Available online at sjuoz.uoz.edu.krd

Science Journal of University of Zakho

Vol. 11, No. 2, pp. 273– 279, April-June, 2023

journals.uoz.edu.krd

p-ISSN: 2663-628X
e-ISSN: 2663-6298

DESIGN AND IMPLEMENTATION OF A MATHEMATICAL ENCRYPTION MODEL FOR THE CENTRAL KURDISH FONT BASED ON UNICODE

Ziyad H. Abduljabbar [a*], Zeravan A. Ali [a] , Hanan A.Taher [a]

a Technical College of Administration, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq - (ziyad.hazim, zeravan.ali, hanan.taher)@dpu.edu.krd

Received: 3 Mar., 2023 / Accepted: 22 May., 2023 / Published: 4 June, 2023 https://doi.org/10.25271/sjuoz.2023.11.2.1126

ABSTRACT:

This research focuses on the development of encryption algorithms for the Kurdish language, specifically tailored to the Kurdish alphabet. With the rapid growth and digital advancements in the Kurdistan Region of Iraq, there is a pressing need for accurate encryption methods that can be applied to Kurdish texts in administration and digital governance. To address this need, a mathematical encryption model is proposed, leveraging the Kurdish central font supported by Microsoft Windows to ensure compatibility between sender and receiver. The model utilizes the Unicode representation of Kurdish letters to calculate offset and mod values accurately. The effectiveness of the proposed model is validated through its implementation using the Caesar cipher method. Computation tasks are performed using Excel, while the encryption system is designed and programmed in C#. Extensive testing of the system with diverse key values demonstrates its high accuracy, achieving a high success rate in encrypting Kurdish texts. This research contributes significantly to the field of encryption for the Kurdish language, providing a scientific framework for further advancements in this area.

KEYWORDS: Kurdish language, Unicode, Central Kurdish Font, Encryption, Decryption, Offset Value, Caesar Method.

1. INTRODUCTION

Encryption is one of the most important and powerful controls for the security of a computer system, through which text is encrypted to make it unclear and difficult for intruders to read. With the great development of web technologies at the beginning of the twenty-first century, especially in the field of e-government, computer crimes began to increase and it became necessary to continuously develop encryption algorithms for controlling and defending against breaches and to ensure complete confidentiality and security in storing and exchanging information (Pfleeger, Pfleeger, & Margulies, 2015; Stallings, 2006).

In the midst of this global development in this field, the Kurdistan Region - Iraq experienced a great development in the use of electronic government, which now has a major role in communicating with citizens. This will increase the level of electronic transactions over the net, which should be sufficiently protected (Shareef & Arreymbi, 2013). In addition, the field of information technology has greatly developed in the universities of the Kurdistan Region - Iraq in recent years, and the information security course is now essential in many colleges and institutes. It is, however, preferred to use the Kurdish language along with the standard English language in the practical aspect of information security experiences.

The search included, a study reviewing of the relevant literature, and also an overview about the encryption algorithm for English letter with their ASCII, offset and index values. Then the Introduction to the Standard Coding System Development was presented, and then the research touched on the central Kurdish font as a standard Kurdish font, since the research relied on it to ensure the accuracy of the encryption. Then the research included a full explanation about the steps required to design the mathematical encryption model and how to calculate the offset and mod values for Kurdish letters, with number of tables that show a detail of the mathematical steps and results as well as the figures for the steps required.

The mod function ensures that the letters are wrapped when they are encrypted, and its remain within the same frame limits for the specific language.

Offset represents the displacement of the letter to be encrypted and its value can either a direct value or as a result of encryption equation.

The main contributions of this research are as follows:

Development of a mathematical encryption model for the Kurdish language, enabling accurate encryption and decryption processes.

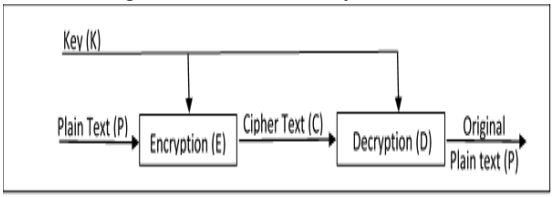
Utilization of the Kurdish central font, supported by the Microsoft Windows operating system, to ensure compatibility and accuracy in encryption.

Calculation of offset and mod values specific to the Kurdish alphabet, ensuring integrity and security in encryption.

Implementation of the proposed model using the Caesar cipher method, providing a practical application of the encryption system.

The rest of the paper is organized as follows: Section 2 provides an overview of the mathematical encryption model, including the calculation of offset and mod values. Section 3 presents the implementation of the proposed model using the Caesar cipher method. Section 4 describes the extensive testing conducted to evaluate the accuracy of the encryption system. Section 5 discusses the results and their implications. Finally, Section 6 concludes the paper by summarizing the contributions and outlining potential areas for future research.

