ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER

Md. Khalid Imam Rahmani[1], Neeta Wadhwa[1] and Vaibhav Malhotra[1]

[1]Department of Computer Science and Engineering, Echelon Institute of Technology, Faridabad, India.
kirahmani@rediffmail.com
neeta.088@gmail.com
vaibhav0223@gmail.com

ABSTRACT

The Vigenère Cipher is a traditional method which involves encrypting alphabetic text by using a series of different Caesar Ciphers based on the letters of a keyword. The Vigenère Cipher works on the set of 26 English alphabets. In this paper we introduce the Alpha-Qwerty Cipher and reverse Alpha-Qwerty Ciphers which are the extensions to the Vigenère Cipher. This cipher works on a set of 92 characters by introducing case sensitivity and by adding digits and some other symbols to the existing Vigenère Cipher which is of 26 characters. This paper also modifies the mapping sequence from the plain text to the cipher text.

KEYWORDS

Cryptography, Alpha-Qwerty cipher, Vigenère cipher, Polyaplhabetic ciphers

1. INTRODUCTION

Cryptography is defined as the art and science of generating secret messages. An original plaintext is coded into the cipher text through the process of enciphering or encryption and plaintext is restored from the cipher text through deciphering or decryption. The many schemes used for encryption constitute the area of study known as cryptography. Cryptanalysis is "breaking the code" without knowledge of the encryption technique. The areas of cryptography and cryptanalysis together are called cryptology [1, 2].

There are basically 4 objectives of cryptography described in [3].

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

2. THE VIGENÈRE CIPHER

The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values. In Caeser cipher each letter is shifted along some places. For example for a shift of 5 A will become f, b will map to g and so on. The Vigenère cipher uses sequence of different shift values and uses a table called tabula recta, Vigenère square, or Vigenère table. The table is a 26 * 26

DOI : 10.5121/acij.2012.3311

matrix in which the English alphabets are written 26 times in different rows representing the different possible shifts. The table is used and substitution is made according to the varying shift values derived from the key [4, 5].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
W	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure1. The Vigenère table [6, 7].

2.1 Algebraic description of Vigenère Cipher

Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25 then Vigenère encryption E using the key K can be written as:

Ci = EK(Pi) = (Pi + Ki) mod26

and decryption D using the key K,

Pi = DK(Ci) = (Ci - Ki) mod26

where

P = P0…Pn is the message,

C = C0….Cn is the ciphertext and

K= K0.....Km is the used key.

2.2 Cryptanalysis of Vigenère Cipher

The Vigenère cipher masks the characteristic letter frequencies of English plaintexts, but some patterns remain For instance, if P is the most frequent letter in a cipher text whose plaintext is in English, one might suspect that P corresponds to E, because E is the most frequently used letter

in English. However, using the Vigenère cipher, E can be enciphered as different ciphertext letters at different points in the message, thus defeating simple frequency analysis.

The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length, then the cipher text can be treated as interwoven Caesar ciphers, which individually are easily broken. The Kasiski and Friedman tests can help determine the key length [8, 9].

The Kasiski examination, also called the Kasiski test, takes advantage of the fact that repeated words may, by chance, sometimes be encrypted using the same key letters, leading to repeated groups in the cipher text.

Frequency analysis: If the length of the key is known or guessed, the ciphertext can be rewritten into that many columns. Each column consists of plaintext that has been encrypted by a single Caesar cipher. Using methods similar to those used to break the Caesar cipher, the letters in the cipher text can be discovered [10, 11].

An improvement to the Kasiski examination, known as Kerckhoffs' method, matches each column's letter frequencies to shifted plaintext frequencies to discover the key letter (Caesar shift) for that column. Once every letter in the key is known, the cryptanalyst can simply decrypt the cipher text and reveal the plaintext. Kerckhoffs' method is not applicable when the Vigenère table has been scrambled.

3. THE ALPHA-QWERTY CIPHER

The alpha-qwerty cipher intends to extend the original 26 character Vigenère cipher to a 92 characters case sensitive cipher including digits and some other symbols commonly used in the English language and can be written from a computer keyboard. The alpha-qwerty cipher also changes the mapping sequence used in the Vigenère cipher. The mapping takes from a extended alphabet sequence to extended qwerty keyboard sequence. To decrypt the code reverse mapping takes place (compliment of encryption) that is from extended QWERTY keyboard to extended alphabet sequence. In short this proposed version extends and rearranges the original Vigenère table, therefore making it much more complex than the existing one.

