Journal of Engineering and Applied Sciences 14 (4): 1331-1338, 2019
ISSN: 1816-949X

New Cryptographic System of Romanized Arabic Text Based on Modified Playfiar

Inas R. Shareef, Noor D. Al-Shakarchy, Enaam Hadi Abd,
Dhamyaa A. Al-Nasrawi, Huda F. Al-Shahad and Hiba J. Aleqabie
Department of Computer Science, College of Science, University of Karbala, Karbala, Iraq

Abstract: One of the most spoken language in the world today is Arabic language. The other hand the development of applied e-Government in most fields, required using of internet, many treatments may be in Arabic language. The most critical challenge is to achieve a sufficient level of security and prevent unauthorized users from acknowledged on important information during transmission of data. The researches of encryption and decryption Arabic languages can be considered few and old. In this study, new method was proposed consist of three major steps: firstly, romanize Arabic text that mean convert from Arabic alphabet to Latin alphabet. Secondly, the rominized text encrypted/decrypted with modified Playfair cipher using 6×8 matrix and unicode. The encryption/decryption implemented by generating Knight tour key. Finally, Deromanizing process to get Arabic plain text. The proposed system was evaluated by (statistical characteristics, frequency test and serial test and entropy). The experimental results proved that the romanizing process provide the confusion and diffusion concepts which are the goal of any cipher system. These concepts supply the randomness of ciphertext and make system more robust against any third parity.

Key words: Romanizing system, cryptographic, ciphertext, key generation, randomness, unicode, Knight tour

INTRODUCTION

Because of the huge amounts of personal data that deling with the internet, it has become very important to develop ways to protect information from people with bad intentions. There are several exchanges of information need to be confidential. So, it is therefore, necessary to develop ideas in area of cryptographic.

Cryptography is the area of study that uses the mathematics to ciphering and deciphering data. Cryptography permits you to keep and convey data safely through risky channels (internet). Unlike cryptography, cryptanalysis is the science of understanding and resolve secure connection. Classical cryptanalysis is multidispelentry cover several science fileds include inganalytical reasoning, application of mathematical tools, pattern finding, endurance will power and of course lots of luck. Cryptanalysts are also called attackers (Stallings, 2005).

Arabic language is the one of widely spoken language in the world. It has distinctive features that differentiate it from the other languages (Hassan *et al*., 2018). It is the second most usually utilized script after Latin. Arabic language includes 28 fundamental letters, 3 long vowels (Alef (ا), Waw (و) and Yeh (ي)) and 25 consonants (Al-Nasraw *et al*., 2016).

Cryptography of Arabic text has received the least attention from historians and researchers. There are some research and studies on this subject, Atee (2011) presents symmetric encryption system for Arabic character letters. The developed algorithm based on binary and decimal encoding schema with XOR logical function. The encryption key used in the system consist of 15 digits divided to two parts first 5 digit represent the encoding of first character of message. The second part 10 digit represent the actual key used with the XOR function. Possible to include or not include the key within the message, according to what was agreed upon between the parties. The plaintext divided to blocks of two characters length and encrypted each block of two symbols together by XORing with actual key in order to eliminate the problem of the most frequent letters in the Arabic language and by which they can predict the original text of the message. Although, this method provide the reasonable randomness of the ciphertext but its suffer from loss some data in deciphering process. The frequency characters that eliminates during encoding process of encryption side, cant predicted in the decryption side which causes loss some characters of original message (Atee, 2011).

Alqahtani *et al*. (2013) implement modification of Vigener cipher system based on alphabetic consist of 26 characters of the main Arabic language symbols in addition to Arabic numbers and blank space such as [أ = 0, ب = 1, ... , ي = 27], [28 = blank space] and [٠ = 29, ١ = 30, … , ٩ = 38]. Vigener algorithm as well as its modification is one of the polyalphabetic symmetric cipher system based on modular function (modular 38 in presented

Corresponding Author: Inas R. Shareef, Department of Computer Science, College of Science, University of Kerbala, Kerbala, Iraq

system) which can't hide the natural properties of used language. Thus, this system is more poor against the statistical crypt analysis because the key can be predicted using Kassiski method (Alqahtani *et al*., 2013).