Figure 1. General view for system



2. RELATED WORKS

There are stingy studies to precisely focusing encryption systems especially those who related directly to encryption Kurdish texts. (Kako, 2018) proposed a related work covering digital security and its role in protecting information privacy were evaluated. The researcher used several encryption algorithms have been evaluated and the significant role of Unicode in communication and its security has been demonstrated. (Alkhudaydi & Gutub,

* Corresponding author

2021) introduce and suggest an effective system for hiding the Arabic text based on two algorithms, namely: light-weight cryptography (LWC) and Arabic text steganography.(Shareef & Arreymbi, 2013) implied two modifications to the Playfair cipher algorithm, the first by using the Unicode and the second without using the Unicode, adopting on the Romanization system, that ensures the removal of the natural characteristics of the Arabic language using the Knight Tour key. (Tawfiq, 2018) imported an enhanced LSB substitution algorithm for masking Kurdish text content written in a text file into digital picture, while (Maram, Gnanasekar, Manogaran, Balaanand, & Applications, 2019) concentrated on emphasizing the importance of Unicode as playing an important role in digital communication, as it covers about 120 languages in the world and relying on it in developing UNICODE data privacy and security encryption algorithms (UDPS) to ensure data security in digital communication. Although (AL-Shakarchy, AL-Shahad, & AL-Nasrawi, 2018) offered an encryption method that provides sufficient confidentiality depending on the Unicode and crossover, by mapping table for English alphabet used in plaintext and mapping table for Arabic alphabet used in key generation. At the same time (Kako, 2018) tried to develop an algorithm to encrypt and decrypt Kurdish letters using the decimal value of the letters to ensure the security of Kurdish communications. Whereas (Khairullah & Ratul, 2018) develop an algorithm to encrypt and decrypt Kurdish letters using the decimal value of the letters to ensure the security of Kurdish communications. However, (Ahmed, Ahmed, Ahmed, & Science, 2015) planned to hide the information written in Bengali language and stored in digital documents by adopting the Unicode, but (AL-Nasrawi, Hashem, & Odhaib, 2014) focused on development of Playfair encryption algorithm to support the Kurdish text by using an array of size in order to increase security during the messaging process through an unreliable network in privacy and authentication. (Rashid, 2020) Used RSA encryption algorithm to develops an encryption system for Kurdish and English text as well. Furthermore, (Shirali-Shahreza & Shirali-Shahreza, 2008) utilized an approach Hide the Arabic and Persian text depending on the Unicode to ensure confidential communication and prevent illegal copying and distribution of the text.

The main contribution of this work, to the problem of encryption Kurdish text is by suggesting a mathematical encryption model in order to enable substitution encryption algorithms to become applicable with the Kurdish alphabet, and after that the influence of our approach was definitely accurate as a sequence recognized the existing limitation of encryption regarding Kurdish alphabet.

3. ENCRYPTION ALGORITHM OVERVIEW

Encryption system is the system concerned with encryption and decrypting text. The general encryption system can be denoted by the following general equations:

C=E(P); … (1) Encryption Algorithm.

P=D(C); … (2) Decryption Algorithm.

Where:

P = [P1, P2, …., Pn]; (3) String of plain text.

C = [C1, C2, …., Cn]; … (4) String of cipher text.

Most of substitution encryption methods, like Caesar, Vigenere, Affine, and Hill algorithm, rely on modular mathematical operations, (mod n), where (n) is the number of letters in specific language, that means the calculations are done in a circular motion, i.e. if the result is greater than (n), the result will reduce and warps turn around. For example, in English language, which consist of (26) letters, here the values of (n) are equal to (26), so that Z+2=B. Thus, all results of mod operation in English language will be between (0-25). Before implementing the(mod) function and starting with any of the above-mentioned encryption methods, it is important to obtain pure index values for English letters and make them into a sequence (0-25), and this is done by subtracting the ASCII code value for the first letter, that referred to as the offset value, from the ASCII code value for all letters. In English, the ASCII codes (65='A') and (97='a') are represent the offset values for uppercase and lowercase letters respectively, table 1.

As it shown in table 1 below, where the following two equations are applied for each of the uppercase and lowercase letters:

1- Index (any capital letter) = ASCII code (that capital letter)-65.

2- Index (any small letter) = ASCII code (that small letter)- 97.

Through this research, a mathematical encryption model will be proposed to calculate the offset and mod values for the Kurdish language based on central Kurdish font, in order to rely on them in applying encryption methods on the Kurdish text (Ghauri, 2021; Hawezi, Azeez, & Qadir, 2019; Kareem, 2016).

Table 1. Standard English letters with their ASCII code and index

index	letter	ASCII code	letter	ASCII code
0	A	65	a	97
1	B	66	b	98
2	C	67	c	99
…	…	…	…	…
23	X	88	x	120
24	Y	89	y	121
25	Z	90	z	122