The greater character set allows more type of messages to be encrypted like passwords. It also increases the key domain and hence provides more security.

3.1 Character set

The character set of the Alpha-Qwerty Cipher is given in the figure 2. Plain text sequence is:
a-z, A-Z, 0-9, ` ~ ! @ # $ % ^ & * ( ) _ - = + { } [ ] | ; : " <> , . ? /

Cipher text sequence is:
q-z, Q-Z, ` ~ ! @ # $ % ^ & * ( ) _ - = + { } [ ] | ; : " <> , . ? / , 0-9

3.2 Algebraic description

The algebraic description of the extended version is similar to that of the original cipher. It uses modulo 92 instead of modulo and cipher text Ci is derived using a sequence different from plain text sequence Pi.

Ci = EK(Pi) = (Pi + Ki) mod92

and decryption D,

Pi = DK(Ci) = (Ci - Ki) mod92

where, **P = P0…Pn** is the message,

C = C0….Cn is the ciphertext and **K = K0.....Km** is the used key.

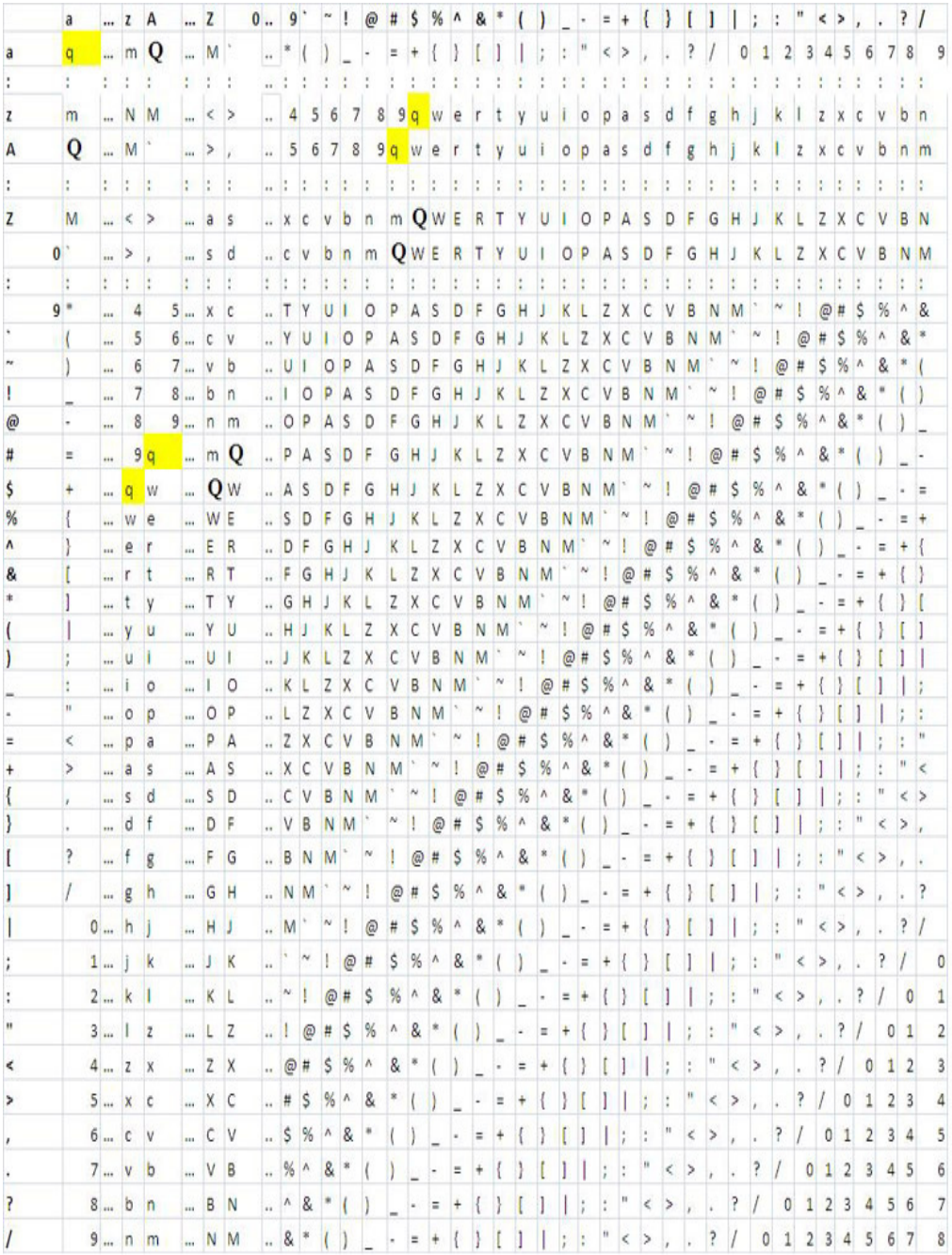

Figure 2. Alpha-Qwerty Cipher

3.3 Experimental Design

The Alpha-Qwerty cipher has been implemented in a working project. The project has been developed using J2SE 1.6 which encrypts or decrypts the plain text into cipher text based on the key provided by the user. The front end of the project appears in the figure 3.

The key is entered in the key field and input text is entered is provided in the input field which is encrypted or decrypted based on the option selected.

In the example of figure 4, we encrypt the text “transfer10,100toswissaccount” using the key Hell12* to
“`csn]^"N$)iggY`lRI*l7Iufm;+8”.

