QWERTY Cipher
An Extended Substitution Cipher

Mr. Sushil Andhale
Lecturer, Computer Technology dept,
Babasaheb Gawde Institute of Technology,
Mumbai, India
sushil.andhale@mmbgit.org

Ms. Priti Rane
Lecturer, Computer Engineering dept,
Babasaheb Gawde Institute of Technology,
Mumbai, India
priti.rane@mmbgit.org

***Abstract*—** Substitution cipher is use to encrypt plaintext into ciphertext for secure communication. The message is encrypted by substituting the letter of alphabet n places ahead of the current letter, where 'n' acts as a key The Substitution Cipher works on the set of 26 English alphabets. In this paper we introduce the QWERTY Cipher which is the extension to the Substitution Cipher. This cipher works on set of 36 characters only by adding digits and some other symbols to the existing substitution cipher in addition to that changes the mapping sequence used in the substitution cipher. The mapping takes from an alphabet sequence to extended QWERTY keyboard sequence.

***Keywords* —** *QWERTY, ciphertext, substitution, plaintext, key.*

*****

1. INTRODUCTION:

Cryptography is defined as the art and science of making and breaking secret codes or messages. An original data called as plaintext is encoded into the ciphertext through the process of encryption and plaintext is restored from the cipher text through decryption. A key is used to configure a cryptosystem for encryption and decryption [1].

With any cipher, the goal is to have a system where key is necessary in order to recover the plaintext from the ciphertext. That is even if attacker has complete knowledge of algorithms used and other information he/she can't recover the plaintext without the key. A fundamental tenet of cryptography is that the inner workings of cryptosystem are completely known to the attacker, and the only secret is key [1].

There are four basic principles of Cryptography [2]:

1. Confidentiality: Aims to prevent unauthorized reading of message.
2. Integrity: Assuring the receiver that the received message has not been changed in any way from the original.
3. Authentication: Identifying or verifying a person who he/she claims to be.
4. Non-repudiation: A mechanism to confirm that the sender really sent this message.

2. SUBSTITUTION CIPHER:

In simple substitution, the message is encrypted by substituting the letter of alphabet n places ahead of the current letter. For example, with n = 3, the substitution which acts a key is:

Plaintext :
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

Cipher text:
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

Where we have followed the convention that the plaintext is lowercase and the ciphertext is uppercase. In this example, key would be stated more succinctly as "3" since the amount of shift is the key.

Using the key of 3, we can encrypt the plaintext message

Attackatdawnonpearlharbour

By looking up each letter in the plaintext row and substituting the corresponding letter in ciphertext row or by simply replacing each letter by the letter that position ahead of it in the alphabet.
In this particular example, the resulting ciphertext is,

DWWAFNDWGAZQRQSHDUOKDUERXU

however as it substitutes original letter with new one using shifted key, it is known as simple a substitution.

To decrypt we simply look up the ciphertext letter in the ciphertext row and replace it with the corresponding letter in the plaintext row, or simply shift each ciphertext letter backward by three. This kind of simple substitution with a shift of three is known as the Caeser's cipher because it was reputedly used with success by Julius Caeser.

If we limit the simple substitutions with shifts, then the possible keys are

n Є { 0,1,2,3……., 25 }.

2.1 Algebraic description of Substitution Cipher

Substitution cipher can also be viewed algebraically. If we take the letters A–Z are to be the numbers 0 – 25, then the Substitution encryption E using the key *n* can be written as:

Ci = E(Pi + *n*) mod26

and decryption D using the key K,

Pi = D(Ci - *n*) mod26

Where

P = P0… Pn is the message,

C = C0…. Cn is the ciphertext and

***n* = *n*0..... *n*m** is the used key.

3. THE QWERTY SUBSTITUTION CIPHER:

The QWERTY substitution cipher intends to extend the original 26 character substitution cipher to a 36 characters cipher including digits and some other symbols commonly used in the English language and can be written from a QWERTY computer keyboard. Furthermore mapping sequence used in substitution cipher is also changed in QWERTY cipher. The mapping takes from an alphabet sequence to extended QWERTY keyboard sequence. To decode the code reverse mapping takes place (complement of encryption) that is from extended QWERTY keyboard to extended alphabet sequence. In short this proposed extended version extends and rearranges the original substitution, therefore making it much more complex and secure than the existing one. The larger character set allows more type of messages to be encrypted. It also provides more security by increasing the key domain [3].

3.1 Character set

The character set of the Qwerty Cipher is given in figure 1, with all possible shifts of keysapce 0 - 35
Plain text sequence is:

q w e r t y u i o p a s d f g h j k l z x c v b n m 1 2 3 4 5 6 7 8 9 0

Cipher text sequence (key *n* = 3) is:

R T Y U I O P A S D F G H J K L Z X C V B N M ! @ # $ % ^ & * ( ) Q W E

Here we are replacing digits with its equivalent shift symbols, and thus making more complex and secure.