Kuppuswamy and Alqahtani (2014) present symmetric key algorithm on Arabic characters. They propose a modular 37 and Arabic letters assigning to the integer value also numerals 0-9 also assigned as an integer number called as synthetic value. They are selecting random integer and calculate inverse of the selected integer with modular 37. From the experimental results, the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data (Kuppuswamy and Alqahtani, 2014). The core of this system is the random number selected but the calculation of inverse to the random selected number must be satisfied number theory theorems: "if GCD (a, n) = 1; then these exist an integer x, $0<x<n$ such that ax mod n = 1" where a is the random selected number, x is inverse of a and n represent the number of alphabetic 37. Otherwise, the inverse cant calculated.

Rihan and Osma (2016) present a genetic algorithm in the weight adjusting process during trainig of proposed Artificial Neural Network (ANN). The architecture of proposed ANN introduced by 12 notes as input layer represent ascii code of input plaintext characters and 12 notes as output layer which represent ciphertext random numbers for Arabic language. This cryptography technique training the ANN and deal weights matrix as chromosome in genetic algorithm to determine the best weights results. The weights that saved from genetic neural network training process represent the secret key of the cipher system and must share by the sender and the recipient. In sender side the weights matrix used to generate the ciphertext. The receiver side use inverse weights matrix in order to obtained Char's ASCII code (Rihan and Osma, 2016). In spite of the proposed ANN system provide good randomness to the ciphertext but it is important drawcomes of it. The weights matrix represent the key of the system and although, this key is secret but selecting another key required to re-trained the network on other data. On the other side computing the inverse weights matrix required more time and efforts.

Mansour and Fouad (2017) introduce a hybrid encryption algorithm based on natural language phonetics significantly. The encryption algorithm can be divided to two steps. The first step is mapping the phonetic difference between languages by the computer keyboard. Direct ASCII mapping is used in that system. The second step is the Private Key Exchange (PKE) which can be implemented by ciphering process. The system modeled the phonetic intermediate language such as Arabic language used in that system, then identify many keys for each language to determine which of the keystrokes will be used. Direct ASCII mapping and the model of phonetic intermediate language constant for each language that causes the system couldn't hide the natural properties of the original language (Mansour and Fouad, 2017).

Shaban and Al-Din (2017) introduce an Arabic text encryption method as NP-hard problem based on a one way function. The proposed system employ a principle of integration to achieve security and complexity of system. This method provided robust against statistical cryptanalysis which can be more difficulties for predicting the correct keys and correct plain text. The core of the proposed system based on integration formula and the goal is to couldn't guess the correct integration formula thus, implies to couldn't guess the correct keys. The recent methods and tools in the mathematics based linear and differential cryptanalysis can represent the weak point of that system (Shaban and Al-Din, 2017).

Despite of this number of research and studies, still a need for an efficient method that can be hide the natural features of the Arabic language besides that provid high efficient against cryptanalysis methods. Unfortunately, these methods do not always guarantee robust against the statistical cryptanalysis because there is no prove of that.

In this study, new method of cryptography was proposed based on confusion (which achieves by rominazation system) and diffusion concepts (which achieves by unicode) to overcome the natural features of the Arabic language. The rominized text encrypted/ decrypted with modified Playfair cipher using 6×8 matrix and unicode. The encryption/decryption implemented by generating Knight tour key. Thus, the contributions of this study are summarized as:

- Rominazation system for Arabic adapted with major modifications taking into account the alphabet in one byte only
- Modify version of Payfair cipher using 6×8 matrix as well as key generated by Knight tour
- Enhance version of Playfair cipher using unicode

MATERIALS AND METHODS

The native language of more than 200 million people in North Africa and the Middle East is Arabic. In most Internet applications that use Arabic language an adequate level of security must be achieved during data transfer. Therefore, new cryptographic method was

