A systematic study on classical cryptographic cypher in order to design a smallest cipher

Md. Shamim Hossain Biswas*, Dr. Md. Asraf Ali, Dr. Mostafijur Rahman, Mr. Md. Khaled Sohel, Mr. Md. Maruf Hasan, Kausik Sarkar, Abu Shamim Aminur razzaque

* Department of Software Engineering, Daffodil International University
Bangladesh

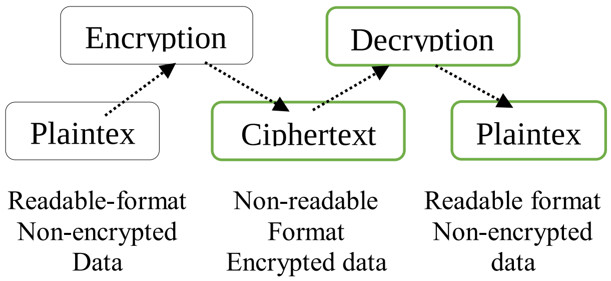
DOI: 10.29322/IJSRP.9.12.2019.p9662
http://dx.doi.org/10.29322/IJSRP.9.12.2019.p9662

Abstract- The cryptography is the branch of Cryptology. It is a combination of mathematics and computer Science. It is the study of obscuring information in cyberspace. Cipher is a set of algorithm which comprise of encryption and decryption. The cipher paly important role in modern technology. The technologies involving communication including the Internet, Mobile Phones, Digital Television, and ATM machine rely on cipher in order to maintain security and privacy. Thinking about aforesaid importance of cipher in cryptography, in this article, we have designed a smallest cipher which may be efficient in RFID chips. The smallest cipher has been comprised of five mathematical operation: Exponentiation, Multiplication, Addition, Subtraction and Division based on systematic study of classical cipher. The proposed cipher is a keyless cipher, but it is very efficient in secret information passing.

Index Terms- Cryptography, Classical Cypher, Smallest cipher

1. Introduction

In cryptography, a cipher is an algorithm for encrypting and decrypting data. To encipher a message, we need to convert information into cipher or code using encryption algorithm.


Encryption
Decryption
Plaintex
Ciphertext
Plaintex
Readable-format Non-encrypted Data
Non-readable Format Encrypted data
Readable format Non-encrypted data

Cryptography has been numerous phase of evolution. Early ciphers were designed to allow encryption and decryption by hand but those are developed and used today due to emerging computer technologies and its sophisticated performance. A list of classical cipher is given bellow.

1.1 Classical Cypher

XOR cipher, NULL Cipher**,** Baconian Cipher, Caesar Cipher, ROT$_{13}$ Cipher, Affine Cipher, Atbash Cipher, keyword cipher, Auto-key Cipher, Bifid cipher, Trifid cipher, Railfence Cipher, ADFGVX Cipher, ADFGX Cipher, Straddling Checkerboard Cipher, Permutation Cipher, Running Key Cipher, Nomenclators Cipher, Four-square cipher, Beaufort Cipher, Base64 Cipher, Lorenz Cipher, Enigma Machine Cipher, Polybius Square Cipher, Simple Polybius Cipher, Porta Cipher, Vigenere Cipher, Homophonic Substitution Cipher, Playfair Cipher, Hill cipher, Fractionated Morse Cipher, Scytale Cipher, Grille Cipher, VIC Cipher.

The remaining of this article is organized as a follows. Section 2 present classical literature review, Section 3 presents author contribution, Section 3.1.for illustration of proposed cipher, Finally, Section 4 and 5 show conclusion and acknowledgement.

2. Literature Review of Classical Cypher

2.1 XOR cipher

This is an additive cipher. It was invented in 1917 by Gilbert Vernam who was an engineer at Bell Telephone Laboratory. It is computationally inexpensive, however, it is vulnerable in plaintext attack and frequency analysis. It is often used in computer malware. The details can be found in [1-2].

2.2 NULL Cipher

It means that nothing Cipher**.** It is used in Steganography. This cipher can confuse the cryptanalyst to presume real message. The NULL cipher used to prison inmates in order to detect their most suspicious messages passing inspection. The detail of this cipher can be found in [3-6].