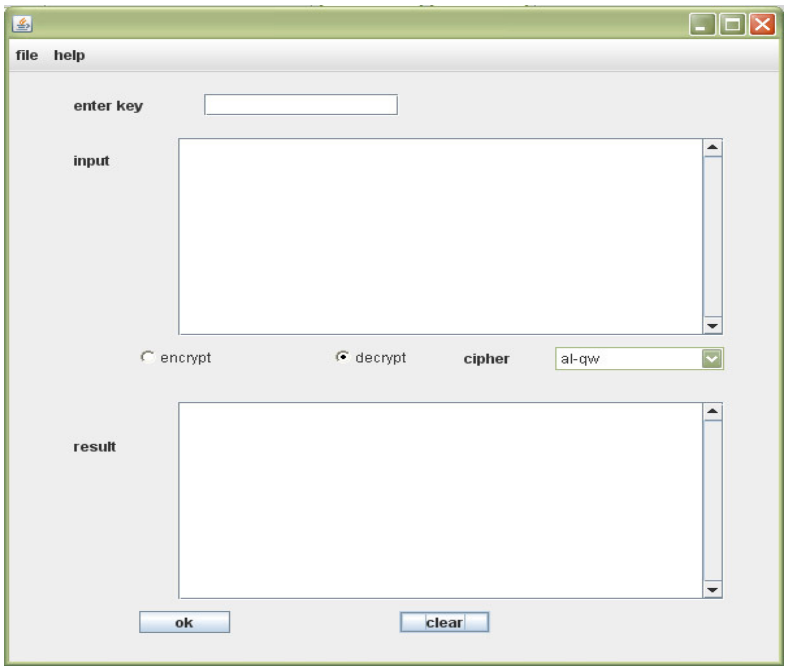

Figure 3. GUI of implementing tool

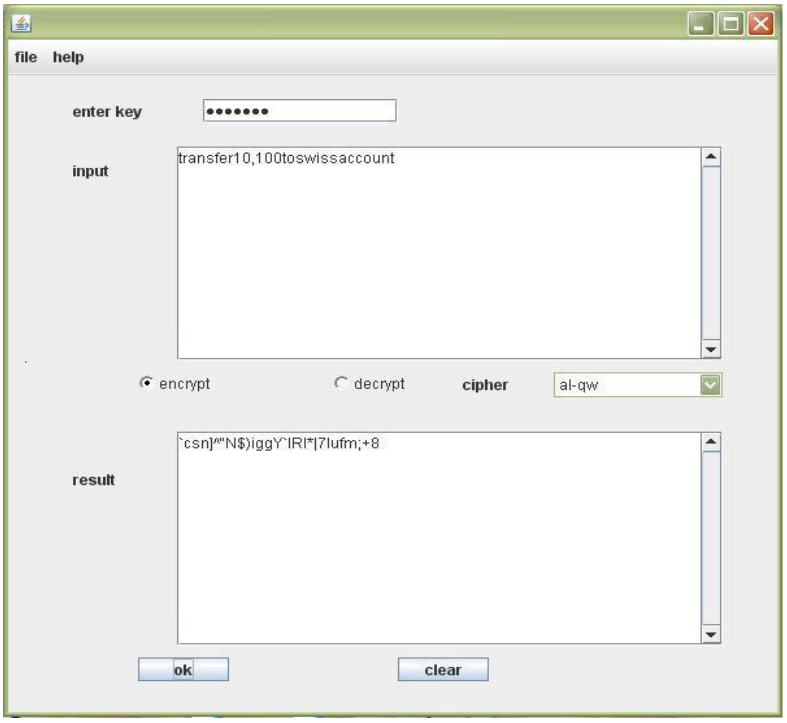

Figure 4. Encryption process

The plain text can be obtained back by selecting decrypt option & using the cipher text as input field. The example shows presence of characters and digits in both message and key which was not possible in the Vigenère cipher.

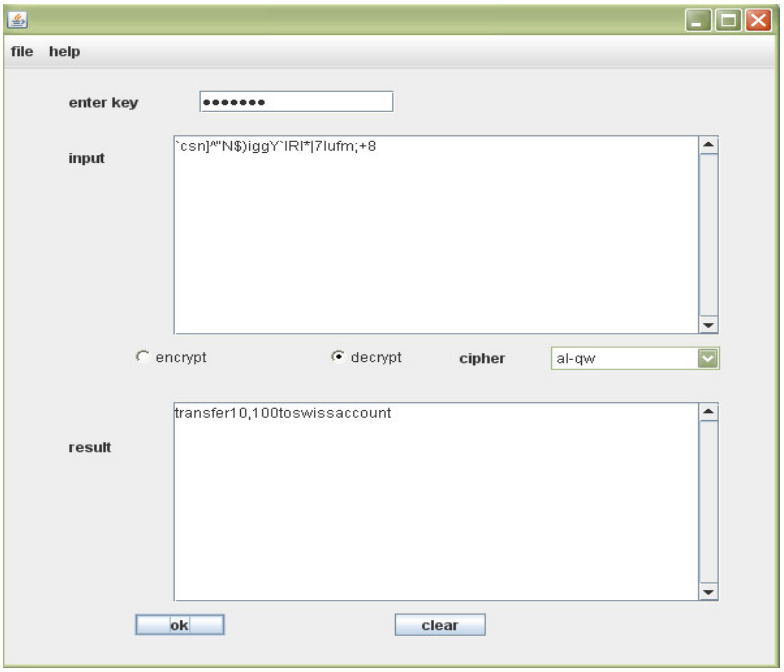

Figure 5. Decryption process

4. REVERSE ALPHA-QWERTY CIPHER

The reverse Alpha-Qwerty cipher is similar to the Alpha-Qwerty cipher in terms of the algebraic description and also the experimental design specified above for alpha-qwerty cipher can also implement this reverse alpha-qwerty cipher.

The reverse Alpha-Qwerty cipher however differs from the normal alpha-qwerty cipher in terms of the character sequence used for plain text and sequence. This provides an additional advantage of greater level of confusion in the cipher text.

4.1 Character set

The character set of the Reverse Alpha-Qwerty Cipher is given in the figure 6. Plain text sequence is:
q-z, Q-Z,` ~ ! @ # $ % ^ & * ( ) _ - = + { } [ ] | ; : " <> , . ? / , 0-9

Cipher text sequence is:
a-z, A-Z,0-9, ` ~ ! @ # $ % ^ & * ( ) _ - = + { } [ ] | ; : " <> , . ? /

4.2 Experimental Design

The experimental design for Alpha-Qwerty cipher can be used for reverse Alpha-Qwerty also just by selecting the required option in the drop-down list. The Plain text sequence ‘transfer10,000toswissaccount’ using the key “hell12*” gives the cipher text as “:tfCQcf~s"ie)_ZtkDt?d(zxNA.q@”.