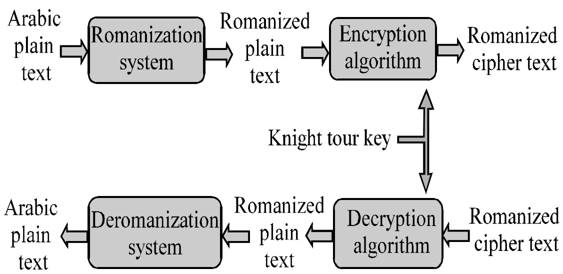

Fig. 1: Proposed cryptographic system

Adapted rominazation system
Inputs: Arabic plain text
Output: Rominazed plain text
For each char in Arabic plain text if char in dictionary: get Latin charcter else: do nothing

Fig. 2: Example of rominazing system

proposed based on rominazing system for Arabic languge. The encryption/decryption process was implemented step by step as illustrated in Fig. 1. While the following subsections explaines the details of these steps.

Rominazation system for Arabic language: The romanization of Arabic mean convert a written and spoken Arabic to the Latin script in a systematic way. There are several purposes for romanized Arabic among them transcription of names and titles, language education, cataloging Arabic language works, ..., etc. Unfortunately, no uniform results in the romanization of Arabic because the Arabic script usually omits vowel points and diacritical marks from writing (Anonymous, 2018; Raphael and Sundaram, 2012). The purpose of romanization system in proposed method is to overcome the natural features of the Arabic language. Rominazation system for Arabic adapted with major modifications taking into account the alphabet in 1 byte only and the romanization is generally reversible. Table 1 shows the maping of adapted rominazation system for Arabic.

Table 1 contain 48 characters, all Arabic letters which are in unicode range from 0621-063A and from 0641-064A besides the arabic digits in unicode range from 0660-0669 (Al-Nasrawi *et al*., 2015, 2018) and two special characters (“and”). Note from Table 1 that for each Arabic symbol there is a unique Latin symbol in just one byte. Programmarly, rominazation system and derominazation was implemented by dictionary data structure in c# as mapping process see the following pesedo code that explains adapted rominazation system for Arabic text while the example of Arabic plain text and equivelence rominaized plain text based on Table 1 was shown in Fig. 2.

Table 1: Adapted rominazation system

Arabic	Latin	Hex	Arabic	Latin	Hex
ء	â	00E2	ظ	Z	005A
أ	ã	00E3	ع	Á	00C1
آ	ä	00E4	غ	G	0047
ؤ	ö	00F6	ف	f	0066
إ	ï	00EF	ق	q	0071
ئ	î	00EE	ك	k	006B
ى	¥	00A5	ل	l	006C
ا	Â	00C2	م	m	006D
ب	B	0062	ن	n	006E
ة	Ð	00F0	ه	h	0068
ت	T	0074	و	w	0077
ث	ø	00F8	ي	y	0079
ج	J	006A	Space	i	0069
ح	H	0048	.	a	0061
خ	Æ	00C6	٠	0	0030
د	d	0064	١	1	0031
ذ	Ð	00D0	٢	2	0032
ر	r	0072	٣	3	0033
ز	z	007A	٣	4	0034
س	s	0073	٥	5	0035
ش	§	00A7	٦	6	0036
ص	$	0024	٧	7	0037
ض	D	0044	٨	8	0038
ط	T	0054	٩	9	0039

Knight tour key: All chess pieces move in straight line except the Knight. It moves in an L shape in any direction. The legal move for a Knight is two positions in one direction, then one in a columnar direction, Fig. 3. In Knight’s tour, each square must be visited exactly once.

In most symmetric cryptographic systems, the encryption/decryption key are the same. These systems require that the sender and receiver agree on a key before they can communicate securely (Stallings, 2005). The purpose of this step is to generate encryption/decryption key where used the principle of Knight tour, the resulted key called (Knight tour key). There are some important parameters to generate the Knight tour key. First, the dimensions of chess board which depend on the alphabet used in cryptography system. In proposed method 6×8 chess board was used. Second, the key length which equal to the number of Knight tour moveis. Third, the starting point of Knight tour. In this study, initial position of Knight tour is (0, 0). Figure 4 shows 6×8 chessboard and the alphabets of rominazed text.

