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then; those new forms of cryptography came soon after the widespread development of computer communications. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. This paper describes cryptography and its types and then proposes a new symmetric key algorithm X-S cryptosystem based on stream cipher. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained.

Keywords

Cryptography, Encryption, Decryption, X-S cryptosystem, Pretty Good Privacy, Symmetric Key Algorithm.

I. INTRODUCTION

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with[2]. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals[5]. "Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key [1]. Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key" and, unfortunately, "private key") encryption, the same key (or another key fairly easily computed from the first) is used for both encryption and decryption. In asymmetric (also called "public-key") encryption, one key is used for encryption and another for decryption. More specifically, this paper deals with the Symmetric Key cryptography. A new Symmetric Key cryptographic algorithm has been proposed in this paper with its advantages and disadvantages.

II. CRYPTOGRAPHY HISTORY

Cryptography, the science of encrypting and decrypting information, dates as far back as 1900 BC when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate[6]. There are many notable personalities who participated in the evolution of Cryptography. For example, “Julius Caesar (100-44 BC) used a simple substitution with the normal alphabet (just shifting the letters by 3 positions) in government communications”[2], and later, Sir Francis Bacon in 1623, who described a cipher is known today as a 5-bit binary encoding. He advanced it as a steganographic device by using variation in type face to carry each bit of the encoding”. For all the historical personalities involved in the evolution of cryptography, it is William Frederick Friedman, founder of Riverbank Laboratories, cryptanalyst for the US government, and lead code-breaker of Japan’s World War II Purple Machine, who is “honored as the father of US cryptanalysis”[3][6]. In 1918 Friedman authored The Index of Coincidence and its applications in Cryptography, which is still considered by many in this field as the premiere work on cryptography written this century. During the late 1920s and into the early 1930s, the US Federal Bureau of Investigation (FBI) established an office designed to deal with the increasing use of cryptography by criminals. At that time the criminal threat involved the importation of liquor. According to a report written in the mid-1930s by Mrs. Elizabeth Friedman; a cryptanalyst employed by the US government like her husband, William F. Friedman, the cryptography employed by bootleggers. Although cryptography was employed during World War I, two of the more notable machines were employed during World War II: the Germans’ Enigma machine, developed by Arthur Scherbius, and the Japanese Purple Machine, developed using techniques first discovered by Herbert O. Yardley. In the 1970s, Dr. Horst Feistel established the precursor to today’s Data Encryption Standard (DES) with his ‘family’ of ciphers, the ‘Feistel ciphers’, while working at IBM’s Watson Research Laboratory[10]. In 1976, The National Security Agency (NSA) worked with the Feistel ciphers to establish FIPS PUB-46, known today as DES. Today, triple-DES is the security standard used by U.S. financial institutions. Also in 1976, two contemporaries of

Feistel, Whitfield Diffie and Martin Hellman first introduced the idea of public key cryptography in a publication entitled "New Directions in Cryptography". Public key cryptography is what PGP, today's industry standard, uses in its software. In the September, 1977 issue of The Scientific American, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman introduced to the world their RSA cipher, applicable to public key cryptography and digital signatures. The authors offered to send their full report to anyone who sent them self-addressed stamped envelopes, and the ensuing international response was so overwhelming the NSA balked at the idea of such widespread distribution of cryptography source code. In the mid-1980s ROT13 was employed by USENET groups to prevent the viewing of “objectionable material by innocent eyes”, and soon thereafter, a 1990 discovery by Xuejia Lai and James Massey proposed a new, stronger, 128-bit key cipher designed to replace the aging DES standard named International Data Encryption Algorithm (IDEA). This algorithm was designed to work more efficiently with “general purpose” computers used by everyday households and businesses. Concerned by the proliferation of cryptography, the FBI renewed its effort to gain access to plaintext messages of US citizens. In response, Phil Zimmerman released his first version of Pretty Good Privacy (PGP) in 1991 as a freeware product, which uses the IDEA algorithm. PGP, a free program providing military-grade algorithm to the internet community, has evolved into a cryptographic standard because of such widespread use. The initial versions of PGP were geared towards the more computer literate individual, but to the individual nonetheless. Phil Zimmerman could be compared to Henry Ford in his efforts to provide PGP to every home by making it free, and therefore, affordable. Today, PGP's updated version is offered free to the public. In 1994, Professor Ron Rivest, co-developer of RSA cryptography, published a new algorithm, RC5, on the Internet. It had been claimed that RC5 is stronger than DES[3].