4. STANDARD CODING SYSTEM DEVELOPMENT

Due to the importance of coding system as it is the basis in the coding process, at the beginning in this research was to conduct an exploratory survey study on coding system, its types and stages of development, and what is the type currently adopted in to encode the Kurdish letters. ASCII code was developed in 1960, which was the basis for the representation of symbols in the computer memory, as it can be represent 128 symbols (0..127) depending on (7 bits), and since the ASCII system is able to represent only English letters, and in order to double the number of character that can be encoded, so the ASCII system was developed by IBM Corporation in 1981 to become an extended ASCII code by adding one bit to become (8 bits), so the number of symbols that can be represented become (255) characters. But this was not enough to represent the many other languages of the world, like Japanese, Arabic, Kurdish, etc., so Unicode system was developed in 1990, which is compatible with the (ASCII) system, and consists of (23 bits), where it became possible to represent (2147483647) characters, Thus, now, it became possible to represent the letters of all the languages of the world, including the Kurdish language, which needs 24 bits to represent its letters. But with all this benefit from the Unicode system, another problem arose, which is represented by the large reservation of memory, i.e. for example, the letter (A) which was represented by (1 byte) in the ASCII code system, now needs (4 bytes) with the Unicode system and this is what caused a great waste in memory, and in order to solve this problem, UTF-8 was invented by Ken Thompson on September 2, 1992, which is an improved version of the Unicode by which guarantees allocate memory (reservation) exactly to a matching class boundary for the language to which the character belongs, and according to that, UTF-8 will assign the exact number of bits for any character (Aleqabie, Al-Nasrawi, Al-Shakarchy, Alshahad, & Abd, 2019; Korpela, 2006; Miltner & Society, 2021; Pyeatt, 2016).

5. CENTRAL KURDISH FONT

In fact, there are many types of fonts currently using in the computer system to write the Kurdish letters , and it is better to choose the appropriate font type that provides compatibility

between the sender and the receiver, as well as to provide a standard encryption environment, and accordingly, the research preferred to use the central Kurdish font that provided by Microsoft Windows , so the first step of practical part will be represent with install this keyboard, so after completing this

process, the central Kurdish font will be added and appear among the language options available on the taskbar (AL-Nasrawi et al., 2014; Korpela, 2006; Ramanathan, 2022), Figure 2.

Figure 2. Adding Central Kurdish font

6. DESIGN A MATHEMATICAL ENCRYPTION MODEL FOR KURDISH LETTERS

The alphabet of the Kurdish language consists of 33 letters, table 2.

Table 2. Kurdish Alphabet

خ	ح	چ	ج	ت	پ	ب	ا
ع	ش	س	ز	ژ	ڕ	ر	د
ڵ	ل	ڤ	ك	ق	گ	ف	غ
ی (ێ)	وو	ۆ	و	ه	هـ	ن	م

The Unicode value of Kurdish letter in Central Kurdish font are not contiguous as is the case in the English language, but interspersed with some letters and movement symbols of the Arabic language, for this reason, the mathematical analysis in this research was based on the actual position of the Kurdish letter on keyboard, as shown in "Fig. 3" and Table 3. As it is known, the Kurdish letters, like letter of other languages, are centred on the second, third and fourth line of the keyboard. Accordingly, "Fig. 4" shows the steps required for the proposed mathematical encryption model for Kurdish letters, through this model, the limits of the Unicode values were determined, where the Kurdish language letters are located within this segment that was determined by the two output values calculated by this model, these were represented by:

1. The offset value = 1569: which represents the minimum Unicode value for the central Kurdish font, therefore, the Index (any Kurdish letter) = Unicode (that letter) - 1569.
2. The Mod value = 181: which will be relied upon in the mathematical equations of the encryption algorithms to ensure obtaining the value of Unicode within the limits of the Kurdish language, i.e. the limits where the Kurdish letters are ranging with (0-180).

Table 4 shows the segment of the Unicode values (0 - 180), which included the letters of the Kurdish language were determined through the proposed model. "Fig. 5" represents the pseudo code for building the mathematical encryption model of the Kurdish language.

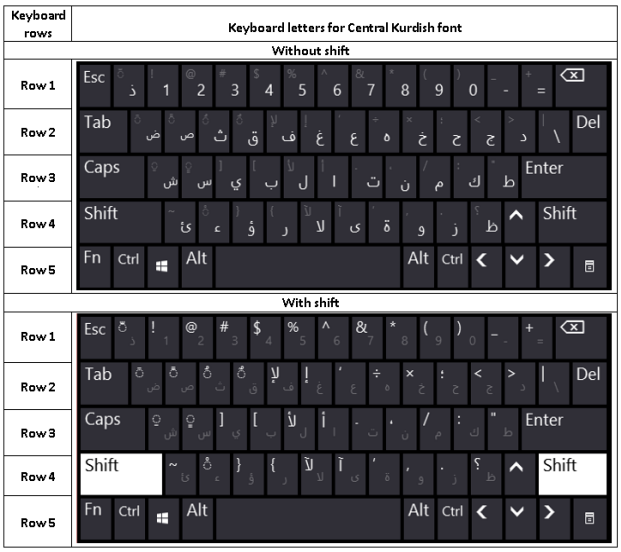


Figure 3. Keyboard letters for the Central Kurdish font.

