



## **ENCRYPTION MODE OF LANGUAGE SYMBOLS**

Kalpana Dwivedi<sup>1</sup>, Shantanu Sharma<sup>2</sup>, Jyoti Jadon<sup>3</sup>

**Abstract-**The paper emphasizes on modern encryption techniques that if taken into consideration can be proved as a bottleneck in the industry of the cyber security. We often forget the importance of languages that are used in the communication. The countries across the world are encrypting their codes in their native languages. Three levels of encryption are involved in our encryption. First level involves the use of the simple polynomial algebraic equation. Second level involves the use of the right shift of the alphabet depending on the values of the keys and the sub-keys. The third level encryption involves the use of the language symbol codes that will function in accordance to the even or odd sequence. The methodologies involved will be demonstrated using the high level programming languages.

**Keywords -** Cryptography, Encryption, Language Symbols, Operator Sequencing

### **1. INTRODUCTION**

Cryptography is a bottleneck in the field of the cyber security and it involves the encryption and decryption of the data, files and even application software. It is something that was developed ages ago around thousands of years ago to protect the information of the dynasties. At that time of encryption and decryption the keys were not involved in computation, but with time the more powerful cryptography algorithms were developed which involved the usage of keys. In the current scenario of technology it involves the usage of very strong computational algorithms which can sometimes involve the usage of supercomputers. DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are the cryptographic standards as per the US government. Modern Cryptography can be divided into two sub-parts: Symmetric-key cryptography: Only one key to encrypt and decrypt. Asymmetric-key cryptography: Two different keys to encrypt and decrypt.

### **2. LITERATURE REVIEW**

#### *2.1 Cryptanalysis -*

The art of breaking ciphers which is often considered to be the vital aspect when it comes to cyber security. A lot of research is done on this particular section by the computer hackers and there is a dazzling array of algorithms under defined under this section. The Index of Coincidence was one of the first methods which was recognized in the field. The research took a further growth when breaking of the enigma came out in the late 1940. In the current or the modern cryptanalysis the Differential Methodology is used in cryptanalysis in breaking of the DES encryptions. There are three types of cryptanalysis known to us depending on the types of text:

Ciphertext only

Known ciphertext/plaintext pairs

Chosen plaintext or chosen ciphertext

In the year 1990 it became very easy for the programmers to break the 40-bit key encryption which eventually has now shifted to the 128 bit encryption technique. When we talk about the RSA cryptoalgorithms, the factoring record was 39 digits in the year 1970 which became 768 digits in the year 2009.

#### *2.2 Cryptography -*

Cryptography is something which is known to exist since mankind came into existence. Until the First World War the ciphers were not much efficient as it involved raw approach to handle the secrecy. After the First World War several new things were employed in the process such as punched cards, relays etc. which later led to the usage of rotor machines by the Second World War. The first use of cryptography was employed by Spartans (400 BCE). On the Defense of Fortifications was one of the earliest study on the subject by Aeneas Tacticus during the 4<sup>th</sup> century BCE. Polybius Checkerboard was just another concept in the field in which letters were replaced by pair of symbols. Monoalphabetic ciphers were used by Romans which involved the shift of the positions. Compilation of ciphers by Gabriele de Lavinde of Parma was the first European manual on cryptography (c. 1379). The first cipher disk was described by Leon Battista Alberti (Trattati in Ciphra) in 1470. In the current scenario of cryptography **DES** encryption is used which ranges from 64 bits. In October 2000 **AES** became the new standard as per the norms by NIST. Whenever we vary the various concepts in the development of the algorithms we get the best of

<sup>1</sup> Department of computer science and Engineering, NIET, Greater Noida, Uttar Pradesh, India.

<sup>2</sup> Department of computer science and Engineering, NIET, Greater Noida, Uttar Pradesh, India.

<sup>3</sup> Department of computer science and Engineering, NIET, Greater Noida, Uttar Pradesh, India.

the Cryptography. The works on Public Key Cryptography and Sharing Networking Resources is considered a bottleneck in the field of cryptography.

### 3. PROPOSED ALGORITHM

#### 3.1 Shantanu sabidurian algorithm

The encryption algorithm is developed using the symbol codes of three languages. We use encryption algorithm to secure our information on digital platforms. The three levels of encryption is proposed in our algorithms. The application of public key cryptography is used in demonstrating our work. The decryption of different language symbols in one line becomes a hectic task.

For first level encryption: The encoding of letters with 1-2-1 takes place. Each word is replaced with digits 1 or 2.

For second level encryption: The generation of key and the sub-key takes place is done using an algebraic equation.

For third level encryption: The three languages are assigned a keyword with different subscripts. The sequence is different for odd length words and even length word.

step1: user\_input(word);

step2: randomize(1 or 2) for word[i=0...length-1] // first level encryption

step3: user\_input(sentence);

step4:  $K=n+k^p$ ; //K is key, k is sub-key, n is the position of the alphabet, p is the order

step5: user\_input(k)

step6: Right\_Shift(sentence[index]+K) //second level encryption

step7: user\_input(total languages);

step8: if total languages=n

step9: then if(length(word)=odd call sequence(L1L2L3..LN)); //third level encryption

step10: else call sequence(LNL(N-1)...L1);

step11: encode\_symbol();

Each symbol which will be encoded with respect to any of the language which validate its value using a graph which shows the symbol codes for various alphabets.

For demonstration Russian language is used for encryption of English letters.