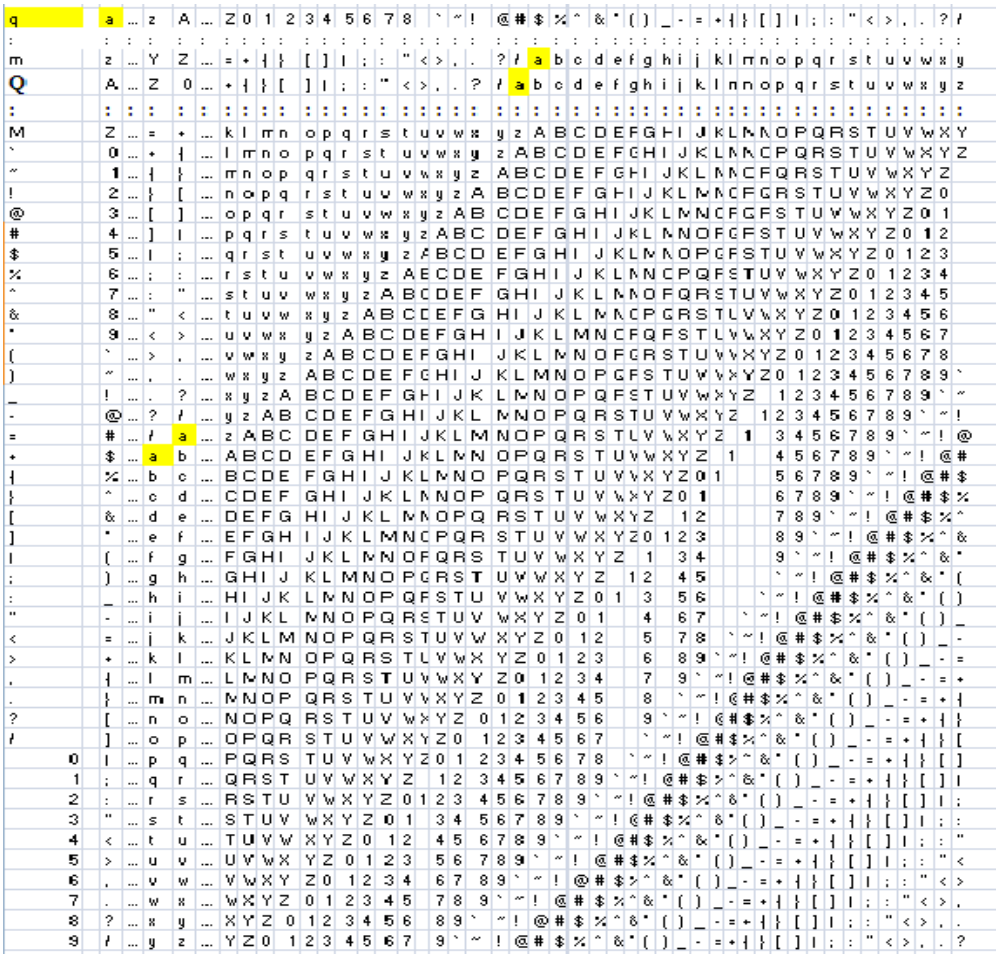

Figure 6. Reverse Alpha-Qwerty Cipher

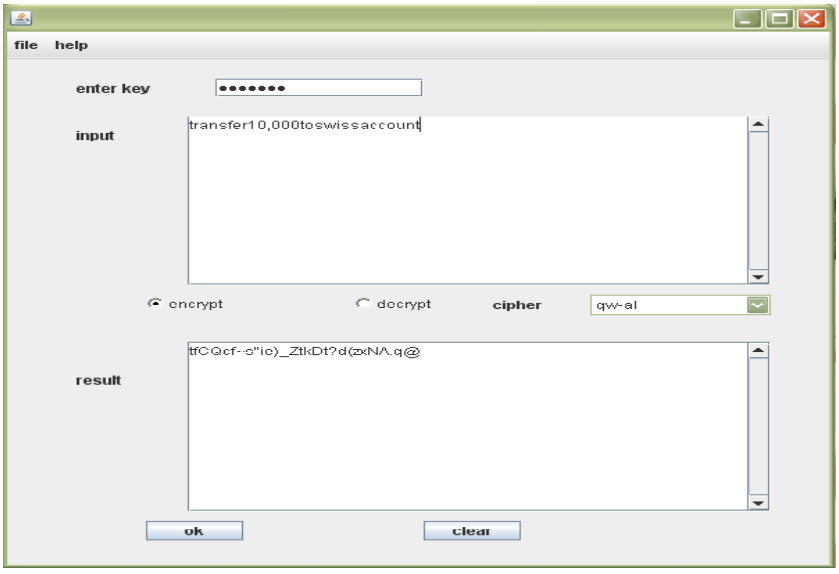

Figure 7. Encryption (Reverse Alpha-Qwerty)