Table 3. Calculate the offset and mod values

Keyboard rows	Unicode corresponding to the keyboard letters of the central Kurdish script											
Without shift											Min1	Max1
Row 2	letter	ق	و	ه	ر	ت	ی	ێ	ح	ۆ	پ	
	Unicode	1602	1608	1749	1585	1578	1740	1574	1581	1734	1662	1574	1749
Row 3	letter	ا	س	د	ف	گ	ه	ژ	ک	ل			
	Unicode	1575	1587	1583	1601	1711	1607	1688	1705	1604		1575	1711
Row 4	letter	ز	خ	ج	ڤ	ب	ن	م					
	Unicode	1586	1582	1580	1700	1576	1606	1605				1576	1700
												1574	1749

With shift											Min2	Max2
Row 2	letter	وو	ي	ر	ط	ێ	ء	ع	ۆ	ث		
	Unicode	1608	1610	1685	1591	1742	1569	1593	1572	1579		1569	1742
Row 3	letter	أ	ش	ذ	إ	غ	©	أ	ك	ل			
	Unicode	1570	1588	1584	1573	1594		1571	1603	1717		1570	1717
Row 4	letter	ض	ص	چ	ظ	ی	ة	-					
	Unicode	1590	1589	1670	1592	1609	1577	1600				1577	1670
												1569	1742

Maximum(Max1,Max2) = 1749 (ه)	Minimum(Min1,Min2) = 1569 (ء)
Mod value = Range+1 = 181	Offset= Minimum= 1569 (ء)

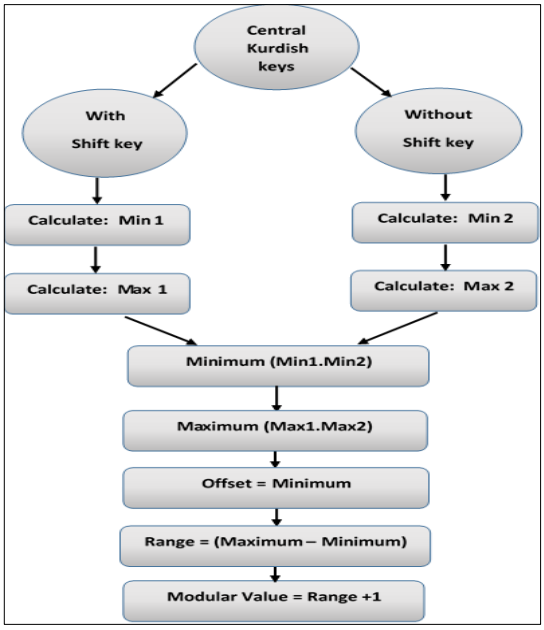


Figure 4. Steps required for the proposed mathematical encryption model for the Kurdish letters

```
For writing (Any Kyrdish_Message)
{
    If (Font(Central_kurdish). Select=True)
    {
        If(key(letter). Pressed = True)
        {
            If(Key(shift). Pressed != true)
            {
                Min1= Min(Unicode(letters)). Select;
                Max1= Max(Unicode(letters)). Select;
            }
            Else
            {
                Min2= Min(Unicode(letters)). Select;
                Max2= Max(Unicode(letters)). Select;
            }
        }
        Minimum= Min (Min1, Min2);
        Maximum= Max (Max1, Max2);
        Offset = Minimum;
        Range= Maximum- Minimum
        Modular_Value= Range+1;
    }
}
```

Figure 5. Pseudo code for calculating the offset and mode values

7. IMPLEMENTATION OF THE PROPOSED MATHEMATICAL MODEL TO ENCRYPT A KURDISH TEXT

After completing the design of the proposed mathematical encryption model, now comes the time to implement and test it. The accuracy of encryption and decryption was verified by applying this model using the Caesar cipher method. Where the values of offset and mod that were produced by the proposed mathematical model were used (Maghrebi, Portigliatti, & Prouff, 2016). The general equations for encryption and decryption of any Kurdish letter based on the proposed mathematical encryption model as shown in the following equations:

CKL=E(PKL) = ((Unicode (PKL)-1569) +key) mod 181; …….(1) Encryption Algorithm

PKL=D(CKL)= ((Unicode (CKL)-1569) - key) mod 181; ……(2) Decryption Algorithm

Where:

CKL= Ciphered Kurdish letter.

PKL= Plain Kurdish Letter.

Key: Any numeric value.

The value (1569), represents the minimum Unicode value for all the characters in the Central Kurdish keyboard.

The value (181), Represents the actual number of all characters in the segment that are located together with the Kurdish letters in the Central Kurdish keyboard.

The steps required for encryption and decryption can be illustrated in the two flowcharts shown in Figure 6 and Figure 7 respectively.

Table 4. The boundaries of the Unicode values (0 - 180), which included the letters of the Kurdish language were determined through the proposed model.