The generation of Knight tour key based on Warnsdorff’s rule: “Always move to an adjacent,

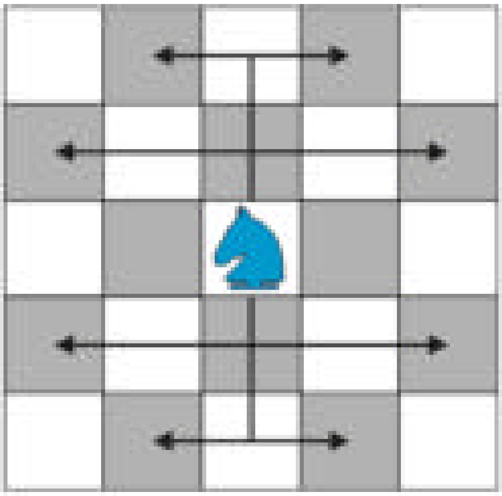

Fig. 3: Legal moves for a Knight

```
{'â', '¥', 'j', 'z', 'Z', 'l', 'i', '4' },
{'ã', 'Â', 'H', 's', 'Á', 'm', 'a', '5' },
{'ä', 'b', 'Æ', '§', 'G', 'n', '0', '6' },
{'ö', 'ð', 'd', '$', 'f', 'h', '1', '7' },
{'ï', 't', 'Ð', 'D', 'q', 'w', '2', '8' },
{'î', 'ø', 'r', 'T', 'k', 'y', '3', '9' }
```

Fig. 4: 6×8 chessboard

unvisited square with minimal degree" (Ganzfried and Cull, 2004) which explained in the following pesedo code Algorithm 1:

Algorithm1: Generating Knight Tour key
Inputs: 6×8 chessboard
Output: Knight Tour board with moves number
Set initial position on the chessboard Mark the first position to "1" For each possible moves on the board: -find the set of positions accessible from the current position -find the position with minimum accessibility -Mark the board with the current move number Return the marked board with the move number

The key length is agreed upon by the sender and recipient when encryption/decryption are applied. Figure 5 shows the example of Knight tour key with length 17. The blue circle means start position while red circle represents end postion. Because the key generated by Knight tour, there is no repetition in the characters. Note the Knight tour key in Fig. 5 is "âH ä¥sl519wTt$bïrq".

Encryption/decryption method: In this study, we will explaine the encryption/decryption of proposed method

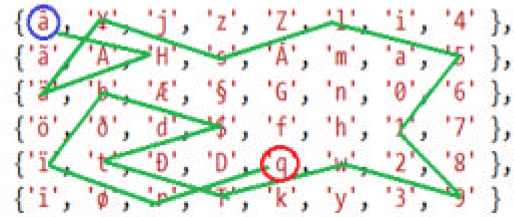

Fig. 5: Example of Knight tour key with length 17

```
{'â','H','ä','¥','s','l','5','1' },
{'9','w','T','t','$','b','ï','r' },
{'q','j','z','Z','i','4','ã','Â' },
{'Á','m','a','Æ','§','G','n','0' },
{'6','ö','ð','d','f','h','7','Ð' },
{'D','2','8','î','ø','k','y','3' }
```

Fig. 6: Modified Playfiar encryption matrix

in detials. After the rominazation system and key generation are completed, the encryption process begins.