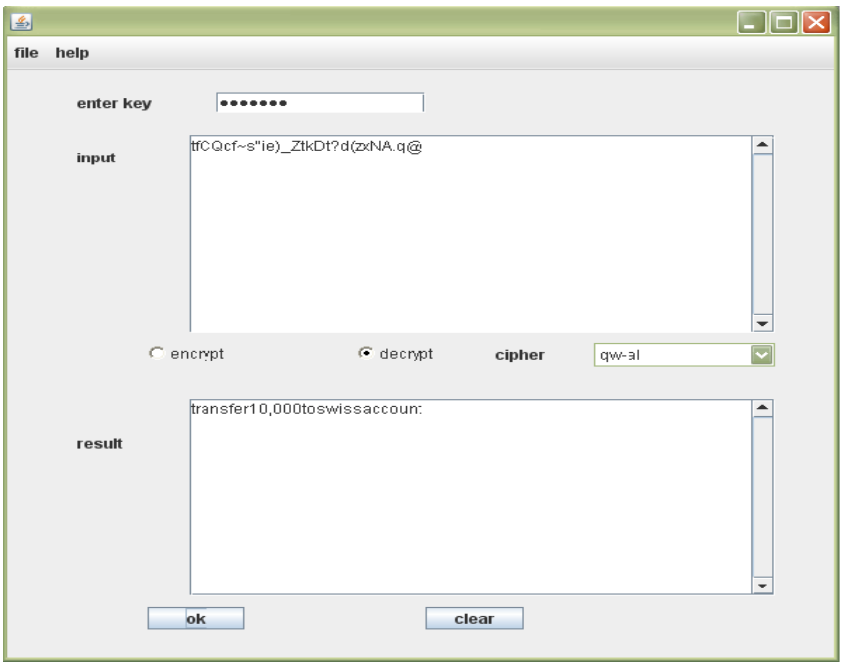

Figure 8. Decryption (Reverse Alpha-Qwerty)

5. ALGORITHM

The experimental implementation is based on the algorithm given below.

Alpha-Qwerty algorithm

Arrays Alpha [92] and Qwerty [92] store the 92 character plain text sequence order and cipher text sequence order to be followed respectively. Arrays ke[] is used to store the key. Array txt [] initially stores the original message which is updated to cipher text. Integer variables len and charlen store the keylength and length of message respectively. Array en[][] will store the mapping sequence that is generated from the key and is repeatedly applied.

Step 1: Obtain key from the user and copy to ke[]. Calculate keylength and copy to len

Step2: for i:=0 to len -1

```
{
        for j:=0 to 91
        {
                if ke[i] is equal to Alpha [j]
                {
                f:=0;
                for n:=0 to 92- j
                {
                        e[i][n]=Qwerty[f];
                        f++;
                }
```

```
        k:=0;
        for n:=92-j to 91
        {
                e[i][n]=Qwerty[k];
                k++;
        }
```

Step 3: copy message to txt[]. Length of message is copied to charlen.

Step 4: if encryption selected

```
        {
                s:=0;
                for m:=0  to charlen-1
                {
                for r:=0 to 91
                {
                        if txt[m] is equal to alpha[r]
                        {
                                txt[m]:=en[s][r];
                                break;
                        }
                }
                s++;
                if s is equal to len
                {
                        s=0;
                }
        }
        return txt[];
}
else{           //decryption selected
        s:=0;
        for m:=0 to charlen-1
        {
                for r:=0 to 91
                {
                        if txt[m] is equal to en[s][r]
                        {
```

```
                                txt[m]:=alpha[r];
                                break;
                        }
                }
                s++;
                if s is equal to len
                {
                        s=0;
                }
        }
        return txt[];
}
```

Reverse Alpha-Qwerty:

In the implementation of the Reverse Alpha-Qwerty cipher the working of arrays Alpha[92] and qwerty[92] has to be reversed.

6. COMPARISON WITH THE EXISTING VERSION

The greater character set allows more messages to be encrypted and other documents whereas the original version covered plain text involving only the 26 English characters. The messages can now allow digits and symbols which if used with a wisely chosen key will increase the complexity as the alphabets may even be written as digits or symbols. The same applies for digits and symbols, therefore providing greater masking and any third person trying to understand the cipher text will find it confusing.