2.3 Baconian Cipher

It is used in steganography. This was invented by Francise Bacon in 1605.It can hide the message and distract a person from finding the real one. It offers a very little security. The details of the Baconian Cipher can be found in [7-8].

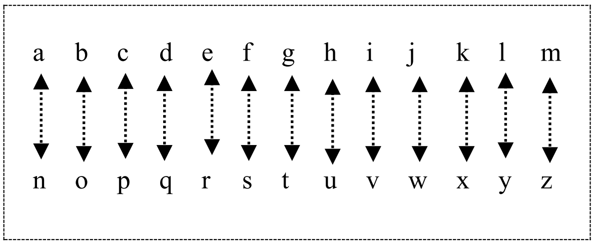
2.4 Caesar Cipher

It is one of the earliest cipher in cryptography. It is a substitution cipher. It was invented by Julius Caesar. The encryption is done by modular arithmetic using modulus 26. It first transform the letters into decimal number then apply modulus 26. It does not provide security. It has not any application in modern technology. The details about this cipher can be found in [9-10].

2.5 ROT$_{13}$ Cipher

It is a substitution cipher. The letter are replaced after 13th rotating. The ROT$_{13}$ Cipher is variant of Caesar cipher which was developed in Rome. In Mathematics, this is sometimes called an involution. In cryptography, it is called a reciprocal cipher.

ROT$_{13}$



Its strength is limited. It does not offer any security. It is used in puzzle solution. The details about this cipher can be found in [11-13].

2.6 Affine Cipher

It is a mono-alphabetic substitution cipher where each letter is mapped to its numeric number. It uses simple mathematical method for doing both encryption and decryption. It is better than Caesar cipher. It is vulnerable to all of the attacks that work against substitution ciphers. The details about this cipher can be found in [13-14].

2.7 Atbash Cipher

It is a substitution cipher. It has specific key where the letters of alphabet are reversed. It does not provide security and that is why it is vulnerable. The details about this cipher can be found in [14].

2.8 keyword cipher

It is a mono alphabetic substitution cipher. It can be cracked by some educated guessing. It is used in cryptographic practice. The details about this cipher can be found in [14].

2.9 Auto-key Cipher

It is a polyalphabetic substitution cipher. It is closely related to the Vigenere cipher, although, it uses a different method to generate the key. It was invented by Blaise de Vigenere in 1586. The key of this cipher can be attacked by using a dictionary attack. It is used by American Cryptogram Association. This is more secure than polyalphabetic. The details about this cipher can be found in [14].

2.10 Bifid cipher

It combines the Polybius Square with transposition cipher and uses fractionation to achieve diffusion. It was invented by Felix Delastelle. It is strong cipher, however, it can be quickly broken using a simulated annealing algorithm for finding the key square. It was not used by a military or government organization. The details about this cipher can be found in [14].

2.11 Trifid cipher

This is a combination of substitution with transposition and fractionation. It was invented by Felix Delastelle. It is vulnerable as keysquare can be revived by cryptanalyst. The details about this cipher can be found in [14].

2.12 Railfence Cipher

This is a transposition cipher. It does not offer communication security. It is used to cryptographic hobby group. The details about this cipher can be found in [14].

2.13 ADFGVX Cipher

It was invented by Colonel Fritz Nebel in 1918. It was a field cipher used by the German Army during World War I. It was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition. The fractionating nature of this cipher makes further difficulties. The details about this cipher can be found in [14].

2.14 ADFGX Cipher

This is an extension of ADFGVX Cipher. The key for ADFGX cipher is a keysquare and a keyword. It is just a simple substitution cipher and trivial to break. It is used in cryptographic hobby group. The details about this cipher can be found in [14].

2.15 Straddling Checkerboard Cipher

It is one kind device for converting an alphabet to nonsense manner. It is a substitution cipher. This cipher is vulnerable due to having advancement of Computer. The first step to breaking this cipher is to identify the blank positions in the key. This can often be done with frequency information analysis techniques. It has modern uses such as CodinGame. The details about this cipher can be found in [14].

