A Study on some modified Classical Ciphers for Secure Crypto-System

Jayanti Sravani[a], Prof. A Chandrasekhar[b], Dr. Chaganti Pragathi[c]

[a] Research Scholar, [b] Professor , [c] Associate Professor
[a,b,c] Department of mathematics, GITAM Deemed to be University, Visakhapatnam, India
[a] sjayanti@gitam.in, [b] cakkaped@gitam.edu, [c] pchagant@gitam.edu

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The Classical Cryptography in the ancient times is a way for secure communication without Computer technology. Developments in the research and technology provide secure communications so as to make the Cryptanalysis difficult. Several Classical algorithms [1] explain the secure cryptosystems for maintaining Confidentiality and difficulty in the process of Cryptanalysis. In this paper we proposed a modified multiple encryption scheme over Classical Ciphers, affine and Caesar Ciphers for secure communications.

Keywords: Classical Ciphers, Cryptosystem, Caesar Cipher, Affine Cipher and Unicode characters

1. Introduction

The possibility of hacking or harming the messages which are communicated over secured channels is becoming low and designing such secure Cryptosystems which are not vulnerable is also becoming a challenging task. The recent research work focuses on Cryptology (the art of writing and solving the codes). Designing a mathematical model for secure Cryptosystems plays a vital role in Cryptology. The two types of Cryptography are Modern Cryptography and Classical Cryptography. The first Classical Cipher Caesar Cipher, an ancient Cipher deployed at the time of Julius Caesar which works with shift key 3 over modulo 26 where the plain text is over alphabets A to Z. By the Brute force attack the Caesar is vulnerable. In order to enhance the security several ciphers are developed [3][4][6][7]. In [1] and [5] classical ciphers are combined with Caesar cipher. The Classical ciphers work on letters and digits which can be modified for security enhancement. In [5] the plain text is considered over ASCII characters. In [1], while encryption, plain text characters positions have been swapped with the other characters in the plain text initially and then affine cipher has been applied. The same has been performed while decryption as well. In [5], the combination of Caesar and Affine cipher is used for encryption and decryption over ASCII characters for reliability when compared to the same code over alphabets. In [2], plain text was made to undergo encryption twice using Caesar and Affine ciphers and then the transposition cipher in the rice planting groove pattern was applied to their combination where the work was carried on ASCII characters. In this paper a method has been proposed which undergoes double encryption using Caesar Cipher initially and Affine Cipher later and vice-versa while decryption. The number of characters that are involved in this method is 143859 which represent the Unicode characters. Unicode characters include ASCII codes and several other scripts and symbols. The decimal equivalents of the Unicode characters are used for performing the operations as per the algorithm defined.

The Caesar cipher works as:

Encryption: $C \equiv P + k \ (mod\ n\ )$

Decryption: $P \equiv C - k \ (mod\ n\ )$

$n = number\ of\ characters\ (26\ alphabets)$

$k = key$

$C = Cipher\ text$

$P = Plain\ text$

Affine Cipher is an extension of Caesar Cipher with a combination of multiplicative cipher and shift cipher.

Encryption: $C \equiv a * P + b\ (mod\ n\ )$

Decryption: $P \equiv a^{-1} * (C - b) mod\ n$

$where\ n = number\ of\ characters$

$a = first\ key\ (\gcd(a, n) = 1\ for\ inverse\ of\ a\ to\ exist\ )$

$b = second\ key$

$a^{-1} = inverse\ of\ a\ \left(a * a^{-1}\ \equiv 1(mod\ n)\right)$

$C = Cipher\ text$

$P = Plain\ text$

2. Proposed Method

The following parameters are defined for usage in the algorithm:

$n = number\ of\ characters\ (\ here, Unicode\ characters\ are\ considered\ which\ are\ 143859\ in\ number)$

$a = first\ key\ (\gcd(a, n)\ must\ be\ 1)$

$b = second\ key$

$a^{-1} = inverse\ of\ a\ \left(a * a^{-1}\ \equiv 1(mod\ n)\right)$

$P = Plain\ text$

$P_1 = Initial\ plain\ text(while\ decryption)$

$C_1 = Initial\ Cipher\ text\ (\ while\ encryption)$

$C = Final\ Cipher\ text$

Encryption Algorithm:

Step 1: k = a + b$k = a + b$

Step 2: Convert plain text characters (Unicode) to its decimal equivalent.

