EXTENDED TINY ENCRYPTION ALGORITHM EQUIPPED WITH ARABIC SCRIPT (AXTEA)

S.Z. Naseem, S. Nazir, M.S. Sarfraz, U. Shoaib and A. Altaf
Department of Computer Sciences, University of Gujrat – Pakistan
Corresponding Author's email: zagham@gmail.com

ABSTRACT: Cryptography is a science that deals with secret writing. Now a days, every programming language, browsers, and famous databases support the UTF-8 code. Therefore, it is easier to store Arabic script languages into the database. Most encryption algorithms are used to convert plain text to cipher, whereas cipher is usually in the same language with the text being ciphered or in special characters. In this paper, we enhanced an algorithm (XTEA) and converted English plain text to Arabic script language (for instance, Arabic, Urdu, and Persian) using Extended Tiny Encryption Algorithm (XTEA). The proposed algorithm was implemented in PHP, and the results show that the resultant cipher was more secure. It enhanced the security of data because the medium of the ciphered text was not same as plain text. We named our proposed algorithm as Arabic Extended Tiny Encryption Algorithm (AXTEA).

Keywords: Algorithm, scripted Arabic language, Cryptography, Decryption, Encryption, Key.

(Received 1-6-2018 Accepted 18-9-2018)

INTRODUCTION

People living across the world used different languages and patterns for communication. However, the variations in languages and their pattern of interaction pose barriers to communicate with people living in different regions of the world. The field of computer science is also facing the same issue as English become international language (vetilani, 2009). Whereas, Arabic scripting languages are very rarely used due to its methodologies, unavailability of algorithms and source code (Rehman, 2014). The gap between communication languages can be reduced with the help of some effective decisions. Decades ago, a computer was considered only for affluent (Gupta, 2006). These assumptions proved wrong after the development of massive innovative applications and the computer became affordable and accessible for the common person.

In this modern era of technology, when everyone has access to the internet, the integrity, confidentiality and authentication of data become essential elements of communication. The cryptography is considered the only method to achieve mentioned key elements of communication. Cryptography is derived from Greek words which mean secret writing (Tanenbaum, 2003). It is defined as the renovation of simple words into complex words that will hide original data to make it secure. Cryptography is divided into two vital types: one is Symmetric key cryptography, and other is Asymmetric key cryptography. In a symmetric cipher, a predefined key called shared key is used to encrypt and decrypt data (Azouzi, 2006). A single key is used between the sender and receiver. The sender uses some encryption algorithms and shared key to converting plain text into cipher text whereas, the receiver converts the ciphered text into plain text using the decryption algorithm with the key shared by the sender. In the case of asymmetric cipher, a pair of key, namely public key and private key are assigned to each user (sender and receiver). The pair of the key has its own purpose. The public key is shared with all members whereas; the private key is kept secret by the user. In this algorithm, the sender uses the public key of each corresponding receiver to encrypt the message. Whereas; the receiver uses its private key to decrypt that encrypted message (Salam, 2011).

The five components are involved in this process that includes: plain text, secret key, public key and encryption/decryption algorithms. Symmetric cipher can be divided into two types, i.e. substitution cipher and transportation cipher (Forouzan, 2006). In a substitution cipher, one character of plain text is replaced with another character. Unlike the substitution cipher, the ciphered text is obtained by only swapping the characters of plain text in transportation cipher, t, the content remains in the plain text. The transported plain text is further organized in a two-dimensional table with the help of predefined key (e.g. Hello). The online applications become popular over the years with the rapid growth of internet user (Shoeb, 2013). By closely observing the statistics from developed countries, we conclude that at least four applications are connected to the internet (Daly, 1998; Lin, 2008; Soumitra, 2015). On the other hand, this ratio in under-developed countries reduces to one-half of developed countries. The statistics showed that a huge amount of data transmit over the internet (Lin, 2008).

The several encryption algorithms, routing protocols and advanced tools are used to secure a huge amount of data over the internet (Sivakarthik, 2010).