index	Unicode	Character	index	Unicode	Character	index	Unicode	Character	index	Unicode	Character
0	1569	ء	45	1614	ٮ	90	1659	ٻ	135	1704	ۇ
1	1570	آ	46	1615	ٯ	91	1660	ټ	136	1705	ۈ
2	1571	أ	47	1616	ٰ	92	1661	ٽ	137	1706	ۉ
3	1572	ؤ	48	1617	ٱ	93	1662	پ	138	1707	ۊ
4	1573	إ	49	1618	ٲ	94	1663	ٿ	139	1708	ۋ
5	1574	ئ	50	1619	ٳ	95	1664	ٹ	140	1709	ی
6	1575	ا	51	1620	ٴ	96	1665	ٺ	141	1710	ۍ
7	1576	ب	52	1621	ٵ	97	1666	٦	142	1711	ێ
8	1577	ة	53	1622	ٶ	98	1667	٧	143	1712	ۏ
9	1578	ت	54	1623	ٷ	99	1668	٨	144	1713	ې
10	1579	ث	55	1624	ٸ	100	1669	٩	145	1714	ۑ
11	1580	ج	56	1625	ٹ	101	1670	٪	146	1715	ے
12	1581	ح	57	1626	ٺ	102	1671	٫	147	1716	ۓ
13	1582	خ	58	1627	ٻ	103	1672	٬	148	1717	ە
14	1583	د	59	1628	ټ	104	1673	٭	149	1718	ۖ
15	1584	ذ	60	1629	ٽ	105	1674	ٮ	150	1719	ۗ
16	1585	ر	61	1630	ٿ	106	1675	ٯ	151	1720	ۘ
17	1586	ز	62	1631	ٿ	107	1676	ٰ	152	1721	ۙ
18	1587	س	63	1632	٠	108	1677	ٱ	153	1722	ۚ
19	1588	ش	64	1633	١	109	1678	ٲ	154	1723	ۛ
20	1589	ص	65	1634	٢	110	1679	ٳ	155	1724	ۜ
21	1590	ض	66	1635	٣	111	1680	ٴ	156	1725	۝
22	1591	ط	67	1636	٤	112	1681	ٵ	157	1726	۞
23	1592	ظ	68	1637	٥	113	1682	ٶ	158	1727	۟
24	1593	ع	69	1638	٦	114	1683	ٷ	159	1728	۠
25	1594	غ	70	1639	٧	115	1684	ٸ	160	1729	ۡ
26	1595	ـ	71	1640	٨	116	1685	ٹ	161	1730	ۢ
27	1596	ف	72	1641	٩	117	1686	ٺ	162	1731	ۣ
28	1597	ق	73	1642	٪	118	1687	ٻ	163	1732	ۤ
29	1598	ك	74	1643	٫	119	1688	ټ	164	1733	ۥ
30	1599	ل	75	1644	٬	120	1689	ٽ	165	1734	ۦ
31	1600	ـ	76	1645	٭	121	1690	ٿ	166	1735	ۧ
32	1601	ف	77	1646	ٮ	122	1691	ٿ	167	1736	ۨ
33	1602	ق	78	1647	ٯ	123	1692	ٹ	168	1737	۩
34	1603	ك	79	1648	ٰ	124	1693	ٺ	169	1738	۪
35	1604	ل	80	1649	ٱ	125	1694	ٻ	170	1739	۫
36	1605	م	81	1650	ٲ	126	1695	ټ	171	1740	۬
37	1606	ن	82	1651	ٳ	127	1696	ٽ	172	1741	ۭ
38	1607	ه	83	1652	ٴ	128	1697	ٿ	173	1742	ۮ
39	1608	و	84	1653	ٵ	129	1698	ٹ	174	1743	ۯ
40	1609	ى	85	1654	ٶ	130	1699	ٺ	175	1744	۰
41	1610	ي	86	1655	ٷ	131	1700	ٻ	176	1745	۱
42	1611	ً	87	1656	ٸ	132	1701	ټ	177	1746	۲
43	1612	ٌ	88	1657	ٹ	133	1702	ٽ	178	1747	۳
44	1613	ٍ	89	1658	ٺ	134	1703	ٿ	179	1748	۴
									180	1749	۵

