CLASSICAL CRYPTOGRAPHY FOR KURDISH LANGUAGE

Najdavan A. Kako

Duhok Polytechnic University
najdavan.kako@dpu.edu.krd

doi:10.23918/iec2018.02

ABSTRACT

The most important concern in different data communication and transmission is to secure this data for every county individually. To transmit data through unsecure channel we need to use cryptographic algorithms, Kurdish language spoken by more than five million people. Unfortunately, there is no use of this language alphabet in data encryption and decryption. The purpose of this paper is to introduce the Kurdish alphabet usage in cryptography with a new symmetric algorithm which consist of 34 letters with using its ASCII Unicode and distributing the keys over the secure channel to decipher the text. This is the first attempt to apply an algorithm on the Kurdish characters.

Keywords: Symmetric, Asymmetric, Kurdish language, Modular.

1. INTRODUCTION

Data security known is a set of techniques to write a message in an encrypted form and sent it between the sender and the recipient, the first use of cryptography goes back to 1900 BC when the Egyptians used hieroglyphs to serve the Pharaohs [1]. According to some experts' statements, the cryptography appeared spontaneously after the invention of the writing arts with applications between diplomatic letters to the battle plans in the war [2, 3]. After the widespread of computers and developing it in communications and networking fields the new format of cryptography is appeared. When transferring and communicating data, the encryption is very important, especially in non-trusted environment, which includes networks in general and the internet in special. The clear text or plaintext is the data that can be easily read and understood without any particular alteration. The way to hide and disguise this data is called encryption. The ciphertext or the mysterious text is a non-readable and not understandable text, which was conducted by the cryptographic operations. Restoring the ciphertext to the original text is called decryption. The goals that must be achieved to achieve data security are:

- Authentication: The emphasis that the communicating object is the one that it affirms to be.
- Access Control: The averting of unauthorized employ of a recourse
- Data Confidentiality: The averting of data from unauthorized detection.
- Data Integrity: to ensure that data receipted are exactly as sent by an authorized object.
- Nonrepudiation: Provides security against negation by one of the entities included in a connection of having shared in all or part of the connection.
- Availability Service: Proof that the message was sent from a specific destination [4, 5].

The secret key is also embedded to the encryption algorithm, donor and recipient must have gained copies of the secret key in a secure pattern and must keep the key secure. The secret key is classified in cryptography in general either is stream cipher or a block cipher. Stream cipher works on one bit at time with implementation some form of feedback, so the key is constantly changing. Therefore, the cryptography does not only protect data from theft or changing, but, can be used to authenticate users. In general, there are three schemes of cryptographic that typically used to realize these goals: symmetric cryptography (or secret key), asymmetric cryptography (or public-key) and hash functions. Anyways, preliminary unencrypted data have referred to as plaintext. It is enciphered into cipher text, which will in turn usually be deciphered into usable plaintext [6, 7].

2. LITERATURE REVIEW

Symmetric key algorithm using ASCII characters proposed by Ayushi (2010). Anyone can be understood the message in clear text knowing the language if there is no codified method applied to the message in any way. Thus, we have to hide information from anyone for whom it is purposed, even they are on observation for encrypted data to ensure that we must use coding scheme [8].

An encryption algorithm based on ASCII value of data proposed by Satyajeet R. Shinge, Rahul Patil proposed (2014). They used a symmetric cryptographic algorithm based on the ASCII values of characters in the plaintext to encrypt and decrypt data. The timely execution of suggested algorithm was better and less. To encrypt the message the technique generates key spontaneously and it is transformed to another string for both encryption and decryption [9].

The effective symmetric key algorithm on Arabic characters introduce by Prakash Kuppuswamy, Yahya Alqahtani (2014). They proposed an integer value numerate from 0-9 called synthetic value assigning to a modular 37 and Arabic letters. Select an integer value and calculate its inverse with modular 37. To decrypt messaging the symmetric key allocation should be executed over the secured channel [10].

A. Vijayan, T. Gobinath and M. Saravanakarthikeyan (2016) in this research, they introduce an algorithm called AVB algorithm “ASCII value based encryption system” which is used to improve the data safety. The algorithm use ASCII value of data. ASCII value of the character is coded using normal mathematical calculation for number of time on a specific character and transformed to numerical value. Then, the cipher text is decoded to obtain the plain text [11].

In 2016 Pramod Gorakh Patil, Vijay Kumar Verma proposed “a reliable secret key algorithm for encryption and decryption of text data”. An effective, reliable symmetric key based algorithm was proposed by them to encrypt and decrypt the data text. They use ASCII (8 bit) value of characters and implement some simple logical NOT and binary division to calculate and produce. The implementing of the proposed technique is very simple to understand [12].