Encryption algorithms have several types, which includes; data encryption standard, triple data standard, advanced encryption standard and blow fish (Schneier, 1993; Neelima, 2015). Data encryption standard was first introduced by NIST based on IBM Lucifer algorithm (Feistel, 1994). In 1974 DES used as standard algorithm because of its popularity. However, several weakness were found for certain the key length The triple data standard, is the enhancement of data encryption standard; it uses the same technique with three times increment of key length, which make it slower than other encryption technique (Singh, 2011). The third type is an advanced encryption standard, which is also introduced by NIST in 1997 to replace data encryption standard, it becomes very popular because of its speed and flexibility (Westulnd, 2002). It is mostly being used in small devices. The fourth type of encryption algorithm is called blow fish, which is being used very commonly and introduced by Bruce Shenier (Schneier, 1993; Kazys, 2015). Cryptography is the combination of the multiple algorithms and techniques to protect the data from any unauthorized persons. In our paper, we proposed the XTEA algorithm localized into Arabic which is very useful, secure and difficult to break for crypt analysist. The coming part of the paper in this section will discuss the work done in encryption algorithms.

The Tiny Encryption Algorithm (TEA) is a block cipher encryption algorithm that uses a symmetric key encryption technique (Needham, 1994; Wheeler, 1997). It uses a different method for encryption, instead of memory consuming data arrays; it encrypts data using many iteration cycles (Forouzan, 2006). Various cycles like XOR, Integer addition and left/right shift are utilized instead of any mind-boggling system. The number of rounds before changing a single bit spread to near 32 is at generally 6, with the goal that 16 cycles may suffice, and it suggests 32. It uses 128-bit key as this is sufficient to counteract modest inquiry strategies being successful in 1996. Kelsey (Feistel, 1994; Jamuna, 2016) established that the effective key size of TEA was 126 bits. The Tiny Encryption Algorithm is a Feistel cipher in which multiple algebraic operations are performed. Figure 1 describes the process and working of TEA.

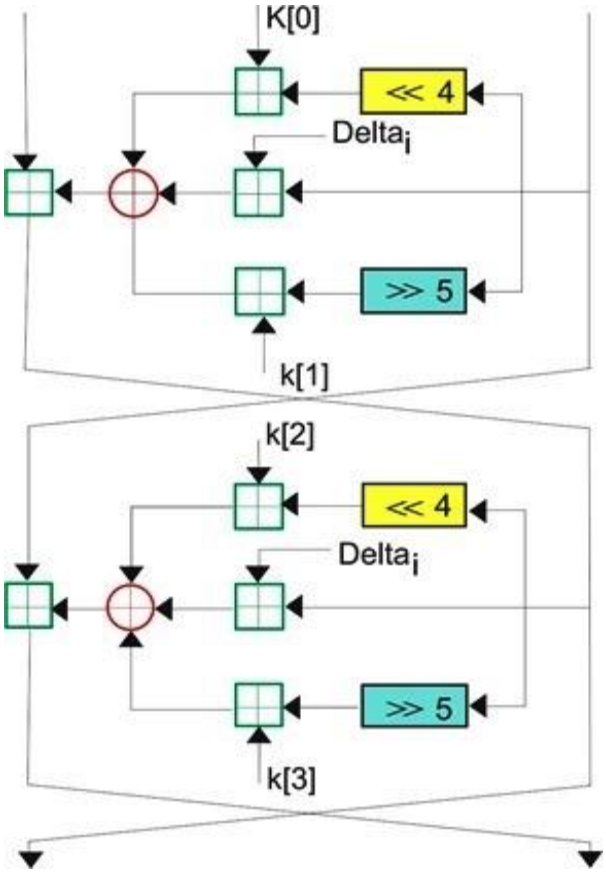

Figure-1: The process of TEA: Integer addition, XOR operation, Right and Left shifts of data is used (Salam, 2011)

In 1997 David Wheeler and Roger Needham presented the XTEA (Extension Tiny Encrypt Algorithm) (Singh, 2011) after finding the weakness in TEA in cryptanalysis. It is also fiestel structure block cypher, having 64 bits block with 128 bits key. Different changes occurred in XTEA. The subkeys idea is introduced in this algorithm. The disorder of addition, XOR, shifts operators and irregular sequence of subkeys are used to make it more secure (Wheeler, 1997). Figure-2 describes the process and working of XTEA. The process of right and left shift XOR and Integer addition is shuffled in XTEA.