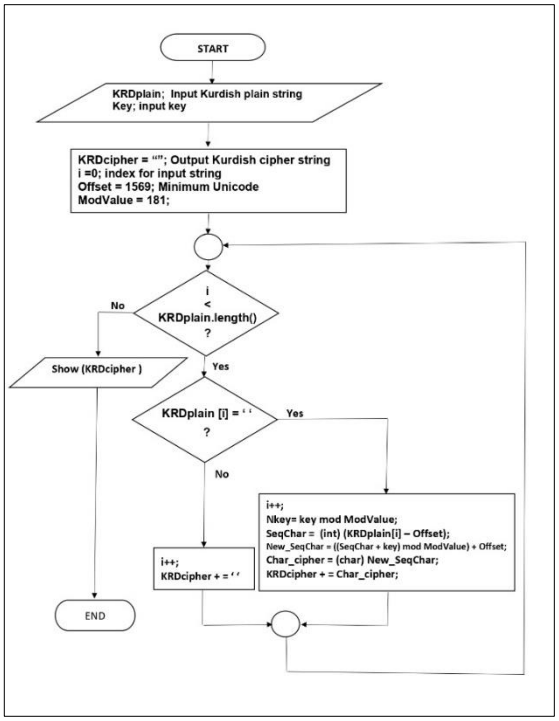


Figure 6. Steps for the Encryption Process

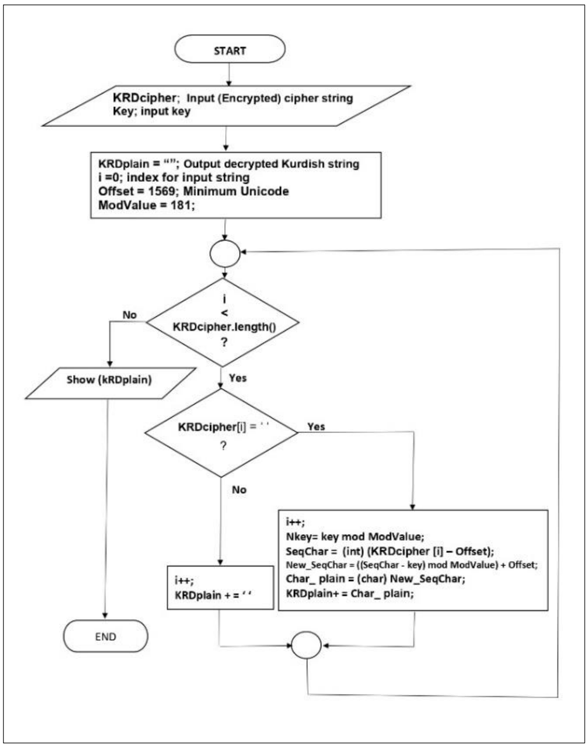


Figure 7. Steps for the Decryption Process

Table 5. Required calculation for proposed mathematical encryption model

Encryption $C_i = E(Pi)$						
P = "ئەز خو فێری زمانێ کوردی دکەم"						
Offset= 1569				Mod Value = 181		
Key = 120				$\overline{key}$ = Mod (120,181)		
Col#1	Col#2	Col#3	Col#4	Col#5	Col#6	Col#7
Ch#	Pi	$\overline{P}_i$=UNICODE(Pi)	$\overline{\overline{P}}_i = \overline{P}_i - 1569$	$\overline{\overline{C}}_i = mod((\overline{\overline{P}}_i + \overline{key}),181)$	$\overline{C}_i = \overline{\overline{C}}_i + 1569$	C_i =UNICHAR($\overline{C}_i$)
1	ئ	1574	5	125	1694	ڞ
2	ە	1749	180	119	1688	ژ
3	ز	1586	17	137	1706	ڪ
4	خ	1582	13	133	1702	ڦ
5	و	1608	39	159	1728	ۀ
6	ف	1601	32	152	1721	ڹ
7	ێ	1742	173	112	1681	ڑ
8	ر	1585	16	136	1705	ک
9	ی	1740	171	110	1679	ڏ
10	ز	1586	17	137	1706	ڪ
11	م	1605	36	156	1725	ڽ
12	ا	1575	6	126	1695	ڟ
13	ن	1606	37	157	1726	ھ
14	ێ	1742	173	112	1681	ڑ
15	ک	1705	136	75	1644	٬
16	و	1608	39	159	1728	ۀ
17	ر	1585	16	136	1705	ک
18	د	1583	14	134	1703	ڧ
19	ی	1740	171	110	1679	ڏ
20	د	1583	14	134	1703	ڧ
21	ک	1705	136	75	1644	٬
22	ە	1749	180	119	1688	ژ
23	م	1605	36	156	1725	ڽ
Result of encryption C = ڞژڪڦۀڹڑکڏڪڽڟھڑ٬ۀکڧڏڧ٬ژڽ						

Table 6. Required calculation for proposed mathematical encryption mode

Decryption $P_i = D(C_i)$						
C = ڞژڪڦۀڹڑکڏڪڽڟھڑ٬ۀکڧڏڧ٬ژڽ						
Offset= 1569				Mod Value= 181		
Key = 120				$\overline{key}$ = Mod (120,181)		
Col#1	Col#2	Col#3	Col#4	Col#5	Col#6	Col#7
ch#	C_i	$\overline{C}_i$ =Unicode(C_i)	$\overline{\overline{C}}_i = \overline{C}_i - 1569$	$\overline{\overline{P}}_i = Mod(\overline{\overline{C}}_i - \overline{key}),181)$	$\overline{P}_i = \overline{\overline{P}}_i + 1569$	P_i =UNICHAR($\overline{P}_i$)
1	ڞ	1694	125	5	1574	ئ
2	ژ	1688	119	180	1749	ە
3	ڪ	1706	137	17	1586	ز
4	ڦ	1702	133	13	1582	خ
5	ۀ	1728	159	39	1608	و
6	ڹ	1721	152	32	1601	ف
7	ڑ	1681	112	173	1742	ێ
8	ک	1705	136	16	1585	ر
9	ڏ	1679	110	171	1740	ی
10	ڪ	1706	137	17	1586	ز
11	ڽ	1725	156	36	1605	م
12	ڟ	1695	126	6	1575	ا
13	ھ	1726	157	37	1606	ن
14	ڑ	1681	112	173	1742	ێ
15	٬	1644	75	136	1705	ک
16	ۀ	1728	159	39	1608	و
17	ک	1705	136	16	1585	ر
18	ڧ	1703	134	14	1583	د
19	ڏ	1679	110	171	1740	ی
20	ڧ	1703	134	14	1583	د
21	٬	1644	75	136	1705	ک
22	ژ	1688	119	180	1749	ە
23	ڽ	1725	156	36	1605	م
Result of Decryption P = ئەز خو فێری زمانێ کوردی دکەم						

