Data Encryption / Decryption process using PSZ methodology and performance Analysis with RSA.

Mr.Anil Hingmire

[1] Vidyavardhini's college of Engineering & Technology, Mumbai University,

Abstract—

A day-to-day use of cryptography in our life is increasing tremendously, this is because of necessity of our multimedia documents to be protected from unauthorized person. As the days are passing the old algorithms are not remained so strong as cryptanalyst are familiar with them. Today the computers are faster and in feature its speed will increase more and more. Brute force attacks are made to break the encryption and they are growing so faster. These attacks are the main drawbacks of older algorithm. But with feature this algorithms will be replaced by new techniques that will provide better protection. In this paper we are going to proposed new encryption technique which is more faster, better immune to attacks, more complex, easy to encrypt and many more advanced security feature included. This Document displays the comparison between PSZ algorithm and RSA Algorithm which are used in the encryption of plaintext into cipher text that are generally used in cryptography.

Keywords:
cryptography, cryptanalyst, symmetric encryption, Authentication key, RSA etc.

INTRODUCTION

Nowadays the use of internet in society for various purposes including information distribution is familiar worldwide. Data transmitted over the Internet passes through many servers and/or routers and there are many opportunities for third parties to intercept that transmission. Preventing interception is impossible; instead, the data must be made unreadable (encrypted) during transmission, with a way for the intended recipient to be able to transform the received transmission back to its readable form (decryption process) . When a message is *encrypted*, that means that it is transformed into a form when the data is passed through some substitute
technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data and that is not readable. When a message is *decrypted*, it is returned to its original readable form. Encryption can provide strong security for data to give sensitive data the highest level of security.

The goal of encryption is to make data unintelligible to unauthorized readers and extremely difficult to decipher when attacked.
The security of encrypted data depends on several factors like what algorithm is used, what is the key size and how was the algorithm implemented in the product.

Here in this paper a proposed new technique related cryptography for protecting documents. Complexity of this algorithm is more but in quite easy manner and makes it quite difficult for cryptanalyst to break. Different feature of RSA and the new proposed algorithm will be compared and will check its result and planed for future [7,8].

A. *RSA*

Rivest, Shamir and Adelman algorithm for cryptography system. This is an encryption algorithm totally based on mathematics. A lot of mathematical computation it includes in its encryption and decryption. There are two kinds of encryption RSA algorithm exist. One is called Symmetric RSA and other is Asymmetric RSA algorithm [7,8] .

Symmetric RSA uses a single key that must be kept secrete. Its speed is faster. Asymmetric RSA uses double key of which one key is public key and other is private key. Its speed is quite slower [8].

RSA founds a complete mathematical base its implementation is full of calculation and uses two large prime numbers. It includes taking power of terms, modulo division and final representation. Its basic is the large prime numbers and mathematical calculation based on term like(taking power and modulo of power). This provides essential security and in start it was assumed unbreakable [7,8].

But this mathematical base is prime problem as it quite time consuming and took lot of time for long documents. This time is quite important in multimedia system

also essential on distributed client server technology. Another problem with RSA is that its choice for primary keys which must be prime to each other. With the development in technology RSA is nowadays breakable by using attacks like Brute force. So its protection is nowadays limited [8].

NEW PROPOSED ALGORITHM AND ITS PROCEDURE

1) New proposed algorithm (PSZ)

In this section we are going to introduce our algorithm and its working. Algorithm follows three fundamental encryption skim. This includes a phase of Substitution, Position and Zigzag encryption. It generates only single key and takes a key level from the users which is used in Substitution and Position method. Since it undergoes three phases the overall complexity increases and algorithm becomes quite immune to attack.

The generated key is based on length of text as well as a private key is generated which must be kept secrete. So it provided double secrete level protection. Even the complexity is very high time taken by algorithm to encrypt is less and procedure to encrypt the text is simple Thus algorithm is become so multipurpose usable.

We will explain the algorithm by the way that it follows sequence for encryption.

- **Position Method**

. In This technique a word may be a alphabet, number or special character is shift on the basis of the key provided by the end user.

Procedure can be step wised explained as follows:

Step1: Enter the Source file and key level

Step2: Check whether key is valid or not (i.e:0<key<11)

Step3: Access a valid encryption string of alphabets from database.

Step4: Encrypt Source file on basis of accessed string.

Step5: Generate a key for user on the basis of length of file.

- **Substitute Method**

A Substitution technique is based on replacing the character by shift provided by the user. By this feature a lot of complexity getting added and it is quite difficult for cryptanalyst to break the code.

Procedure can be step wised explained as follows:

Step1: Take the positional encrypted and user provided key level

Step2: Divide the file into block of length 64 byte.

Step3: substitute character on basis of shift provided by the user.