Step 3: $C_1 \equiv (P + k) mod\ n$

Step 4: $C\ \equiv (a * C_1 +\ b) mod\ n$

Step 5: Convert the decimal equivalents of the cipher text to Unicode characters.

Decryption Algorithm:

Step 1: Calculate $a^{-1}\ \left(\ a * a^{-1}\ \equiv 1(mod\ n)\right)$

Step 2: Convert cipher text characters (Unicode) to its decimal equivalent.

Step 3: $P_1 \equiv\ a^{-1} * (C - b) mod\ n$

Step 4: $P \equiv (P_1 - k) mod\ n$

Step 5: Convert the decimal equivalents of the plain text to Unicode characters.

3. Results and Discussion[8][9]

The above defined method can be understood through an illustration for the plain text “Universe”:

Encryption:

Here we consider Unicode characters $n = 143859$.

Let $a = 2$ and $b = 5$ be the keys sent to the receiver over a secure channel.

Then $k = a + b = 2 + 5 = 7$.

Table 1.

Plain text(Unicode)	U	n	i	v	e	r	s	e

Decimal equivalent	85	110	105	118	101	114	115	101
Initial Cipher Text (Decimal equivalent) $C_1 \equiv P + 7(mod\ 143859)$	92	117	112	125	108	121	122	108
Final Cipher Text (Decimal Equivalent) $C\ \equiv 2 * P + 5(mod\ 143859)$	181	239	229	255	221	247	249	221
Final Cipher Text	¿	ï	Å	ÿ	Ý	÷	ù	Ý

Decryption:

Here $n = 143859$.

Receiver receives the keys $a = 2$ and $b = 5$.

Then calculates $k = 7$ and $a^{-1} = 71930(a * a^{-1} \equiv 1(mod\ n) implies\ 2 * a^{-1}\ \equiv 1(mod\ 143859)$)

Table 2.

Cipher text(Unicode)	¿	ï	Å	ÿ	Ý	÷	ù	Ý
Decimal equivalent	181	239	229	255	221	247	249	221
Initial Plain Text ($P_1 \equiv 71930 * (C - 5) mod\ 143859)$	13235120	16831620	16112320	17982500	15536880	17407060	17550920	15536880
	92	117	112	125	108	121	122	108
$P\ \equiv (P_1 - 7) mod\ 143859$	85	110	105	118	101	114	115	101
Final Plain Text	U	n	i	v	e	r	s	e

Thus the designed cryptosystem yields the desired results.

4. Conclusion

The above proposed method enhances the security to a greater extent because of the fact that in order to decrypt the cipher text one needs to have access to keys in both the steps. In fact, the rice planting groove pattern transposition cipher can be applied to the obtained cipher texts with the involvement of keys to encode the message for making the algorithm even more complex to perform cryptanalysis.

The implementation of this method on Unicode characters also adds to the security enhancement as the number of Unicode characters is 143859 which is a product of three prime numbers 3, 79 and 607 which increases the possibilities of key combinations making it difficult for cryptanalysis by brute force attack. This method can be used for password authentication since the Unicode characters are more in number.

References

1. Ajay babu Srimoju(2017) : Modification of Affine Cipher algorithms for Cryptography password : International Journal of Research in Science and Engineering-volume:3 Issue: 2.
2. D. S. Ginting(2017) : Modification of Symmetric Cryptography with Combining Affine Chiper and Caesar Chiper which Dynamic Nature in Matrix of Chiper Transposition by Applying Flow Pattern in the Planting Rice : Advances in Science, Technology and Engineering Systems Journal 2 6-12
3. Dey, S(2012) : SD-AREE:A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted : available online: https://arxiv.org/abs/1205.4279
4. Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath(2011) : A new Symmetric key Cryptography Algorithm using extended MSA method :DJSA symmetric key algorithm, : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June,2011, Page-89-94

5. Wulandari, S. Y. (2020). Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message. Proceeding International Conference on Science and Engineering, 3, 741-744 available online:https://doi.org/10.14421/icse.v3.595
6. Sundarayya P(2016) : Some Technique Algorithms of Extension of Affine Cipher Cryptosystem Using Residue Modulo Prime Number : Open Journal of Applied & Theoretical Mathematics
7. Sundarayya P & Vara Prasad G (2019) : A public key cryptosystem using Affine Hill Cipher under modulation of prime number : Journal of Information and Optimization Sciences, 40:4, 919-930, DOI: 10.1080/02522667.2018.1470751
8. https://en.wikipedia.org/wiki/Unicode
9. https://www.branah.com/unicode-converter.