Cryptanalysis is artistry to analyze the information hidden in the ciphertext to retrieve the plain text. In XTEA, the weakness is found to reacquire the plaintext without knowing key and algorithm (Schaefer, 2009). In TEA cryptanalysis, various cryptanalysis techniques are proposed like Differential cryptanalysis, Related-Key Cryptanalysis and Impossible Differential Cryptanalysis (Kelsey, 1997; Marcio, 2017). Cryptanalysis is very helpful in enhancing data secrecy and security.

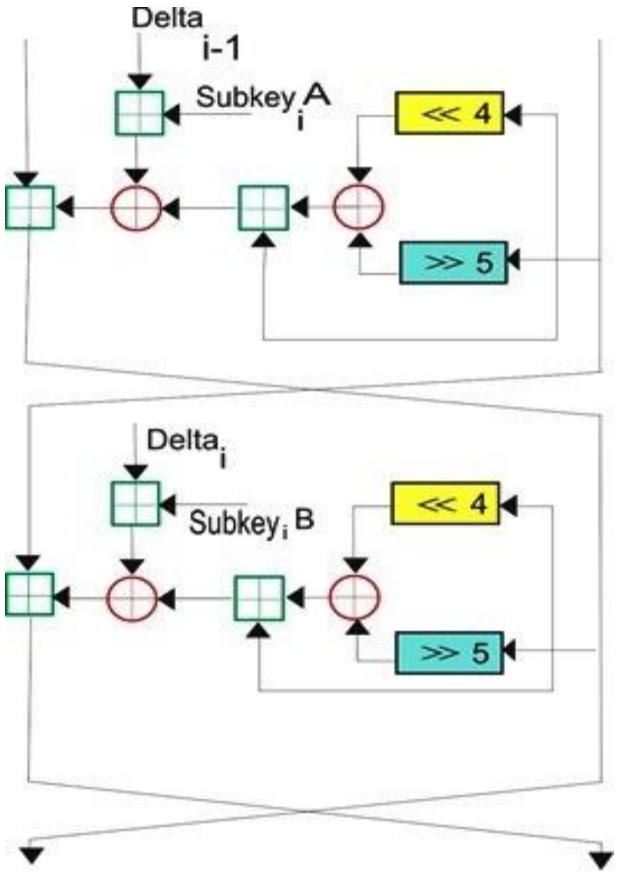

Figure-2: The process of XTEA for two rounds (Salam, 2011)

MATERIALS AND METHODS

In AXTEA, we had defined a table (Table-1) with Arabic characters that possess equal ASCII codes as of English characters. For example, we set Arabic word ا (alif) equal to ASCII code 88, which is the ASCII code of English character X. We also compared encrypted text (cipher) to the conversion table and replaced English characters with Urdu characters. For example, we had an "Xqi" cipher, and we replaced it using our conversion table to "اک ل" or "کل ا". A detailed table is given below (cross-reference).

Every implementation had its conversion table which was different from others. This will make the algorithm more secure, and even if crypt analysis of the algorithm is known, the attacker will not be able to decrypt AXTEA unless he has the conversion table. We can make more than 1 conversion tables by replacing 1st character with 1st table, 2nd character with 2nd table and so on. This would make AXTEA more secure and can avoid repetition detection. Urdu has a total 38 letters, Arabic has 28 letters while English has 52 characters (small + capital). We can use extra characters from other languages of the same script, for example, Persian, Pashto, Sindhi etc.

A k-permutation of a set with a number of elements n is a selection of k elements taken from the set of n elements such that the order of elements should be different, and repetition of the elements is not allowed.