The Playfair cipher is a way to encrypt text in classical cryptography system. This cipher is an example of a double letter word system which means encoding characters in pairs. The cipher method needs a key that does not contain duplicate characters and if any should be deleted. The Playfair cipher use a matrix of 25 with 5 columns and 5 lines including the Latin letters in sequence after deleting the letter J and replacing it with I. The key letters are first placed in the matrix (Stallings, 2005). The encryption rules of the Playfire cipher system is summarized as follows:

- Rule 1: If m1, m2 in same row, then c1, c2 are the two characters to the right of m1, m2, respectively
- Rule 2: If m1, m2 in the same column, then c1, c2 are below the m1, m2
- Rule 3: If m1, m2 are in different rows and columns then c1, c2 are the other corners of rectangle
- Rule 4: If m1 = m2 a null character (e.g., x) is inserted in the plaintext between m1, m2 to eliminate the double
- Rule 5: If the plaintext has an odd number of characters a null character is appended to the end of the plaintext

In this study, two Playfair cipher modifications ware proposed. First, without unicode by a using 6×8 matrix containing the resulting alphabet from the rominazation system "48 characters" (Fig. 6). Second with unicode by using unicode.

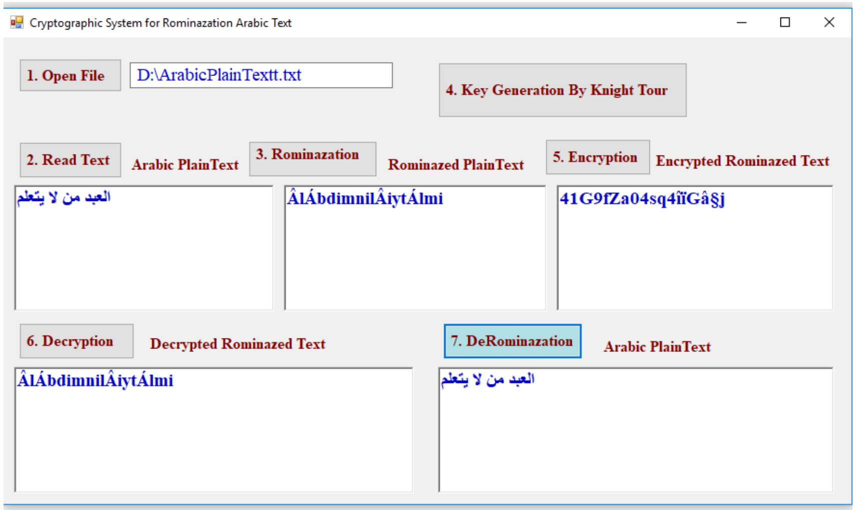

Fig. 7: GUI of modified Playfiar cipher system without unicode

In general, the two modified Playfire cipher (without and with unicode) was explained in details in the following subsections.

Modifications Playfair cipher without unicode: A several modifications have been proposed described:

- Use 6×8 matrix instead of 5×5 matrix
- Modified matrix does not contain all English characters but only the resulting symbols from rominazation system
- No repetion symbols in the key because it generated by Knight tour which visit every square only once in chessboard. So, there is no repetition
- When the plaintext word consist of odd number of characters, a symbol " " is added to complete the pair
- The space was considerd in modified Playfire matrix The ciphertext seems to be a stream of characters instead of separate words that are easy to guess. The space symbol romanized to "i", Table 1
- All encryption rules of the Playfire cipher system applied in modification Playfire cipher except rule 4. That mean the rule was not considerd in modified Playfair cipher. Therefore, reption in pair letters was allowed

Now, we will explain the proposed method in details by example. We encrypt the Arabic plaintext "العبد من لايتعلم" using modified Playfair cipher without unicode. Figure 6 shows the modified Playfair encryption matrix with Knight tour key of length 17. For decoding, the process is inverse. Figure 7 shows the GUI of modified Playfair cipher system without unicode.

Example1

Arabic Plaitext:	العبد من لا يتعلم
Romanized Plaintext:	ÂlÁbdimnilÂiytÁlmi
Diagraphs:	ÂlÁb dimnilÂiytÁl mi
Romanized Ciphertext:	41G9fZa04sq4ïïGâ§j

Modifications Playfair cipher with unicode: In unicode, there is a unique number for every character, regardless of what platform, application, device or language. Unicode used in many applications such as information hiding (Rahma *et al*., 2013a, b; Kumar *et al*., 2015) also in text editors (Al-Nasrawi *et al*., 2014), cryptography (Al-Shakarchy *et al*., 2018; Balajee, 2011; Raphael and Sundaram, 2012).