3. PROPOSED WORK

Since it is a first attempt to use Kurdish letters in cryptography to ensure data transmission their environment. Kurdish language is read and write in two ways either as a Latin alphabet or Arabic (Persian) alphabet, which is the official language in the country and starting from right to left, but we have proposed in our experiences the text that begins from left to right as it is in the English alphabet. One of the defying parts of modern computer science is to encipher and decipher the data in an effective way. In this research, we propose an algorithm that uses the ASCII values of the plaintext to encrypt it. This method randomly generates a key to uses it with encryption and decryption. Because of using the same key in the encryption and decryption procedure, it can be said that this is symmetric cryptographic algorithm. Whoever, the user Identification involve of Kurdish alphabets consist 34 letters. We are making a synthetic table using Kurd letters and their ASCII given in the Table 1.

TABLE 1.
ASCII for Kurdish Letters

ڕ	ر	د	خ	ح	چ	ج	ت	پ	ب	ا	ئ
12	11	10	9	8	7	6	5	4	3	2	1
1685	1585	1583	1582	1581	1670	1580	1578	1662	1576	1575	1574
ل	گ	ک	ق	ڤ	ف	غ	ع	ش	س	ژ	ز
24	23	22	21	20	19	18	17	16	15	14	12
1604	1711	1705	1602	1700	1601	1594	1593	1588	1587	1688	1586
		ێ	ی	ە	ھ	وو	ۆ	و	ن	م	ڵ
		34	33	32	31	30	29	28	27	26	25
		1742	1740	1749	1607	1735	1734	1608	1606	1605	1717

New Symmetric Key Algorithm

Key generation

Step 1: Choose randomly any number to be a key1

Step 2: Choose again any number making key2 then repeat step 2.

Step 3: Using modulo 1720 to find the inverse of key2.

Encryption algorithm

Step 1: Generate the decimal value of the character using text-to-decimal converter

Step 2: Add character value with random selected key1.

Step 3: Multiply the step 2 output with random selected key2

Step 4: Calculate with modulo 1720.

Step 5: Convert Decimal to Text

Decryption algorithm

Step 1: Convert text to decimal

Step 2: Multiply received letter with inverted key2

Step 3: Subtract the result of step 2 with key1

Step 4: Calculate with modulo 1720.

Step 5: Convert decimal to text.

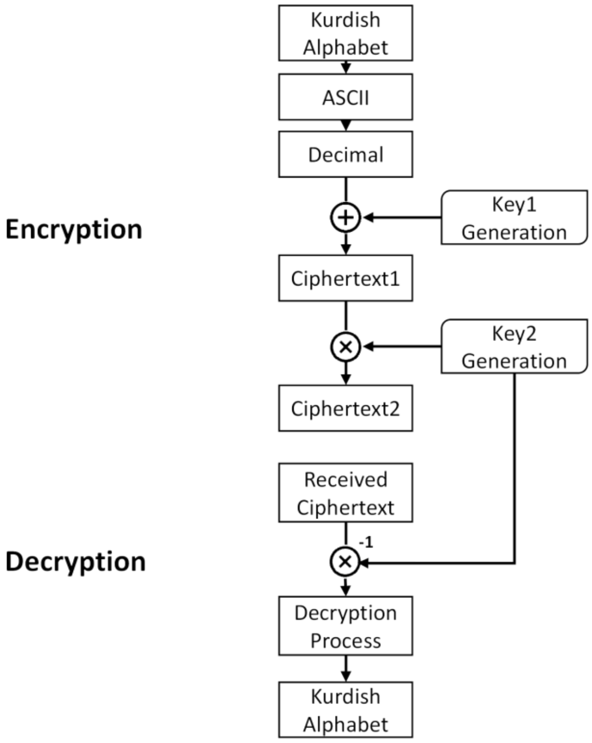

FIGURE 1. Encryption/Decryption Algorithm

4. IMPLEMENTATION

The effect of security is to encrypt text professionally that can abate the value of protest and capability of edition and falsehood. The confidentiality of data needs the encryption clearly to address. Furthermore, it can be used to achieve the privacy of data that can be read only for authorized one and difficult to modify in significant behavior. It is a keystone of network protocols security to be provided to accomplish network tasks. The results are described through an agreed-on sequence of protocol action. A good example when some users required the availability of resources for some operating system at different tasks. Hence, encryption is support availability. So, the heart of computer security is encryption.

ئەگەر هوین نەبن یەک

TABLE 2.
Kurdish Decimal Values.

ی	و	ه	ر	ە	گ	ە	ئ
1740	1608	1607	1585	1749	1711	1749	1574
ک	ە	ی	ن	ب	ە	ن	ن
1705	1749	1740	1606	1576	1749	1606	1606

Processing of key

1) Choosing a two random integer number to be key1 =17 and key2= 41.

2) Finding modular multiplicative inverse for key2 = 881 to use in decrypting.

Encrypti

TABLE 3.
Encryption Method.

