ISSN 2229-5518

Secured Communication through Fibonacci Numbers and Unicode Symbols

A. Joseph Raphael, Dr. V. Sundaram

Abstract— The objective of cryptography is to make it feasible for two persons to exchange a message in such a way that other persons cannot understand. There is no end to the number of ways this can be done, but here the proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message. The original message usually called plain text is converted into cipher text by finding each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode symbols, which avoid suspicion from the third party when send through an unsecured communication channel. There are two levels in the proposed method; (i) converting plain text to cipher text and (ii) converting cipher text to Unicode symbols. In each level, security key is used to encode the original message which provides two levels of security from intruders. On the other end, the extraction algorithm is designed in such a way that the process converts the Unicode symbols into cipher text and then cipher text to plain text. This encoding and decoding scheme of the proposed method is significantly different as compared to the traditional methods.

Index Terms— Cipher text, Decryption, Encryption, Fibonacci Number, Key, Plain text, Unicode Symbols

1 Introduction

From the dawn of civilization to the highly networked societies that we live in today, communication has always been an integral part of our existence. What started as simple sign communication centuries ago have evolved into many forms of communication today, the internet being just one such example. Methods of communication today include radio communication, telephonic communication, network communication and mobile communication. All these methods and means of communication have played an important role in our lives, but in the past few years, network communication, especially over the internet, has emerged as one of the most powerful methods of communication with an overwhelming impact on our lives. Such rapid advances in communications technology have also given rise to security threats to individuals and organizations.

Cryptography is the art and science of secret writing. The term is derived from the Greek language krytos means secret and graphos means writing. Encryption is the actual process of applying cryptography. Much of cryptography is math oriented and uses patterns and algorithms to encrypt messages, text, words, signals and other form of communication. Cryptography has many uses, especially in the areas of espionage, intelligence and military operations. Today, many security systems and companies use cryptography to transfer information over the Internet. Some of this encryption is highly advanced; however, even simple encryption techniques can help uphold the privacy of any person.

2 Cryptography

The most ancient and basic problem of cryptography is secure communication over an insecure channel.

2.1 Related Terms

Cryptology [3] encompasses both cryptography and cryptanalysis and looks at mathematical problems that underlie them.

Cryptosystems are computer systems used to encrypt data for secure transmission and storage.

Plain text is a message or data which are in their normal, readable form.

Encryption is encoding the contents of the message in such a way that hides its contents from outsiders.

Cipher text results from plaintext by applying the encryption key.

Decryption is the process of retrieving the plaintext back from the cipher text.

Substitution cipher involves replacing an alphabet with another character of the same alphabet set.

Mono-alphabetic system uses a single alphabetic set for substitutions.

Poly-alphabetic system uses multiple alphabetic sets for substitutions.

Caesar cipher is a mono-alphabetic system in which each character is replaced by the third character in succession. Julius Caesar used this method of encryption.

A digital signature is a block of data that is generated by the sender of a message using his/her secret key.

2.2 Cryptographic Goals

Authentication: is the process of providing proof of identity of the sender to the recipient; so that the recipient can be assured that the person sending the information is who and what he or she claims to be [1].

Privacy/confidentiality: is the process of keeping information private and secret, so that only the intended recipient can understand the information.

Integrity: is the method to ensure that information is not tampered with during its transit or its storage on the network. Any unauthorized person should not be able to tamper with the information or change the information during transit.

Non-repudiation: is a mechanism to prove that the sender really sends this message.

2.3 Types of Cryptographic Algorithms

In general, there are three types of cryptographic schemes typically used to accomplish the cryptographic goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext.

2.3.1 Secret key cryptography

The process of encryption and decryption of information by using a single key is known as single key cryptography or symmetric key cryptography. In symmetric key cryptography, the same key is used to encrypt as well as decrypt the data. The main problem with symmetric key algorithms is that the sender and the receiver had to agree on a common key.

2.3.2 Public key cryptography

This cryptography technique is based on a combination of two keys—secret keys and public key. It is also known as asymmetric encryption. In this process, one key is used for encryption, and the other key is used for decryption. This process is known as asymmetric cryptography because both the keys are required to complete the process, and these two keys are collectively known as the key pair. In asymmetric cryptography, one of the keys is freely distributable and this key is called the public key which is used for encryption. Hence, this method of encryption is also called public key encryption. The second key is the secret or private key and is used for decryption. The private key is not distributable, like its name suggests, is private for every communicating entity.

2.3.3 Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a *digital fingerprint* of a file's content often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords.

2.3.4 Drawbacks of Existing Methods

- Transmission time for documents encrypted usng public key cryptography is significantly slower than symmetric cryptography.
- The key sizes must be significantly larger than symmetric cryptography to achieve the same level of protection.
- Public key cryptography is susceptible to impersonation attacks.