III. PURPOSE OF CRYPTOGRAPHY

In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because X and Y are in remote locations, X must be sure that the information she receives from Y has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Y and not someone impersonating Y. Cryptography is used to achieve the following goals:

□***Confidentiality***: To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair[9].

□*Data integrity*: To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication codes or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered[1][9].

□*Authentication*: It assures that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent[8]. It basically provides authenticity to the communication.

IV. TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into ciphertext (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are

1) Public Key Cryptography which is also known as Asymmetric Key Cryptography and
2) Private Key Cryptography which is also known as Symmetric Key Cryptography.

i. ***Public Key Cryptography:*** Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement[5]. It overcomes over the biggest shortcoming of private key encryption i.e. key distribution problem in secret key cryptography[3]. It offers superior security than its counterpart. Now, it is the most widely accepted and used encryption standard in the commercial applications.

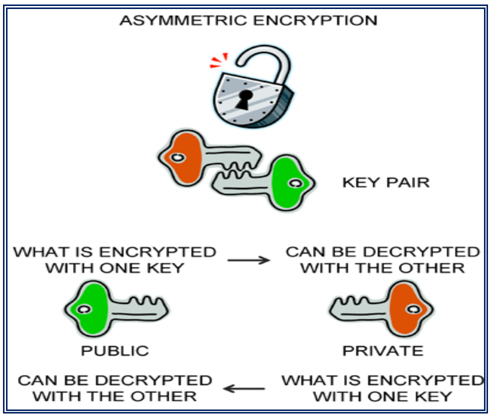
ASYMMETRIC ENCRYPTION
KEY PAIR
WHAT IS ENCRYPTED WITH ONE KEY
CAN BE DECRYPTED WITH THE OTHER
PUBLIC
PRIVATE
CAN BE DECRYPTED WITH THE OTHER
WHAT IS ENCRYPTED WITH ONE KEY

Figure 2: Public Key Encryption

ii. ***Private Key Cryptography:*** In private/ secret key cryptography, a single key is used for both encryption and decryption. As shown in Fig. 1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption[6]. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

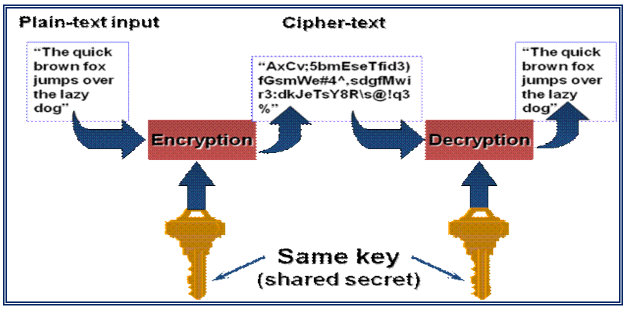
Plain-text input
Cipher-text
"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid3) fGsmWe#4^.sdgfMwi r3:dkJeTsY8R\s@!q3 %"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same key (shared secret)

Figure 1: Private Key Encryption

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher[7]. Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors[2], they are, by their nature, periodic so that the keystream will eventually repeat.

V. NEW SYMMETRIC KEY ALGORITHM

The new proposed encryption algorithm eXtended-Security (X-S) based on stream ciphers work as follows:

Step 1: Take character by character of plain text as the input.
Step 2: Substitute this character by the third letter to the right (same for digits and special symbols defined in the ASCII)
Step 3: Generate the ASCII value of the letter.
Step 4: Generate the corresponding binary value of it.
[The binary outcome must be of 8 digits; else zeros can be padded in the front to make the output 8-bit binary number]
Step 5: Apply shift right operation on this binary number 'n' number of times.
Step 6: Take a four digit number as the encryption key.
Step 7: Divide the output of step 5 with the chosen key.
Step 8: Store the remainder in first 3 digits & quotient in next 5 digits (If any of these are less then 3 and 5 digits respectively, then zeros can be padded in front.)
Step 9: A special symbol is chosen from a look-up table and is converted into 8-bit binary number.
Step 10: Result to step 8 and step 9 is then XORed to get the final output as ciphertext.