In this study, unicode was used to add more security to proposed method. All modification in Playfair without unicode was implemented here but adding another step of convert rominazed ciphertext to unicode. This step was done by combining hex code of pairs to outcome one chatcter in unicode. For the same example above, the result of encryption was explianed in Fig. 8.

Example2

Arabic Plaitext:	العبد من لا يتعلم
Romanized Plaintext:	ÂlÁbdimnilÂiytÁlmi
Diagraphs:	ÂlÁb di mnilÂiytÁl mi
Romanized Ciphertext:	41G9fZa04sq4ïïGâ§j
Hex code of Romanized Ciphertext:	3431 4739 665A 6130 3473 7134 EEEF 47E2 A76A
Unicode of Romanized Ciphertext:	㐱䜹晚愰㑳焴・䟢Ꝫ

Fig. 8: GUI of modified Playfiar cipher system with unicode

Note that the alphabets was changed completely and the length of text was shrunk.

RESULTS AND DISCUSSION

The most important goal of cryptology are data protection and information confidentiality through cryptosystems. All cryptography designer attempt to achieve perfect security such that the probability or difficulty that the plaintext found by the attacker after and before the ciphertext observed is the same. In general, when designing cipher system, many features must be take into account. These features presented by Shannon to prove that the cipher system is perfect security.

In this study, we focus on analysing the randomness of the proposed cipher system (statistical characteristics, frequency test, serial test and entropy).

Statistical characteristics: Ability of the proposed system to hiding the natural properties (statistical characteristics) of a natural language. Each character in a certain natural language have its own frequency in any text that satisfies the probability law:

$$\sum_{n=z}^{a} pn = 1$$

The exterminated results of statistical characteristics for two modified Playfire cipher (without and with unicode) was explained in Fig. 9 and 10 with Arabic plaintext length 983.

Note from Fig. 9 and 10 that modified Playfire cipher with unicode system is more efficient to hide the natural feature of Arabic language than the other modification.

Frequency test: In this subsection, we will evaluate the proposed system in terms of its ability to pass the statistical tests by frequency test according to the Eq. 1:

$$x^2 = \frac{(n_0 - n_1)^2}{n} \quad (1)$$

Where: $0<x^2<3.84$

n = Length of sequence

n_0 = Number of 0's in sequence

n_1 = Number of 1's in sequence

Serial test: Serial test according to the Eq. 2:

$$x^2 = \frac{4}{n-1}\sum_{i=0}^{1}\sum_{i=0}^{1}(n_{ij})^2 - \frac{2}{n}\sum_{i=0}^{1}(n_i)^2 + 1 \quad (2)$$

$x^2 \leq 5.99$

Where:

n = Length of sequence

n_0 = Number of 0's in sequence

n_1 = Number of 1's in sequence

n_{ij} = Number of ij in sequence

The exterminated results of frequency and serial tests for two modified Playfire cipher (without and with unicode) was explained in Table 2 with Arabic plaintext length 983.