3 UNICODE

3.1 Birth of Unicode

ASCII, a character set based on 7-bit integers is still popular and its provision for 128 characters was sufficient at the time of its birth in the 1960s. The growing popularity of personal computing all over the world made ASCII inadequate for people speaking and writing many different languages with different alphabets. Newer 8-bit character sets, such as the ISO-8859 family, could represent 256 characters. This solution was good enough for many practical uses, but was a bit limiting for all the languages in the world [4]. In the end, the other parts of the world began creating their own encoding schemes, and things started to get a little confusing. It became apparent that a new character encoding scheme was needed, and the Unicode standard was born.

3.2 What is Unicode?

Unicode is a character encoding standard that has widespread acceptance. Unicode defines a large number of characters and assigns each of them a unique number, the Unicode code, by which it can be referenced. This encoding standard provides the capacity to encode all the characters used for the written languages of the world. The objective of Unicode is to unify all the different encoding schemes so that the confusion between computers can be limited as much as possible. The most common Unicode encodings are called UTF-n, where UTF stands for Unicode Transformation Format and n is a number specifying the number of bits in a basic unit used by the encoding. Two very common encodings are UTF-16 and UTF-8. In UTF-16, which is used by modern Microsoft Windows systems, each character is represented as one or two 16-bit (two-byte) words provides code point for more than 65000 characters (65536). Unix-like operating systems, including Linux, use another encoding scheme, called UTF-8, where each Unicode character is represented as one or more bytes [4]. The benefit of Unicode is that, it assigns each character a unique value and symbol, no matter what the platform, no matter what the program, no matter what the language [5].

4 NEW APPROACH USING FIBONACCI NUMBERS AND UNICODE SYMBOLS

Cryptography has now become an industry standard for providing information security, trust, controlling access to resources, and electronic transactions. Its use is no longer limited to just securing sensitive military information. In the proposed method, the plain text is converted into cipher text

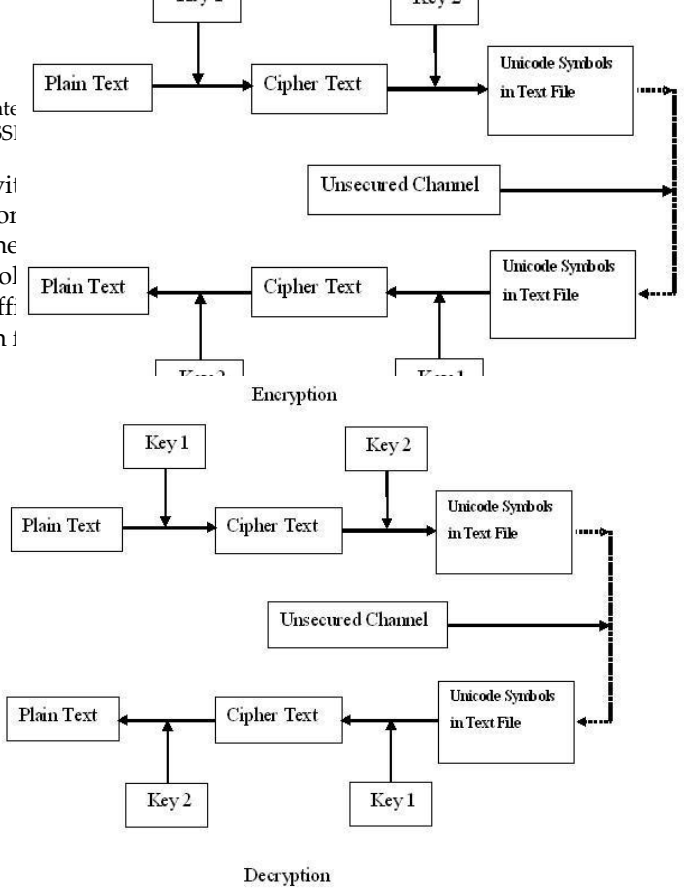


Figure 1: Affine Transformation of Encryption and Decryption Process

4.1 Encryption Method

In the proposed method, the original message called plain text is converted into cipher text with the help of Fibonacci numbers generated. Here, each character is extracted from the original message and is replaced with another character, the way the character is chosen to replace the original character makes this method unique and different when compared to the traditional methods. The obtained cipher text is converted into Unicode symbols, and these symbols in a text file are transmitted to the recipient through an unsecured communication channel. Since the message is encrypted in two levels, it is hidden from others and makes the decryption process more difficult for any intruders. The conversion of plain text to Unicode symbols undergoes two phases namely; converting plain text to cipher text and converting cipher text to Unicode symbols.