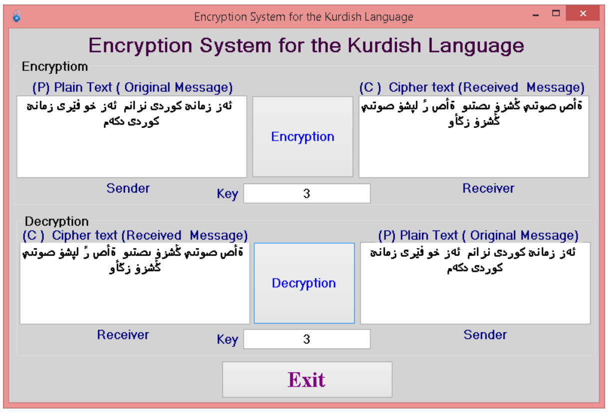


Figure 8. Encrypt and Decrypt Kurdish text with primary key value =3

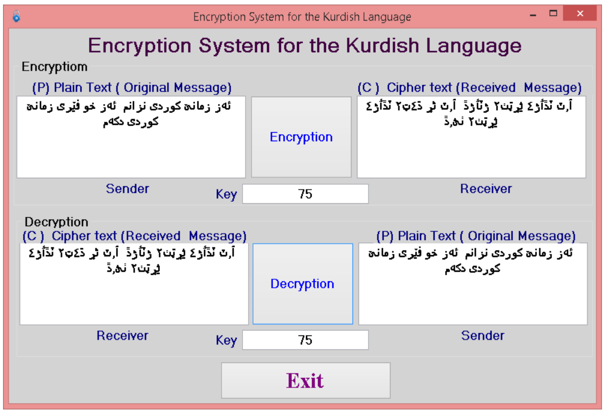


Figure 9. Encrypt and Decrypt Kurdish text with primary key value= 75

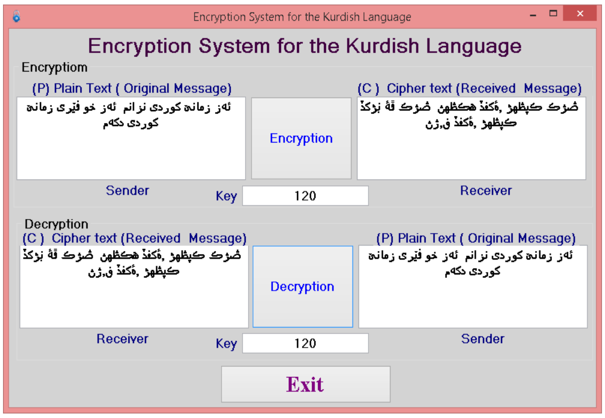


Figure 10. Encrypt and Decrypt Kurdish text with primary key value=120

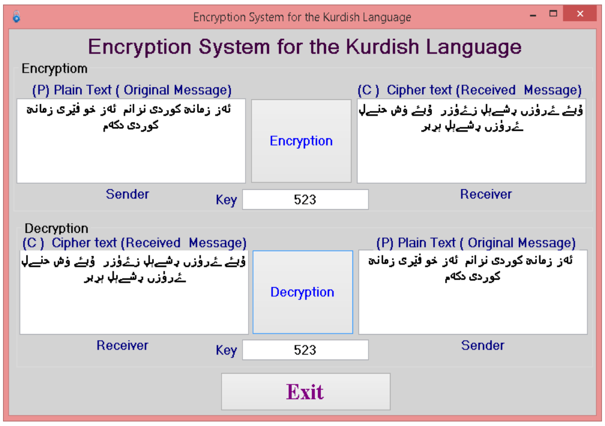


Figure 11. Encrypt and Decrypt Kurdish text with primary key value=523

8. RESULTS AND DISCUSSIONS

The Excel program was used to perform the required calculations for the mathematical encryption model to calculate the offset and the mod values. The above two tables 5 and 6, represented the encryption and decryption steps respectively. Both of these tables had the same number of columns, due to the similarity of the arithmetic operations in both steps. The only difference is in the fifth column, where the encryption process represents the adding of the key value, whereas the decryption process is representing the subtracting of the key value (Rajasekharaiah, Dule, & Sudarshan, 2020; Thakur, Qiu, Gai, & Ali, 2015). These two tables were divided into two main parts:

Part one:

This part includes the columns from (col#1) to (col#4), whose role is to receive the letter from the Kurdish text and convert it into an index number ranging from (0-180), that can be illustrated as follows:

1- Column (col#1): the letter sequence within the Kurdish text.
2- Column (col#2): the relevant letter within the Kurdish text.
3 - Column (col#3): conversion of the Kurdish character into its corresponding Unicode value.
4 - Column(col#4): subtracts the offset value (1569) from the Unicode value into values ranging between (0-180).

Part two:

This part includes the columns from (col#5) to (col#7). These columns complete the encryption (or decryption) process and return the Unicode to the corresponding letter. This can be illustrated as follows:

1- Column (col#5): adding (or subtracting) the value of the key, and then apply the mod operation by (181) to ensure that the Unicode values wrap between (0-180) after the calculation.
2 - Column (col#6): adding the subtracted offset value (1569) to get the actual Unicode value.
3 - Column (col#7): converts the Unicode value to its corresponding letter.

C# programming language was used to design and code the encryption system. The interface of the encryption system, where the Kurdish sentence was (ئەز زمانێ کوردی نزانم ئەز خو فێری زمانێ کوردی دکەم), and the key values were (3,75,120 and 523) is shown in the figures: “Fig. 8”, “Fig. 9”, “Fig. 10” and “Fig. 11” respectively.

From the above results tables: 5 and 6, and the figures: “Fig. 8”, “Fig. 9”, “Fig. 10” and “Fig. 11”, it can be concluded that by using the Unicode value for the actual location of the Kurdish letter on the keyboard, the mathematical encryption operations will not require the Kurdish letters to be sequential.