No. of Total element n = English alphabets (small + capital) = 52

No. of selected element k from the given in changed order.

$$P(n,k) = \frac{n!}{(n-k)!} = \frac{52!}{(52-52)!} = \frac{52!}{1} = 52!$$

According to the above given formula calculation of all possible conversion tables is impossible for the system to store in the memory because factorial of 52 is a large number (8.0658175e+67).

RESULTS AND DISCUSSION

The proposed system is composed of XTEA with additional cipher table of Arabic scripted language. The system is sub-divided into two parts that implements two possible processes, i.e. encryption and decryption. The block diagram is shown in Figure-3.

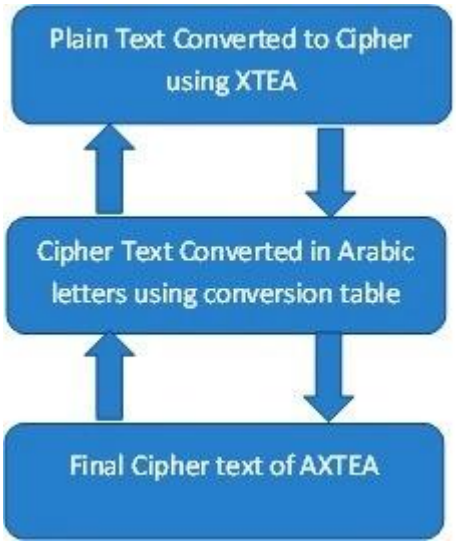

Figure-3: Working of AXTEA algorithm

For a clear explanation, an example is demonstrated, Figure-4 and Figure-5. We encrypted a string, "a quick brown fox jumps over the lazy dog" into "q kveox rp ebooou zaistyg hcfjlmn d rwua" using XTEA with the specified key and then that string is converted into Arabic/Urdu scripted text using table. For instance, we have "ء" for U, "خ" for f etc. and finally we obtained encrypted text shown below:

“/فسھےنعجشٹقژحئل۲۲ک۳دخن
<ٹئرطج/۷<ھخشقصحۓ۸تگنجۃڑآگتبٹ۲اچر۰ت۶۰نھز۸ئشنقجبۃ۷ف
۹۴ض۱>پ=”.

We have implemented the algorithm using PHP language. The Implementation of XTEA integrated with Arabic cipher table is available on http://xtechnos.com/research/axtea/.

Table-1: Sample Conversion Table Based on Random Alphabets Selection.

English	ASCII	Urdu	English	ASCII	Urdu	English	ASCII	Urdu	English	ASCII	Urdu
D	68	آ	W	87	ف	M	77	ذ	d	100	ے
X	88	ا	E	69	ق	R	82	ر	f	102	ځ
Z	90	ب	Q	113	ک	z	122	ڑ	v	86	څ
C	99	پ	J	74	گ	b	66	ز	l	76	ښ
A	97	ت	I	105	ل	V	118	ژ	t	84	ڼ
L	108	ٹ	S	83	م	m	109	س	h	72	ړ
O	111	ث	j	106	ن	n	78	ش	T	116	ى
a	65	ج	F	70	و	p	112	ص	x	120	ئ
P	80	چ	e	101	ہ	B	98	ض	s	115	ڨ
N	110	ح	i	73	ه	c	67	ط	y	121	ڳ
o	79	خ	H	104	ھ	g	103	ظ	w	119	ګ
K	107	د	U	85	ء	q	81	ع	u	117	أ
Y	89	ڈ	G	71	ی	k	75	غ	r	114	ٹُ

Figure- 4. Interface of AXTEA implemented in PHP

Figure- 5: Example string conversion using AXTEA.

Conclusion: The current paper enhanced the XTEA algorithm and introduced an Arabic script language table in it to generate a cipher, and we named this algorithm as AXTEA. It would be difficult to predict the cipher because AXTEA's cipher is not in English. It will be difficult to find the language of a cipher as many languages use the same script as Urdu, Arabic, Persian, Punjabi, and Pashto. It will be difficult to revert it to English if the attacker will able to find out the language because every implementation will have its conversion table. As aforementioned, AXTEA has 52 conversion tables, so it is impossible for a computer to compute all the conversion tables to break the algorithm and which makes our proposed algorithm less hack prone. AXTEA is still the simple and more secure algorithm. Comparatively AXTEA requires more computer processing than TEA and XTEA, but on the other hand, it is much more secure.