Step4: Store it in array of length 64 byte.

Step5: Use them for remaining procedure of Zigzag.

- **Zigzag Method**

In this procedure we are going to jumble the text by passing thought Zigzag manner. Thus 3rd degree protection is added to the final algorithm. Because of such encryption final encryption pattern is different from normal pattern. So the overall attack is minimised with this technique.

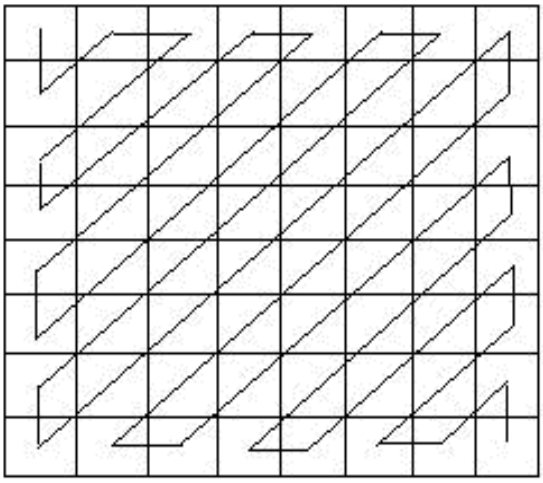


Fig. 1 Example of Zigzag pattern

Procedure can be step wised explained as follows:

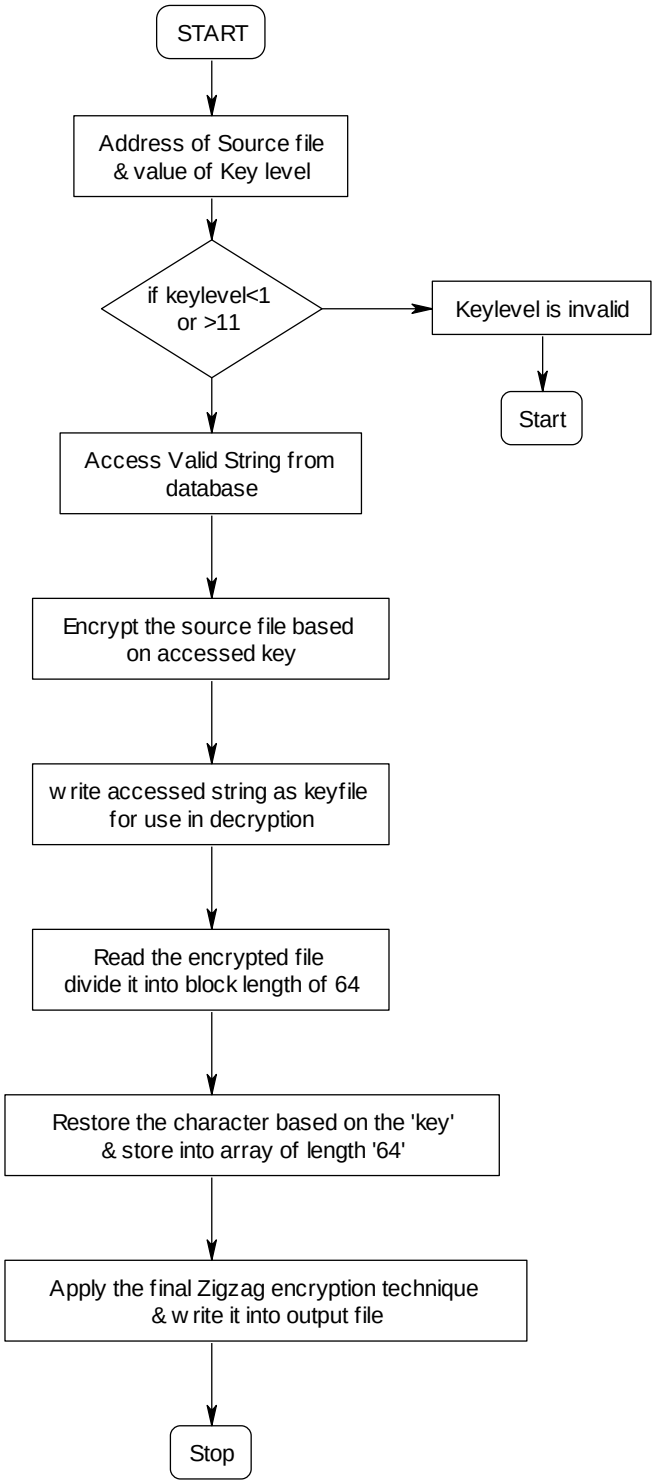
Step1: Take the 64 bytes array

Step2: Apply the Zigzag coding to this array.

Step3: Combine all the 64 bytes array to form a single file of encrypted text.

Step4: Generate the private encryption key for future use for decoding.