Larger character set also means larger key domain. While the set of possible key in case of the original Vigenère cipher for length m was 26^m the extended Vigenère cipher or the Alpha-Qwerty cipher will have a much larger key domain of 92^m for a key of length of m. Hence we see even for a single character key the key domain provided is 3.53 times more, for a key of length 2 the key domain provided is 12.5 times more and so on [12].

The frequency analysis technique used for cryptanalysis will not work for alpha-qwerty cipher because it works only on the frequency of occurrence of the 26 English alphabets. There is no specific frequency of occurrence of digits or other symbols which cause the frequency analysis based cryptanalysis to fail.

7. CONCLUSIONS

The Alpha-Qwerty cipher intends to provide a greater character support as compared to the original Vigenère cipher. The Alpha-Qwerty and the reverse Alpha-Qwerty ciphers intend to extend the traditional Vigenère cipher from the 26 English Alphabets to a character set of 92 characters. The larger character set allows support for a greater set of messages including passwords and other transactions. The use of additional characters also increases the key domain making it more secure especially against brute force attack.

The use of symbols apart from the English alphabets makes both the message and the key more complex and less predictable. The cipher text is less understandable and difficult to break as compared to the original Vigenère cipher. In fact the use of other

characters causes the frequency analysis attack to fail which was implementable on the original Vigenère cipher. Therefore the Alpha-Qwerty and Reverse Alpha-Qwerty ciphers provide much more security. Both of these ciphers have been implemented experimentally on Java platform.

ACKNOWLEDGMENTS

The authors would like to thank heartily to the Chairman of Echelon Institute of Technology, Faridabad, INDIA, for providing a very conducive environment for research and development activities in the institution.

REFERENCES

[1] William Stallings: "Cryptography and Network Security: Principles and Practices" 4th Edition, Prentice Hall".

[2] Dara Kirschenbaum: "Advances in Cryptography History of Mathematics".

[3] http://www.garykessler.net/library/crypto.html.

[4] http://www.simonsingh.net/The_Black_Chamber/vigenere_cipher.html.

[5] Albrecht Beutelspacher: "Cryptology: an introduction to the art and science of enciphering".

[6] http://illuminations.nctm.org/LessonDetail.aspx?ID=L618

[7] http://www.counton.org/explorer/codebreaking/vigenere-cipher.php

[8] http://www.cs.trincoll.edu/~crypto/historical/vigenere.html

[9] Forouzan: "Cryptography and Network Security" 5th Edition, The Tata McGraw-Hill publishing Company Limited".

[10] http://www.math.cornell.edu/~mec/2003- 2004/ cryptography/polyalpha/polyalpha.html.

[11] Matthew C. Berntsen "Automating the Cracking of Simple Ciphers- A thesis."

[12] Stewart Gebbie: "A Survey of Mathematics of Cryptology", A research report submitted to Faculty of Science, University of the Witwatersrand, Johannesburg. February 3, 2002.

AUTHORS PROFILES

Md. Khalid Imam Rahmani is an Associate Professor in Computer Science & Engg. department of Echelon Institute of Technology, Faridabad, INDIA. He is having more than 14 years of teaching, industry and administrative experience. He has done B. Sc. Engg. in Computer Engineering branch from A.M.U., Aligarh, M. Tech. in Computer Engineering branch from M.D.U., Rohtak and is pursuing Ph.D. in Digital Image Processing from Mewar University, Rajasthan, India. His research areas include Digital Image Processing, Wireless Sensor Networks, Wireless & Mobile Computing, Algorithms, Web Technologies, Cloud Computing, Information Security and Programming Languages.

Neeta Wadhwa is an Assistant Professor in Echelon Institute of Technology, Faridabad, INDIA. She has 8 publications in national and international journals and conferences. Her research areas include Cryptography, Network Security, Symmetric Cryptographic Algorithms, and Programming Languages. She is having about 7 years of teaching experience in different universities. She is pursuing her Ph.D. from Jamia Millia Islamia, New Delhi, India.

VaibhavMalhotra is a B.Tech. student in Echelon Institute of Technology, Faridabad, India. He got 94 percentile in GATE-2012 examination. He is currently working on a project in Java. His areas of interest include cryptography and programming in Java/J2EE.