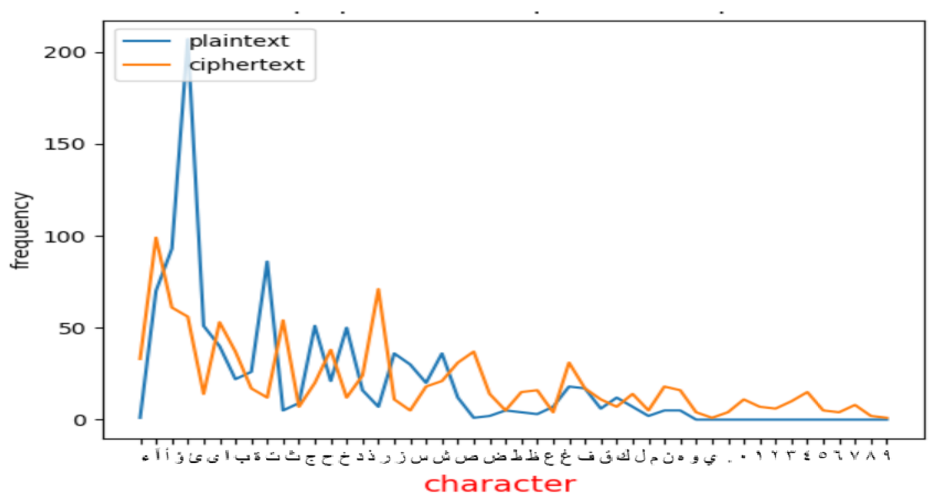

Fig. 9: Natural feature of modified playfire cipherwithout unicode

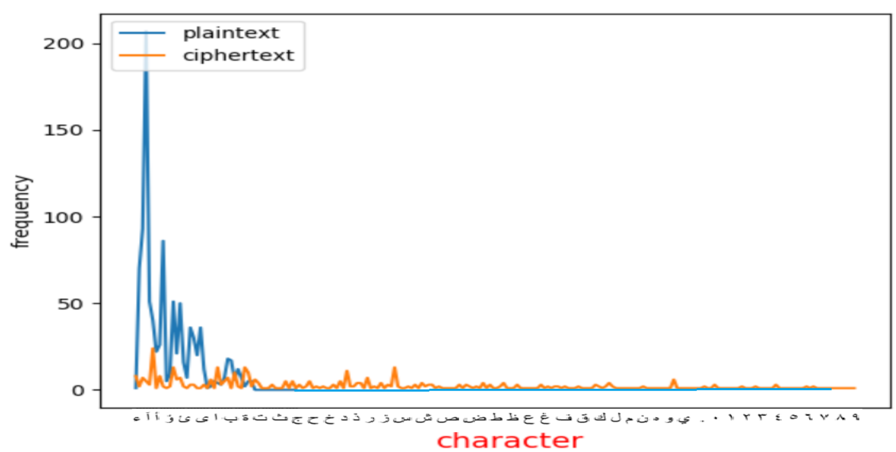

Fig. 10: Natural feature of modified playfire cipherwith unicode

Table 2: Frequency and serial tests

Modification Playfiar type/test type	Result	Status
Arabic ciphertext		
Frequency	2.433781686497672	Pass
Serial	-2002.5184353759487	Pass
Unicode ciphertext		
Frequency	65.120162932790	Not pass
Serial	-3190.90451326801	Pass

Table 3: Result of entropy

Variables	Shannon entropy	Binary Shannon entropy	Log|x|	$\text{Log}\|x\|^N$
Arabic plaintext	4.20832	0.99590	9294.3	(Very large No.)
Arabic ciphertext	5.00265	0.99988	10286.1	(Very large No.)
Unicode ciphertext	7.12215	0.99601	7134.7	(Very large No.)

Entropy: The entropy of a string provides the minimum average number of bits required to encode a random source. In information theory, entropy is the measure of uncertainty associated with a random variable. In terms of cryptography, entropy uses to determine attacker difficulties to be successful. Shannon introduced the notion of perfect security where the probability that the plaintext found by the attacker after the ciphertext observed is the same as the probability or difficulty that the plaintext found before the ciphertext observed. Perfect security used for symmetric cryptosystems and can be represented by Shannon entropy. The Shannon entropy of the message M is:

$$H(M) = -\sum_{m \in M} x\, P(m) \log P(m) \quad (3)$$

Clearly we have:

$$H(M) \leq \log|M|^N$$

The experminated results of entropy for two modified Playfire cipher (without and with unicode) was explained in Table 3 with Arabic plaintext length 983.

CONCLUSION

In this study, new method of cryptography was proposed to achieves confusion and diffusion by rominazation system and unicode. The rominazation system adapted to overcome the natural features of the Arabic language. Also, two Playfair cipher modifications ware proposed (with and without unicode). The encryption/decryption process implemented by generating Knight tour key.