2.16 Permutation Cipher

It comprises of transposition and substitution cipher. This is known as a regular columnar transposition. The message is deciphered by applying the inverse of the permutation. It is being widely used in modern cryptography. The details about this cipher can be found in [14].

2.17 Running Key Cipher

It is a type of polyalphabetic substitution cipher in which a text is used to provide a very long keystream. It does not repeat the key. A statistical patterns in both the key and the plaintext that can be exploited. It is used in cryptographic practices. The details about this cipher can be found in [14].

2.18 Nomenclators Cipher

It uses the elements of substitution ciphers and codes. This is combined with large homophonic substitution tables. The symbols for whole words is called codewords and letters were not distinguished among ciphertext. It used for diplomatic correspondence, espionage and advanced political conspiracy from the early fifteenth century to the late eighteenth century. It is vulnerable. The details about this cipher can be found in [14].

2.19 Four-square cipher

It is like a Playfair cipher. It is significantly stronger than substitution ciphers. It was invented by Felix Delastelle. It can be easily cracked if both plaintext and ciphertext are known. The details about this cipher can be found in [14].

2.20 Beaufort Cipher

It was created by Sir Francis Beaufort. It was a polyalphabetic substitution cipher. It uses a keyword and tableau recta to encipher the plaintext. It is breakable due cryptanalysts to having expertise knowledge in cryptography. It is used in academic cryptographic practice. The details about this cipher can be found in [14].

2.21 Base64 Cipher

It was originally used to encode binary information like images into a character string consisting of printable characters so it could be sent over the protocols like http. This is a keyless cipher. It provides weak security**.** It is used in a number of applications including email and storing complex data in XML. The details about this cipher can be found in [14].

2.22 Lorenz Cipher

It was a high security teleprinter cipher machine for communication by radio in complete secrecy. The security of this machine was not so great. It was used during World War II by the German Army for communication. The details about this cipher can be found in [14].

2.23 Enigma Machine Cipher

This device developed and used in the early mid-20th century to protect commercial, diplomatic and military communication. It uses a form of substitution ciphers. It was used by German military during World War II. The details about this cipher can be found in [14].

2.24 Polybius Square Cipher

It is a substitution cipher. The encryption and decryption involved in Polybius square cypher. It offers very little communication security and can be easily broken by hand. The details about this cipher can be found in [14].

2.25 Simple Polybius Cipher

It uses the ASCII table to encrypt and decrypt**.** Each character convert to ASCII code once upon a time and again converts ASCII to Characters. It is very weak. The details about this cipher can be found in [14].

2.26 Porta Cipher

This is a polyalphabetic substitution cipher. It was invented by Giovanni Battista della Porta. It uses 13 alphabets reciprocally and its enciphering is the same as deciphering. It is strong enough. The Porta cipher can be broken the same way as a Vigenere Cipher. It is recognized by ACA**.** The details about this cipher can be found in [14].

2.27 Vigenere Cipher

This is a polyalphabetic substitution cipher. It uses a keyword. It is little bit strong than mono-alphabetic substitution cypher. It can be cracked by the Chi-sq statistic test. It is used in cryptographic hobby group. The details about this cipher can be found in [14-17]**.**

2.28 Homophonic Substitution Cipher

This is a substitution cipher. It is much more difficult to break than standard substitution ciphers. It is difficult to break if the number of homophones is higher than as usual. The usual method for cracking is Hill Climbing, It is used in cryptographic exercise. The details about this cipher can be found in [14, 18].

2.29 Playfair Cipher

It was the first practical digraph substitution cipher. It was invented in 1854 by Charles Wheatstone, but it was named after Lord Playfair who promoted the use of the cipher. It has an interesting weakness which is repeated bigrams in the plaintext. It used to tactical purposes by British forces in the Second Boer War and in World War I. The details about this cipher can be found in [14, 19-21].

2.30 Hill cipher

It is a poly-graphic substitution cipher based on linear algebra. It was invented by Lester S. Hill in 1929. It was the first poly-graphic cipher. It has several advantages such as masquerading letter frequencies of the plaintext and high throughput. Noninvertible key matrix is the main disadvantage of this cypher. It is no longer used due to the vulnerability against known plaintext-ciphertext attack. It is still useful when combined with other non-linear operations, such as S-boxes. The details about this cipher can be found in [14, 22-23].