PT	Text to Decimal	add key1 = 17	Multiply by key2 =41	mod 1720	Decimal to Text
ئ	1574	1591	65231	1591	ط
ە	1749	1766	72406	166	¦
گ	1711	1728	70848	328	ň
ە	1749	1766	72406	166	¦
ر	1585	1602	65682	322	ł
ه	1607	1624	66584	1224	ӈ
و	1608	1625	66625	1265	ӱ
ی	1740	1757	72037	1517	□
ن	1606	1623	66543	1183	ҟ
ن	1606	1623	66543	1183	ҟ
ە	1749	1766	72406	166	¦
ب	1576	1593	65313	1673	ډ
ن	1606	1623	66543	1183	ҟ
ی	1740	1757	72037	1517	□
ە	1749	1766	72406	166	¦
ک	1705	1722	70602	82	R

Decryption

TABLE 4.
Decryption Method.

CT	Text to Decimal	Multiply by inv. key2 = 881	Subtract with key1 =17	mod 1720	Decimal to Text
ط	1591	1401671	1401654	1574	ئ
¦	166	146246	146229	29+1720	ە
ň	328	288968	288951	1711	گ
¦	166	146246	146229	29+1720	ە
ł	322	283682	283665	1585	ر
ӈ	1224	1078344	1078327	1607	ه
ӱ	1265	1114465	1114448	1608	و
□	1517	1336477	1336460	20+1720	ی
ҟ	1183	1042223	1042206	1606	ن
ҟ	1183	1042223	1042206	1606	ن
¦	166	146246	146229	29+1720	ە
ډ	1673	1473913	1473896	1576	ب
ҟ	1183	1042223	1042206	1606	ن
□	1517	1336477	1336460	20+1720	ی
¦	166	146246	146229	29+1720	ە
R	82	72242	72225	1705	ک

5. CONCLUSION

In this work we attempted an algorithm to encipher and decipher Kurdish letters employing decimal value of its letters to secure Kurdish communications. A two keys are used for encryption/decryption. The algorithm was tested for different sizes of messages and the method of trying Kurdish letters it has been used on other cryptography algorithm. The results exhibits that the proposed method is progressed the performance interaction, however the good quality of security services are provided for Kurds communication in different fields.

6. FUTURE WORKS

Each letter of international languages have a certain frequency depending on its repetition in writing and this method is used as an aid to breaking algorithms. In future we will conduct the frequency analysis of Kurdish letters in both dialects (Kurmanji and Surani) over many sources to get stable distribution of letter frequency analysis.

REFERENCES

[1] A. D’Agapeyeff, “Codes and Ciphers,” A History of Cryptography, Blackfriars Press, 1949.

[2] W. F. Friedman, “History of the Use of Codes,” Aegean Park Press, Laguna Hills, CA, 1977.

[3] R. Nichols, Lanaki’s. “Classical Cryptography Course,” Lecture 6, Part II: “Arabian Contributions to Cryptology”, American Cryptogram Association, Jan. 1996. Accessed from the web February 9, 2013.

[4] S. William, “Cryptography and Network Security” Principles and Practice, 7th edition, Pearson, Inc., 2017 pp 21-45.

[5] S. Singh, “The Code Book,” The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor Books (a division of Random House), New York, 1999.

[6] M. Cozzens and S. J. Miller, "The Mathematics of Encryption," An Elementary Introduction, Vol. 09, Mathematical World, Providence, Rhode Island: The American Mathematical Society, 2013, pp. 133-180.

[7] S. Singh, “Arab Code Breakers,” SimonSingh.net, 2012, accessed February 14, 2013.

[8] Ayushi, “A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications, Vol. 1, No. 3, pp. 1-4, Feb 2010, ISSN: 0975 - 8887.

[9] S. R. Shinge, R. Patil, “An Encryption Algorithm Based on ASCII Value of Data”, International Journal of Computer Science and Information Technologies, Vol. 5, Issue 6, pp. 7232-7234, November 2014, ISSN 0975-9646.

[10] P. Kuppuswamy, S. Al-Khalidi, “New Innovation of Arabic Language Encryption Technique Using New Symmetric Key Algorithm”, International Journal of Advances in Engineering & Technology, Vol. 7, Issue 1, pp. 30-37, March 2014, ISSN: 2231-1963.

[11] A. Vijayan, T. Gobinath and M.Saravanakarthikeyan, “ASCII Value Based Encryption System (AVB)”, International Journal of Engineering Research and Applications, Vol. 6, Issue 6, pp. 08-11, April 2016, ISSN: 2248-9622.

[12] P. G. Patil1, V. K. Verma, “A Reliable Secret Key Algorithm for Encryption and Decryption of Text Data”, International Journal of Recent Trends in Engineering & Research, Vol. 2, Issue 2, pp. 114-118, February 2016, ISSN: 2455-1457.