Based on the experimental results, it was found that all of these modifications led the proposed system to be: robust against cryptanalysis methods, in high level of randomness, scatter the statistical characteristics of plaintext message (natural language), passing the statistical cryptanalysis, difficult to predict plaintext and key, hide the original language of plaintext and using intermediate language. Thus, the proposed system is successful within statistical analysis and applicable easily and efficiently.

REFERENCES

AL-Nasrawi, D.A., A.F. Almukhtar and W.S. AL-Baldawi, 2015. From Arabic alphabets to two dimension shapes in Kufic calligraphy style using grid board catalog. Commun. Appl. Sci., 3: 42-59.

AL-Nasrawi, D.A., H.A. Hashem and M.A. Odhaib, 2014. Unicode text editor for ancient Egyptian hieroglyphs writing system. Egypt. Comput. Sci. J., 38: 48-55.

AL-Shakarchy, N.D., H.F. AL-Shahad and D.A. AL-Nasrawi, 2018. Cryptographic system based on Unicode. IOP. Conf. Series J. Phys., 1032: 1-13.

Al-Nasrawi, D.A., H.F. Sedik and S.M. Hussain, 2016. Digital handwriting imitation of the Fourth Caliph (Imam Ali Bin Abi Taleb). Comput. Intl. J. Digital Content Technol. Appl., 10: 96-105.

Alqahtani, Y., P.P. Kuppuswamy and S. Shah, 2013. New approach of Arabic encryption/decryption technique using Vigenere chiper on mod 39. Intl. J. Adv. Res. IT. Eng., 2: 1-9.

Anonymous, 2018. Report on the current status of United Nations Romanization systems for geographical. UNGEGN Working Group on Romanization Systems, Rome. https://www.eki.ee/wgrs/rom1_ar.

Atee, H.A.Z., 2011. Development of a new way to encrypt the Arabic language letters using the symmetric encryption system. AL TAQANI, 24: 101-111.

Balajee, M., 2011. Unicode and colors integration tool for encryption and decryption. Intl. J. Comput. Sci. Eng., 3: 1197-1202.

Ganzfried, S. and P. Cull, 2004. A simple algorithm for knight's tours. Math. Oregon State Univ., 1: 63-90.

Hassan, M.M., D.A. Al-Nasrawi, R.J. Hassan and N.T. Mahdi, 2018. Rule based method of name entity recognition for matching Allah's finest names in Holy Quran. J. Eng. Appl. Sci., 13: 3618-3623.

Kumar, R., S. Chand and S. Singh, 2015. An efficient text steganography scheme using unicode space characters. Intl. J. Forensic Comput. Sci., 10: 8-14.

Kuppuswamy, P. and Y. Alqahtani, 2014. New innovation of Arabic language encryption technique using new symmetric key algorithm. Intl. J. Adv. Eng. Technol., 7: 30-37.

Mansour, A.M.A. and M.A.M. Fouad, 2017. Cryptography protocol: A novel multilingual adaptive encryption technique with phonetic based ciphering. Intl. J. Secur. Appl., 11: 13-21.

Rahma, A.M.S., W.S. Bhaya and D.A. Al-Nasrawi, 2013a. Data hiding method for English scripts using ligature characters Unicode. Eur. J. Sci. Res., 112: 452-459.

Rahma, A.M.S., W.S. Bhaya and D.A. Al-Nasrawi, 2013b. Text steganography based on unicode of characters in multilingual. Intl. J. Eng. Res. Appl., 3: 1153-1165.

Raphael, A.J. and D.V. Sundaram, 2012. Secured communication through Fibonacci numbers and Unicode symbols. Intl. J. Sci. Eng. Res., 3: 1-5.

Rihan, S.D. and S.E.F. Osma, 2016. Arabic cryptography technique using neural network and genetic algorithm. Intl. Res. J. Comput. Sci., 3: 35-42.

Shaban, S.A. and N.B. Al-Din, 2017. A new algorithm for encrypting Arabic text using the mathematical equation. Diyala J. Eng. Sci., 10: 21-30.

Stallings, W., 2005. Cryptography and Network Security: Principles and Practices. 4th Edn., Prentice Hall, New Jersey, ISBN-13: 978-0131873162.