2- The number of characters, that was equal to (181) does not reflect the actual number of Kurdish letters, as they are actually mixed with Arabic letters and a number of other characters.

3- With the use of different values of the primary key (large or small), the encryption process had the same high efficiency.

8. CONCLUSION

The encryption system for the Kurdish language was designed and programmed based on the mathematical encryption model that is proposed by this research. The central Kurdish font was used to ensure compatibility between the sender and receiver and to obtain high encryption accuracy. The Unicode for Kurdish letters was relied on during the calculations for the mathematical encryption model, and it was used to calculate the offset and mod values. To verify the accuracy of this model, it was implemented using the Caesar cipher method. The encryption system was tested by encrypting several Kurdish texts using different key values. The results showed a striking high accuracy.

9. RECOMMENDATION

The research recommends the necessary development of the mathematical model in order to encode the Kurdish texts mixed with the English texts. In addition to that, adopting the results of the proposed mathematical model and applying them to other encryption algorithms.

10. ACKNOWLEDGEMENTS

Full thanks expressed to Duhok Polytechnic University (DPU). We would like to express our gratitude to head of ITM department, Dr.Amira Bibo Sallow for her guidance and support.

11. COMPETING INTERESTS

Authors have declared that no competing interests exist.

12. FUNDING

We would like to clarify that there was no external funding received for this research project. The manuscript was completed without any financial support or grants. We would like to acknowledge that this study was conducted independently and self-funded.

REFERENCES

Ahmed, O. H., Ahmed, A. M., Ahmed, S. H. J. I. J. o. E., & Science, C. (2015). Improving playfair algorithm to support user verification and all the languages in the world including kurdish language. 4(8), 14058-14062.

AL-Nasrawi, D. A., Hashem, H. A., & Odhaib, M. A. J. E. C. S. J. (2014). Unicode text editor for ancient Egyptian hieroglyphs writing system. 38(2), 48-55.

AL-Shakarchy, N. D., AL-Shahad, H. F., & AL-Nasrawi, D. A. (2018). Cryptographic system based on Unicode. Paper presented at the Journal of Physics: Conference Series.

Aleqabie, H. J., Al-Nasrawi, D., Al-Shakarchy, N., Alshahad, H., & Abd, E. (2019). New Cryptographic System of Romanized Arabic Text Based on Modified Playfiar. Journal of Engineering and Applied Sciences, 14. doi:10.36478/jeasci.2019.1331.1338

Alkhudaydi, M., & Gutub, A. J. S. C. S. (2021). Securing data via cryptography and Arabic text steganography. 2, 1-18.

Ghauri, F. (2021). DIGITAL SECURITY VERSUS PRIVATE INFORMATION.

Hawezi, R. S., Azeez, M. Y., & Qadir, A. A. (2019). Spell checking algorithm for agglutinative languages “Central Kurdish as an example”. Paper presented at the 2019 International Engineering Conference (IEC).

Kako, N. A. (2018). Classical Cryptography for Kurdish Language. Paper presented at the 4th International Engineering Conference on Developments in Civil & Computer Engineering Applications (IEC2018).

Kareem, R. A. (2016). The syntax of verbal inflection in Central Kurdish. Newcastle University,

Khairullah, M., & Ratul, M. (2018). Steganography in Bengali Unicode Text. 27.

Korpela, J. K. (2006). Unicode explained: " O'Reilly Media, Inc.".

Maghrebi, H., Portigliatti, T., & Prouff, E. (2016). Breaking cryptographic implementations using deep learning techniques. Paper presented at the Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings 6.

Maram, B., Gnanasekar, J., Manogaran, G., Balaanand, M. J. S. O. C., & Applications. (2019). Intelligent security algorithm for UNICODE data privacy and security in IOT. 13, 3-15.

Miltner, K. M. J. N. M., & Society. (2021). “One part politics, one part technology, one part history”: Racial representation in the Unicode 7.0 emoji set. 23(3), 515-534.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing: Pearson Education.

Pyeatt, L. (2016). Modern assembly language programming with the ARM processor: Newnes.

Rajasekharaiah, K., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. Paper presented at the IOP Conference Series: Materials Science and Engineering.

Ramanathan, A. J. J. o. O. S. S. (2022). Unishox: A hybrid encoder for short unicode strings. 7(69), 3919.

Rashid, F. J. A. a. S. (2020). Design and implementation a new approach for enhancing encryption and decryption mechanisms.

Shareef, S., & Arreymbi, J. (2013). E-Government Initiatives in Kurdistan Region of Iraq: A Citizen-Centric Approach. In (pp. 1-33).

Shirali-Shahreza, M., & Shirali-Shahreza, S. (2008, 8-10 Sept. 2008). Persian/Arabic Unicode Text Steganography. Paper presented at the 2008 The Fourth International Conference on Information Assurance and Security.

Stallings, W. (2006). Cryptography and Network Security: Principles and Practice: Pearson/Prentice Hall.

Tawfiq, N. E. J. A. J. o. N. U. (2018). Modified Lsb For Hiding Encrypted Kurdish Text Into Digital Image. 7(4), 254-260.

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. Paper presented at the 2015 IEEE 2nd international conference on cyber security and cloud computing.