Acknowledgements: We want to give an extra word of thanks to Mr. Gul Sher Ali who interfaced pleasantly during copyediting and proofreading of this paper.

REFERENCES

Daly, J. (1998). Corporations Use of the Internet in Developing countries. World Bank Publications.

D. Jamuna, S. Emalda (2016), Light Weight Cryptographic Algorithms for Medical Internet of Things (IoT) - A Review, International Conference on Green Engineering and Technologies (IC-GET

El-Azouzi, R.,(2016). Advance in Ubiquitous Networking 2. Proceedings of UNet;16. 397 p. Springer.

Feistel, H. (1994). Block Cipher Cryptography System. Google Patents.

Forouzan, A. (2006). Data Communication and Networks. Tata McGraw- Hill Education.

Gupta, G. (2006). Computer Literacy: Essential in today's Computer-centric World. ACM SIGCSE BUllentin, pp. 115-119.

Kelsey, j. B. (1997). Related-Key Cryptanalysis of 3-way, Biham -des, cast, des-x, newdes, rc2, and tea. International Conference on Infoemationm and Communication Security. Springer.

Kazys, GytisV. And Robertas (2015), An Algorithm for Key-Dependent S-Box

Generation in Block Cipher System, INFORMATICA, Vol. 26, No. 1, page 51–65

Lin, C. a.-S. (2008). Study on Internet Usages, academic achivements, and the exploring capability of regional culture knowledge using Internet: A Case of Primary School Students in Taiwan Transcations So Infromation Science and Applicatios, 5(10), p1428-1437.

Marcio R., Daniel S. and Marcus P. (2017), A Hybrid Block and Stream Cipher Encryption Scheme Based on Collision Resistant Hash Functions, e Ciência e Tecnologia da Presidência da República Federativa do Brasil (CNPQ)

Neelima S. and Sunita M. (2015), Review paper on cryptography, International Journal of Research (IJR), Volume 2, Issue 05.

Needham, R. a. (1994). TEA, A Tiny Encryption Algorithm. International Workshop of Fast Software Encryption . Springer .

Rehman, B. H. (2014). ASCII Based GUI System for Arabic Scripted Language: A case of Urdu. Internation Arab Journal of Information Technology (IAJIT), p 4-11.

Salam, M. R. (2011). A NXM Version of 5X5 Playfair Cipher for Natural Language (Urdu as Special Case). World Academy of Sciecne Engineering and Technology, p73.

Schaefer, E. (2009). An Introduction To cryptography and Crypt analysis. Califfornia's Silicon Valley:Santa Clara University .

Schneier, B. (1993). Description of New variable-LengthKey, 64-bit block Cipher (Blowfish) . International Workshop on Fast Software Encryption . Springer.

Shoeb, M. a. (2013). A Crypt Analysis of the tiny Encrption Algorithm in Key Generation. International Journal of Communication and Technologies, ed 1, p38.

Singh, S. a. (2011). Comparison of data encryption algoritm. International Journal of Computer Science, p125-127.

Sivakarthik, D. a. (2010). Enhancement in Encryption Through Localization.

Soumitra D., Thierry G., Bruno L. (2015), Global Information Technology Report 2015 ICTs for Inclusive Growth World economic forum

Sebastian W., Ashutosh D. and Pawel Mi (2015), Differential-linear and Impossible Differential Cryptanalysis of Round-reduced Scream.

Tanenbaum, A. (2003). Computer Networks. In Computer Networks 4th edition. Prentice Hall.

Vetilani, Z. (2009). Human Language Technology Challenges for computer Science and Linguistics. 4th Language and Technology Conference, LTC. Springer.

Westulnd, H. (2002). NIST Reports Measureable Success of Advanced Encryption Standard. Journal of Research of National institute of standards and Technology, p 56-57.

Wheeler D. Needham, R. (1997). Extended Tiny Encryption Algorithm.