2) Flowchart


START
Address of Source file & value of Key level
if keylevel<1 or >11
Keylevel is invalid
Start
Access Valid String from database
Encrypt the source file based on accessed key
w rite accessed string as keyfile for use in decryption
Read the encrypted file divide it into block length of 64
Restore the character based on the 'key' & store into array of length '64'
Apply the final Zigzag encryption technique & w rite it into output file
Stop

3) Comparison of algorithms on basis of obtained result

- **TIME REQUIREMENTS**

RSA: Encryption and decryption time is more[1].It took about 1078 ms for encryption and 875 ms for decrypting the same file(say ALPHA)[2].

PSZ: Encryption and decryption time is less[1].It took about 125 ms for encryption and 62 ms for decrypting the same file(say ALPHA)[2].

- **CONFIDENTIALITY**

RSA: Encryption requires public key and decryption requires private key so two key are requires [1].To decode it user must need private key so authorised person having private key can only decode the text[2].

PSZ: Encryption requires the key level and decryption requires private key [1]. To decode it user must need private key so authorised person having private key can only decode the text [2].

- **INTEGRITY AND USABILITY**

RSA: Encryption and decryption is accurate if they are run with valid public and private key[1].After encryption plaintext is modified to cipher text which is unreadable which can only be obtained after correct decryption[2].It is well for long text level encryption[3].

PSZ: Encryption and decryption is accurate if they are run with key level and private key[1].After encryption plaintext is modified to cipher text which is unreadable which can only be obtained after correct decryption[2].It is well for long text level encryption as well as short text level encryption[3].

- **KEY LENGHT**

RSA: A Key generated after the encryption is basically depends on the length of the plaintext [1].By experimentally the generated key is 86400 after encrypting the file ALPHA [2].

PSZ: A Key generated after the encryption is basically depends on the length of the plaintext [1].By experimentally the generated key is 78195 after encrypting the the file ALPHA [2].

TABLE I

Pt. no	COMPLETE COMPARISON TABEL		
	Characteristics	**RSA**	**PSZ (proposed Alg)**
1	Time Requirements	More	Less
2	Confidentiality	More	More
3	Integrity & usability	More & long text	More & long text as well as for short text
4	Key Length	More	Less

TABLE II

Time required for Message Encryption

No.	Message Size	RSA (Time in ms)	PSZ (Proposed Algo.) (Time in ms)
1	10	15	31
2	100	16	31
3	1000	79	31
4	10000	703	93
5	100000	6656	594

Time required for Message Decryption

Pt no	Message Size(bytes)	RSA (Time in ms)	Proposed Algo. (Time in ms)
1	10	32	15
2	100	32	15
3	1000	187	15
4	10000	578	78
5	100000	10485	562

CONCLUSION

In this paper we introduced new algorithm which is compared with RSA for its standardization for various characteristics and display following result in the conclusion.

To provide better protection on multimedia system to the multimedia objects we need technique which is better in means of time, immune to attack, applicable to any kind of

documents, easy to handle and understand. Today the copyright protection is most essence in digital world but as with time progress older things like RSA are getting weak because of faster technology. Also with this advancement new things are getting developed which are more powerful than older so we need to move our footsteps towards it to take its full advantage.

Our proposed algorithm is not only faster than RSA but also provides more complexity and also well suitable for larger message size as shown in result. This one is more immune to attack because of its complexity. For small text of encryption also it is most suitable because of its complexity also for long text of encryption it is best as it took lesser time than RSA.

REFERENCE S

1] T.Chueng, Z.Yusoff, A. Sha'ameri "Implementation of pipelined Data Encryption Standard (DES) using Altera CPLD" , IEEE 2000.

2] Gang Hu "Study of File Encryption and Decryption System using security Key" 2010 2nd ICCET, Volume-7, IEEE 2010.

3] Dr.Mohammed M.Alani "DES96- Improved DES security" 2010, 7thInternational Multi-conference on Systems, Signals & Devices. 2010 IEEE

4] C. Sanchez-Avila, R. Sanchez-Reillo "The Rijndael Block Cipher (AES proposal): A comparison with DES" 2001 IEEE.

5] Seung-Jo Han, Heang-Soo oh, Jongan Park "The improved Data Encryption Standard (DES) Algorithm", 1996 IEEE.

6] Q.Gong-bin, J. Qing-Feng, Q.Shui-Sheng "A new Image Encryption Scheme based on DES Algorithm and Chua's Circuit" 2009 IEEE.

7] IEEE P1363 Standard Specifications for Public Key Cryptography, IEEE, November 1993.

8] R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, 21 (2), pp. 120-126, February 1978.

About Author

Mr. Anil M. Hingmire,
Vidhyvardhini's College of Engineering & Technology, Vasai , Mumbai University.