4.1.1 Plain Text to Cipher Text

The conversion from the plain text to cipher text can be explained through an illustration. Let us consider a message to be encrypted and send through an unsecured channel as "HELLO." Each character is replaced with another character based on the Fibonacci number and security key chosen. Any one character is chosen as a first security key to generate cipher text. The characters in the cipher text depend on the security key chosen, and the Fibonacci numbers generated. For instance, let the first security key chosen be v.

Plain Text: **H E L L O**

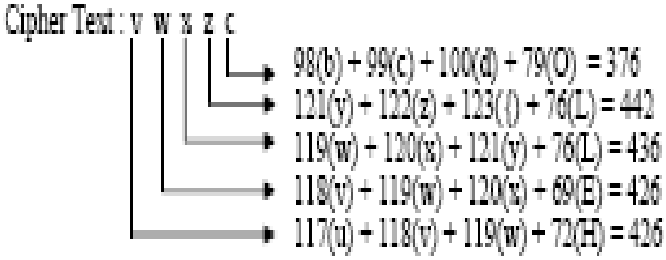
Characters: **v w x** y **z** a b **c** defghijklmnopqrstuvwxyzabc….
Fibonacci : **1 2 3 5 8** …

Cipher Text: v w x z c

The character set follows a round-robin method and the character which falls below the Fibonacci number will be taken as the character in the cipher text. If there are a number of characters in the plain text, the process of finding the replacing character with the Fibonacci number might be difficult because each time the size of the Fibonacci number is increased by adding the previous two numbers. If the application does not support the size of the Fibonacci number, after a fixed range, Fibonacci number can be restarted from the beginning. Since the selection of the character depends on the Fibonacci number, it provides more security for the system, and any unknown person cannot decode the message easily.

4.1.2 Cipher Text to Unicode symbols

In the second level of security, the ASCII code of each character obtained from the cipher text plus the ASCII code of its previous character, and next character is added to the ASCII code of the equivalent character in the original message. Here, ASCII codes of four characters are used as a security key to further encode the characters available in the cipher text to Unicode symbols. For instance,

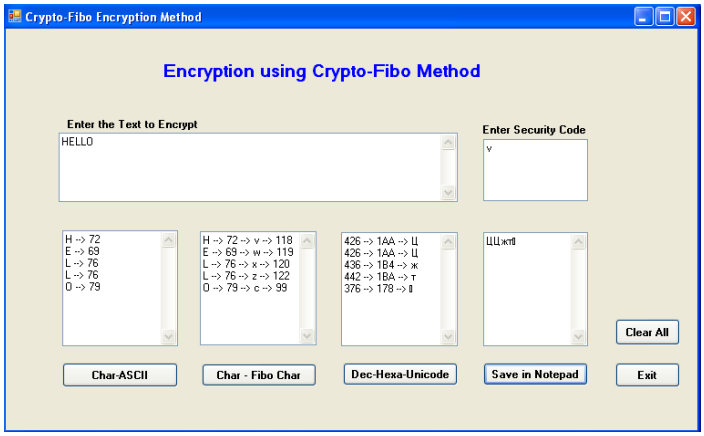


The decimal numbers obtained are converted into hexadecimal values to find its equivalent Unicode symbols. These symbols are saved in a text file which can be sent to the recipient through an unsecured communication channel. By looking at the symbols in a text file no unknown persons can identify what it is and the message cannot be retrieved unless the retrieval procedure is known.

Steps involved in Encryption

1. A sender wants to send a Hello message to a recipient.
2. The original message, also called plaintext, is converted to cipher text by using a key and Fibonacci numbers. The algorithm being used can produce a different output each time it is used, based on the key selected.
3. Cipher Text is converted into Unicode symbols using another key and saved in a text file.
4. The text file is transmitted over the transmission medium.

4.1.3 Implementation



4.2 Decryption Method

The decryption process follows the reverse process of encryption with the help of two keys. At the recipient end, from the received text file each symbol is extracted and mapped to find its equivalent hexadecimal value, further the obtained value is converted into a decimal value to find out the plain text using the key. Without the knowledge of the key, an unknown person cannot even suspect the existence of any secret message in these decimal numbers.