As X-S Cryptographic algorithm is based on private key encryption, hence decryption procedure is exactly opposite to the encoding process. X-S will take character by character of plaintext and convert it into corresponding ciphertext by the above mentioned encryption process. The following diagram illustrates the encryption technique for X-S cryptosystem:

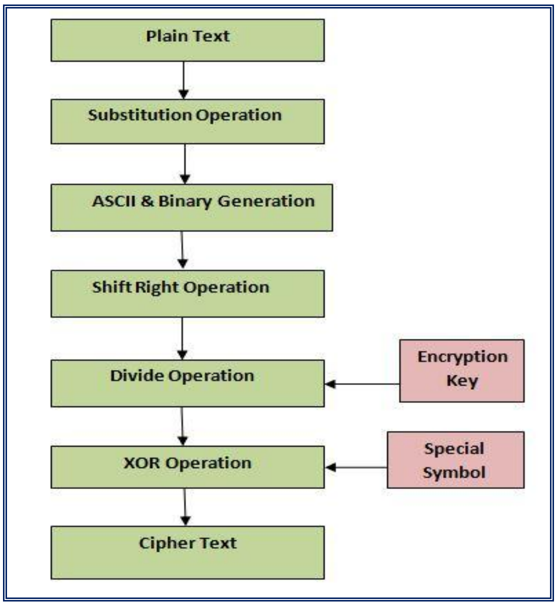

Figure 3: Encryption Procedure of X-S Encryption Algorithm

The X-S cryptosystem offers several advantages like speed of encryption along with better security. It offers security at two levels; first by using encryption key to achieve encrypted text and secondly XORing a special symbol is chosen randomly to complicate the calculation. Choosing the special symbol from a look table is done randomly to provide additional convolution[4]. The two-level safety ensures that even if cracker gets the secret key, still he can't decode the ciphertext until he has the table that contains special symbols. The X-S cryptosystem provides superior security and great encryption and decryption rate. This algorithm is designed for lesser amount of data and it must be used in its capacity to achieve better results.

VI. CONCLUSION

Cryptography is used to achieve few goals like confidentiality, data integrity, authentication, etc. of the data which is sent to the receiver from the sender. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. It has been found that the algorithms which are available at this moment are more or less difficult or complex in nature, and of-course it is quite obvious because those algorithms are used to maintain high level of security against any kind of forgeries. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm X-S has been designed in a quite simple manner but of-course not sacrificing the security issues. A single key is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. Finally, it is concluded that X-S cryptosystem is a one-stop-solution for the small to medium size organizations where optimal security with faster encryption is required for less loads of data.
The Future work may include the following:

- Design X-S algorithm as a public key algorithm for attaining improved defense of data.
- Hardware realization of X-S Algorithm.
- Implementing X-S for supporting both image and audio data.

VII. REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., pp 23-50, 1999.

[2] S.R. Kimbleton & G.M. Schneider, "Computer communications networks: approaches, objectives and performance considerations", ibid., pp. 129-173, 1975.

[3] L. Hill, "Cryptography in an algebraic alphabet", Am. Math. Monthly, 36, pp. 306-312, 1999.

[4] K. Zeng, C.H. Yang, D.Y. Wei & T.R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography", IEEE Computer, pp 8-17, February 199.1

[5] P.P Charles & P.L Shari, Security in Computing: 4th edition, Prentice-Hall, Inc., pp 40-42, 2008.

[6] G. Brassard, "A note on the complexity of cryptography", IEEE Trans., pp. 232-233, Oct 2000.

[7] S. Mathew & K. P. Jacob, "A New Fast Stream Cipher: MAJE4", Proceedings of IEEE, INDICON2005, pp 60-63, 2005.

[8] S.M. Matyas, "Digital signatures—an overview", Computer Networks, vol. 3, pp. 87-94, 1979.

[9] D. Davies, "Tutorial: the security of data in networks", IEEE Computer Society, 1981.

[10] "Data Encryption Standard", FIPS PUB 46, National Bureau of Standards, Washington, DC Jan. 1977.