2.31 Fractionated Morse Cipher

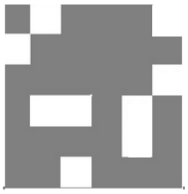
It requires convert the plaintext to morse code. It means that plaintext letters are mixed into the ciphertext letters. One of the benefits of the Fractioned Morse cipher is that it can encipher spaces and punctuation just as easily as letters. The trick to breaking Fractionated Morse is that finding the key. It is used by cryptographic hobby group. The details about this cipher can be found in [14, 24].

2.32 Scytale Cipher

It is the oldest ciphering method. It was difficult for spies to inject false messages into the communication between two commanders because scytale should have same diameter. It could not be easily broken. It used to communicate during military campaigns. The details about this cipher can be found in [14, 24-25].

2.33 Grille Cipher

It was invented by Cardan Grille as a method of secret writing in 1550. The recipient of the message must have possessed an identical grille. The following grid was used to encrypt and decrypt message.



This was an efficient techniques. The method was slow and requires literary skill. Cardan Grille used in both private and diplomatic correspondence. The details about this cipher can be found in [14, 26].

2.34 VIC Cipher

This is a substitution cipher. It is used in several impotant field of ciphers. It was used by Russian spies during the cold war. It is a combination of several things such as Straddlingcheckboard, Double columnar transposition, Lagged Fibonacci generators. The same straddling checkerboard used to encryption and decryption. It managed to remain unbroken. It is well designed and provides quite good security. The details about this cipher can be found in [14, 27].

3 Author Contribution

Presumably let an entity A wants communicate information to other entity B. Entities A and B both should have some confidentiality. The both entities A and B should have same functionalities. An entity A hide the message by solving the equation which consists of Exponentiation, Multiplication, Addition, Subtraction and Division operations. The other entity B opens the message by simply solving an equation which comprises of just two mathematical operations: Division and subtraction.

Encipher method: $c = \frac{\{(2^3 * m)+(2^3-1)+1\}}{2}$

Decipher method: $D = \frac{c}{4} - 1$

This is keyless cipher which has been implemented intentionally because of this research is to create a smallest cipher which facilitates the user to add their respective secret key in order to hide message from adversary.

3.1 Discussion of proposed Smallest Cipher

Assuming that Alice wants to send a secret information A=65 (ASCII value) to Bob, first she encrypts the message as follows.

C = $\frac{\{(2^3 * 65)+(2^3-1)+1\}}{2} = 264$ and then sends it to Bob. Receiver Bob decrypts the code by solving following equation:

D = $\frac{264}{4} - 1 = 65 = A$ (The message is successfully retrieved by the recipient).

4 Conclusion

The proposed smallest cipher method is efficient for message encryption and decryption. The proposed crypto-enabled techniques ensure no security because it is a key less cipher. We have created this cipher just doing mathematical problem solving skills. It represents a concrete ciphertext. We would like to keep a clue that is key-addition with the proposed cipher for future cryptographic researchers.

5 Acknowledgment.

We are very grateful by designing and publishing a smallest cipher. We want to thanks all of the members who are continue supporting the Daffodil International University.

Reference

[1] Richter, Wilfgang, Unbreakable cryptography in 5 minutes, 2012. In: ACM magagines for student.

[2] Professor Tutte Leture notes: additive cipher in 1998 In: University of waterloo.

[3] Federal Bureau of Investigation," Breaking code to stop crime part 1" in 2011(Retrived pdf:30.09.2018)

[4] Mark Adabi, "An atlanta jail intercepted a letter from an inmate whose poses a secret code to orchestrate a murder", in 2018, from Business insider.

[5] Gains, Helen F. "A study of Ciphers and Their Solution",2014, ISBN: 9780486800592, Courier Corporation .pp (4,5)

[6] Gordon, Adam, "Official Guide for Certified Information Systems Security Professionals" Auerbach Publication, 4th edition, 2015.