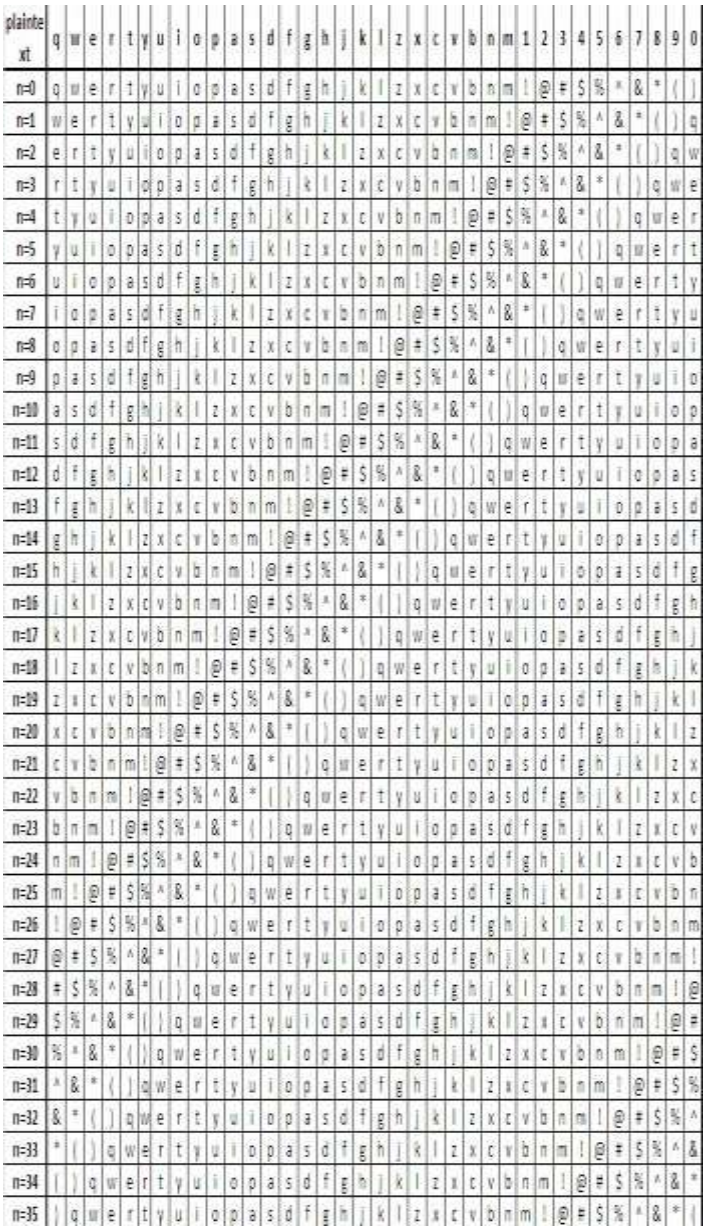

Figure 1. QWERTY Substitution Cipher

 ISSN: 2321-8169
3367 – 3370

3.2 Algebraic description

The algebraic description of the QWERTY version is similar to that of the original substitution cipher. It uses modulo 36 instead of modulo 26 and cipher text Ci is derived using a sequence different from plaintext sequence Pi.

Ci = E(Pi + *n*i) mod36

and decryption D,

Pi = D(Ci - *n*i) mod36

where,

P = P0…Pn is the plaintext message,
C = C0….Cn is the ciphertext and
***n* = *n*0.....*n*m** is the used key.

4. ALGORITHM

The algorithm given below.

QWERTY SUBSTITUTION ALGORITHM

Arrays QWERTY [36] and Cipher [36] store the 36 character plaintext sequence order and ciphertext sequence order to be followed respectively. Arrays N [ ] is used to store the key. Array txt [ ] initially stores the original message which is updated to ciphertext. 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 N [ ].
Calculate keylength and copy to len

```
Step2: for i:=0 to len -1
{
        for j:=0 to 35
        {
                if N[i] is equal to Qwerty [j]
                {
                f:=0;
                for n:=0 to 35- j
                {
                e[i][n]=Cipher[f];
                f++;
        }
                k:=0;
                for n:=36-j to 35
        {
                e[i][n]=Cipher[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 35
        {
                if txt[m] is equal to Qwerty[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 35
        {
                if txt[m] is equal to en[s][r]
        {
                txt[m]:=Qwerty[r];
                break;
        }
}
                s++;
        if s is equal to len
        {
        s=0;
        }
}
return txt[];
```

5. COMPARISON WITH THE EXISTING VERSION

The original version covered plaintext involving only the 26 English characters whereas extended version gives greater character set and thus allows more messages to be

encrypted. This version now allows digits to replace by symbols which if used with cleverly chosen key will increase the complexity and security. Alphabets and digits and replaced with symbols, therefore providing greater masking and attacker trying to understand the ciphertext will find it confusing. We are changing sequence from general alphabet to QWERTY sequnece will also leads to greater security. Extended version has larger character set which means bigger key domain. The set of possible key in case of original version for was 26, while the extended version will have larger key domain of 36.

6. CONCLUSION

QWERTY substitution cipher provides a greater character support than original simple substitution cipher. The QWERTY cipher extends the traditional substitution cipher from the 26 English Alphabets to a character set of 36 characters. The use of additional characters increases the key domain making it more secure especially against brute force attack. The use of symbols instead of digits and the English alphabets makes messages and key more complex and less predictable. QWERTY cipher is difficult to break as compare to traditional substitution cipher as it uses QWERTY sequence rather than general alphabetic sequence. Therefore QWERTY substitution cipher is more secure than original substitution cipher.

7. ACKNOWLEDGMENTS

The authors would like to thank heartily to the Hon, Secretary Babasaheb Gawde Institute of Technology, Mumbai, INDIA, for providing a very conducive environment for research and development activities in the institution.

8. REFERENCES:

[1] WILEY-INDIA: marks satmps “Information security: principles and practices” first edition “Deven Shah”

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

[3] Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012 DOI : 10.5121/acij.2012.3311 107 “ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER” by Md. Khalid Imam Rahmani, Neeta Wadhwa and Vaibhav Malhotra