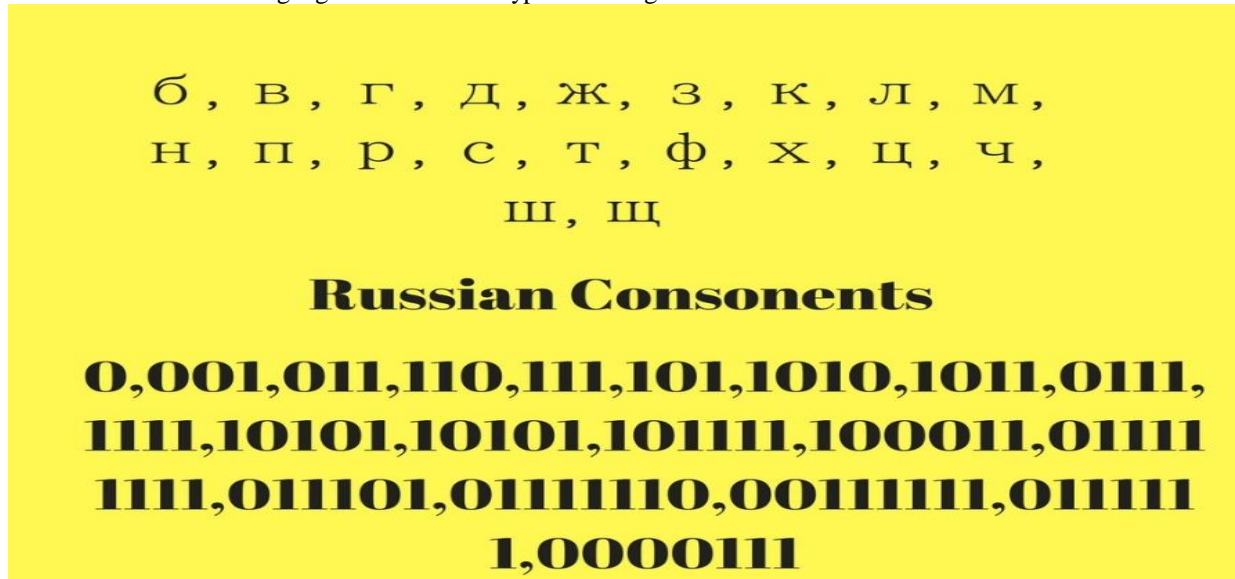


Figure 1. Replacement of language symbols

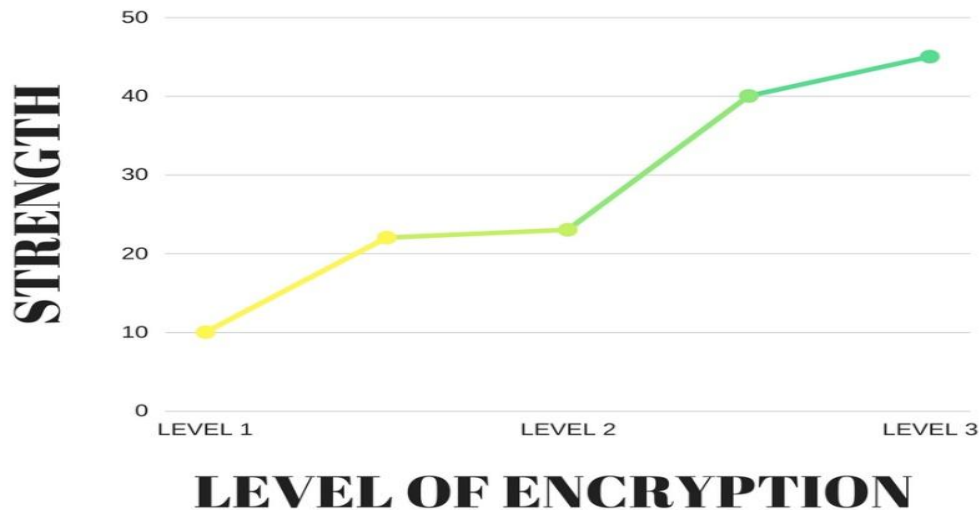


Figure 2. Strength of encryption with increasing level

#### 4. RESULT

The encryption result obtained will range upto 128 bit encryption. If encryption is applied on any sentence:

After applying successive encryption algorithm we obtain

“0001010101011111111111110000111111111111111100001011111110101001011111111101010110101010010101011100011111”

The binary format is obtained. The format can be of any language. The languages can be any in number and it can be any language. The different levels involved help us to secure data efficiently.

#### 5. CONCLUSION

An encrypting algorithms that uses different languages for encryption of information. Each consonant in any language will be developed using chart code demonstrated in Fig.1. Increasing the level of encryption the strength of encryption increases as demonstrated in Fig.2. Complexity of the algorithm is implementation depending and would depend on the number of languages chosen. The computer with less computational power will be quite inefficient to do our work. The concepts that won't perish in the fields of cyber security.

#### 6. FUTURE WORK

A. Decrypting Algorithms: Several decrypting algorithms might be developed for decryption of language symbol based encryption.

B. Public- Private Key: The encryption using different types of keys based on the scenarios can be defined for development of more detailed approach.

C. Machine Learning: The machine learning algorithms can be used for encrypting language symbols.

D. System Software encryption: The system software interfaces can also be made encrypted depending on the scenario.

#### 7. REFERENCES

- [1] B. Schneier, Applied Cryptography, 2<sup>nd</sup>ed., John Wiley & Sons, 1995.
- [2] William Stallings, Cryptography and Network Security, 3<sup>rd</sup>ed, Wiley, 1995.
- [3] Rob Curley, Cryptography: Cracking codes, 1<sup>st</sup>ed, Britannica, 2013.
- [4] Mark Stamp and Richard M. Low, Applied Cryptanalysis, 1<sup>st</sup>ed, Wiley, 2007.
- [5] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.
- [6] Encryption Technology White paper, <http://security.resist.ca/crypt.html>.