Key (chosen to encrypt): v

Characters : **v w x** y **z** a b **c** efghijklmnopqrstuvwxyzabc…

Fibonacci Numbers : **1 2 3 5 8** ……

Obtained Decimal Numbers: **426 426 436 442 376**

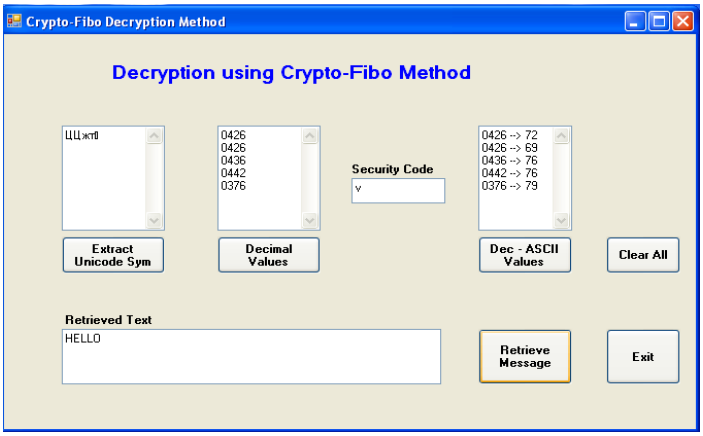
To extract the original plain text, ASCII code of each character from the cipher text plus the ASCII code of its previous character and the next character is subtracted from each obtained decimal number. The remainder is the ASCII code of character in plain text; the accumulated characters form the original plain text.

426 - (117 (u) + 118 (v) + 119 (w)) = 72 (H)
426 – (118 (v) + 119 (w) + 120 (x)) = 69 (E)
436 – (119 (w) + 120 (x) + 121 (y)) = 76 (L)
442 – (121 (y) + 122 (z) + 123 ({)) = 76 (L)
376 – (98 (b) + 99 (c) + 100 (d)) = 79 (O)

Steps involved in Decryption

1. At the recipient end, Unicode symbols are converted to hexadecimal values and then to equivalent decimal values using the same algorithm and key that were used to encrypt the message.
2. Perform subtraction with the decimal values and the ASCII code of characters from cipher text
3. The remainder after subtraction gives the ASCII code of the character in need.
4. The process is repeated for the number of characters in the cipher text and accumulated characters forms the original plain text.

4.2.1 Implementation



5 Combined Crypto-Steganography

Steganography is not the same as cryptography. Data hiding techniques have been widely used for transmission of hiding secret messages for a long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data is encrypted and the cipher text is embedded in Unicode symbols with the help of key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements for communication such as capacity, security and robustness to secure data transmission over an open channel.

6 Advantages

The proposed method is a process that scrambles information by rearrangement and substitution of content making it unreadable to anyone except the person capable of unscrambling it. Security key is provided in converting plain text to cipher text, and another key is used to convert the cipher text to Unicode symbols. Security key in each level is an added advantage to the method. It is difficult to decode the Unicode symbol from the text file which makes the system complicated in retrieval of the message for an unknown person. Moreover, information stored in a text file in the form of symbols increases the amount of information to be conveyed in secret. The advantage of using Unicode symbol reduces the suspicious while transmitting the file through an unsecured communica-

tion channel, else if any intruder tries to convert the symbol to the hexadecimal number nothing can be retrieved unless the retrieval process and the key is known.

7 Conclusion

Cryptography has evolved from an ancient science to an important area of research to secure communications. It has evolved from simple substitution ciphers to quantum cryptography. This method provides the means and methods of hiding data, establishing its authenticity, and preventing its undetected modification or unauthorized use. Furthermore, this presents a scheme that can transmit large quantities of secret information and provide secure communication between two parties. Any kind of text data can be employed as a secret message and is sent over the open channel, in the proposed procedure is simple and easy to implement.

References

[1] http://media.wiley.com/product_data/excerpt/94/07645487/0764548794.pdf, Chapter 1, Basics of Cryptography
[2] http://cs-exhibitions.uni-klu.ac.at/index.php
[3] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12
[4] Michał Kosmulski, Introduction to Unicode, http://www.linux.com/archive/articles/39911
[5] The Unicode Consortium, http://www.unicode.org
[6] B. B. Zaidan, A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences (2010), ISSN 1812-5654
[7] A. Joseph Raphael and Dr. V.Sundaram, "Secured Crypto-Stegano Communication through Unicode", World of Computer Science and Information Technology Journal Vol. 1, No. 4,138-143, 2011, ISSN: 2221-0741
[8] Dipti Kapoor Sarmah, Neha bajpai, "Proposed System for Data Hhiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.
[9] Sashikala Channalli and Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

Authors Profile

A. Joseph Raphael obtained his Master degree in Computer Science from St. Joseph's College, Tiruchirapalli and Master of Philosophy from Alagappa University, Karaikudi. Currently, he is a PhD research scholar at Karpagam University, Coimbatore, India and also working as a lecturer in the department of Information Technology, Ibra College of Technology, Sultanate of Oman.

Dr. V. Sundaram earned his PhD in mathematics from Madras University. He is a research guide of Anna University, Coimbatore and Karpagam University in the field of computer science and computer applications. He is currently guiding several PhD students in the areas of theoretical computer science, network security, cryptography and data mining. He has published several papers in national and international journals and organized 5 national conferences. He is a life member of ISTE and a member of Computer Society of India.