[7] Dupuy, Jr., Paul J. "The Advancement of Learning", 2017,

[8] Helen Founche Gaines, “A study of Ciphers and their solutions”, 1989, p-6. In: Cryptanalysis

[9] Luciano, Denis, Gordon P., “From Caesar Cipher to Public Key Cryptosystems”. In: Cryptology (The College Mathematic Journal), doi: 10.2307/2686311.JSTOR2686311.

[10] Wobst, Reinhardt”An approach to graphs of linear forms”, 2001, In Cryptology unlocked in by B. Smith. ISBN: 978-0-470-06064

[11] Mum Cryptolab publication “On the 2ROT13 Encryption algorithm”, 2004 In: pruefziffernberechnung.de

[12] Didier Stevens, Reverse Engineer, Blog post ROT13 is used in windows, 2016, In: didersteven.com

[13] Singh, Simon, “The science of secrecy from ancient Egypt to Quantum Cryptography”, 2000, ISBN: 0-385-49532-3

[14] The Wikipedia and Practicalcryptography each of them has well description about all of the ciphers.

[15] Martin, Keith M, “Everyday Cryptography” , 2012, In: Oxford University press. p.142. ISBN: 978-0-19-162588-6.

[16] Laurence Dwight smith” The Science of secret writing”, 1955 ISBN: 978-0-486-20247-1

[17] Gustavus J. Simmons “The Vigenere Cipher”, In Britanica.com and crypto Corner, 2018.

[18] Srahl. Fried A. “A Homophonic Cipher for Computational Cryptography”,1973 In: National Computer conference

[19] Cristensen, Chris, “Polygraphic Ciphers”2006, In: Northern Kentuchy University.

[20] Gaines, Helen Fouche” A study of Cipher and their solution”, 1956, Dover, ISBN: 0-486-20097-3

[21] Noor R, Al-Kazaz, Sean A. Irvine, William J. Teahan,” An automatic crypta analysis of Playfair cipher using compression” In: 1st conference of Historical Cryptology, Pages 115-124, 2018, Sweden.

[22] Jeffrey Overbey, William Traves and Ja\erzy Wojdylo,”On the key Space of the Hill Cipher”, 2005, In: Cryptologia, Vol. 29, No.1

[23] Murray Eisenberg” The Linear algebra behind the Hill Cipher”, 2013, In: Researchget publication.

[24] Kelly, Thomas, “The myth of the Skytale”, 1998, In: Cryptologia, 22:244-260, doi: 10.1080/0161-119891886902.

[25] Russel, Frank, “Information Gathering in classical Greece”, 1999. ISBN 0-472-11064-0.

[26] JiaLiul, Tanping Zhoul, Zhuo Zhang, Yanke, YuLei, Minqing Zhang, Xiaoyuan Yang,”Digital Cardan Grille: A modern approach for information hiding”, 2018

[27] Jozef Kollar, “Soviet VIC Cipher: No Respector of Kerckoff’s Principles”, 2016,In: Cryptologia, 40:1,33-48,doi:10.1080/01611194.2015.1028679

- *Md. Shamim Hossain Biswas*

MSc in Software Engineering (Daffodil International University)
BSc in Computer Science & Engineering (Stamford University)
ORCID: 0000-0002-4595-1470, PH: + 8801531 262 445
E-mail:shamim44-165@diu.edu.bd

- *Dr. Md Asraf Ali*

Associate Professor, Department of Software Engineering.
Faculty of Science and Information Technology

- *Mr. Md. Khaled Sohel*

Assistant Professor, Department of Software Engineering.
Faculty of Science and Information Technology

- *Mr. Md. Maruf Hasan*

Assistant Professor, Department of Software Engineering.
Faculty of Science and Information Technology

- *Dr. Md. Mostafijur Rahman*

Assistant Professor, Department of Software Engineering.
Faculty of Science and Information Technology

- *Kaushik Sarker*

Assistant Professor, Department of Software Engineering.
Faculty of Science and Information Technology

- *Abu Shamim Aminur Razzaque*

Lecturer, Department of Software Engineering.
Faculty of Science and Information Technology