Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9386-9388, 2017
ISSN: 1816-949X

UR5 New Symmetrical Algorithm For Security

Nikhita Jatain and Praful R. Pardhi
Department of Computer Science and Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, India

Abstract: Due to the quick growth of communication, security has become an major issue for communication and to prevent the data, so, cryptography is used mainly. Cryptography is used to safe the message and data from attacker or hacker. It is primary necessity in any type of area. Some firm may have large set of data and some many have small set of data. Encryption is one of the ways to secure the data. Encryption is the process of changing appearance or adjusting of a message in order that only the intended recipient can read it. Encryption can provide a means of securing the message. For safety purpose various algorithms are proposed such as AES, DES, 3DES, etc. A new symmetrical cryptography algorithm is proposed here to secure the data from outside attacks. It also additionally avoids the key exchange between the sender and user. Here, security as compared as the size of key will expand at the time of encryption and decryption.

Key words: Cryptography, decryption, encryption, key update, S-box, security

INTRODUCTION

With the grow of security, hacking and cracking of knowledge has also increased. Security of networking systems has become very important. Many companies now rely on web services as a major source of revenue (Raj and Anbu, 2014). If user wants to safeguard the data, then cryptography is must. Cryptography is the art of preventing information by reworking it into an unreadable format. In cryptography the information that is in the form of plaintext gets changed into cipher text by the use of key and this process is known as encryption. The cipher text is then regenerate into plaintext by decryption method. Cryptography systems can be classified into symmetric-key systems that use one key that both the sender and recipient have and asymmetric-key systems that uses pair of keys, a public key known to everyone and private key known to only sender and receiver. There are already many old encryption techniques like DES, AES or 3DES etc., (Stallings, 2007). For providing high security to the data that will be in text or in image kind. All these are used in different applications. In all algorithm different variety of operations are performed like XOR, substitution, shifting, etc. (Fig. 1)

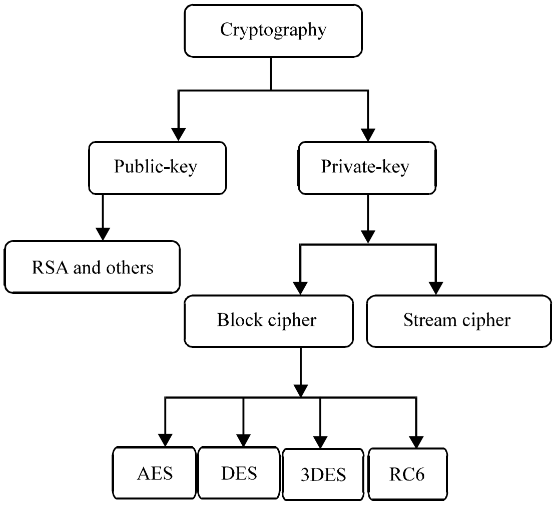

Fig. 1: Cryptography fields

DES algorithm: The Data Encryption Standard (DES) is the symmetric key algorithm for encryption and decryption of message (Singh, 2013). It apply on 64 bit blocks of information by using a 56 bit key size. It uses feistel network that divides block into two halves before doing secret writing of data. It is an old technique used for encryption and decryption.

Disadvantages:

- It is breakable with Brute force attack
- Key size is small so can be easily recognized
- The 4 keys are in total weak keys
- Many DES cracking machines can search entire key space

Corresponding Author: Nikhita Jatain, Department of Computer Science and Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, India

3DES algorithm: The triple data encryption standard is a symmetric-key block cipher which applies the data encryption standard cipher algorithm thrice to each data block. 3DES consists of three different DES keys K_1-K_3. 3DES key has total length 3×56 = 168 bits.

Disadvantages:

- If all the keys are same then it will research as DES algorithm
- Out of total 168 bits keys only 112 bit keys are effective keys

AES algorithm: The Advanced Encryption Standard (AES) is an coding method (Daemen and Rijmen, 2001). The AES encryption algorithm is a block cipher that uses an associate key and several other rounds of encryption AES encryption uses a single key as a part of the encryption process. The key will be of 128, 192 or 256 bits in length. The term 128 bit encryption refers to the use of a 128 bit encryption key. With AES both the encryption and the decryption are performed using the exact key. An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data. It is important to keep the encryption key a secret and to use keys that are hard to guess.

Disadvantages:

- It is very complex
- It requires more round of communication as compare to DES

Proposed system: The main motive behind this algorithm is to provide higher security to the user, so that, he can transfer his confidential information simply. In this study a block cryptography algorithm is presented. Distinctive style of operations is used in this algorithm such as S-box and gate and xor gate (Ramesh and Umarani, 2012). This algorithm rule contains 64 bits of plaintext by 64 bits key size. It avoids key exchange through encryption and decryption method. Here 8 rounds are used for encryption and decryption. Distinct plaintext uses dissimilar key. S-box plays vital role during this algorithmic rule. It has total 8 columns and 256 rows. Each element consists of 8 bits (Amador and Green, 2005). It exchanges the input with completely different code to the output. The order of columns is going to be as:

- Round 1: C1C2C3C4 C5C6C7C8
- Round 2: C2C3C4C1 C8C5C6C7
- Round 3: C3C4C1C2 C7C8C5C6
- Round 4: C4C1C2C3 C6C7C8C5

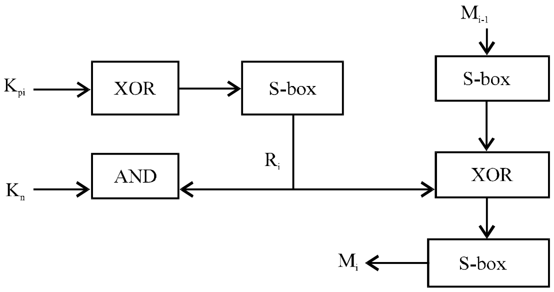

Fig. 2: Encryption process

- Round 5: C5C8C7C6 C3C2C1C4
- Round 6: C6C5C8C7 C2C1C4C3
- Round 7: C7C6C5C8 C1C4C3C2
- Round 8: C8C7C6C5 C4C3C2C1

The sequence of columns in S-box is reorder in every round. Rounds are split into two parts, initial part consists of rounds 1-4 and second half consists of rounds 5-8. Second part is the reflection of initial part of round. During secret writing there are two outward keys K_{pi} and K_n where k_n is equal to (0000000000000000) and (FFFFFFFFFFFFFFFF) values and in K_{pi}, i is the number of round from 1-8 and has primary value as 64 bits, this 64 bits can be similar for every round or may be dissimilar key values. Initially key is split into eight parts of 8 bits each.

Figure 2 shows the encryption of UR5 algorithm of 64 bits. Throughout the time of encoding the plaintext message of 64 bits will gets split into 8 parts as 8 columns of S-box. The column order will going to rely on the round number. The output of S-box probably be XORed with R_i which is round key. The output will get split into 8 parts and then it will apply on S-box. The output will be the input for the next round. The key which is turn out will not depend on other round key. During decryption if any complication will occur then K_n will set to beginning value zero and K_{pi} to its initial key value. In decryption process the order of R_i will get inverse while obtaining plaintext. For next message the key will upgrade itself. Dissimilar keys are used in different rounds.

RESULTS AND DISCUSSION

New symmetric algorithm: In this new symmetrical algorithm 512 bits plaintext is apply with key size 512 bits to encrypt and decrypt the input. It uses 16 rounds for encryption and decryption (Ramesh and Umarani, 2010). Different operations is used namely XOR and S-box. XOR and gates are apply for different move process and S-box is the matrix of 16×16×16 which comprise of 16 slides. The

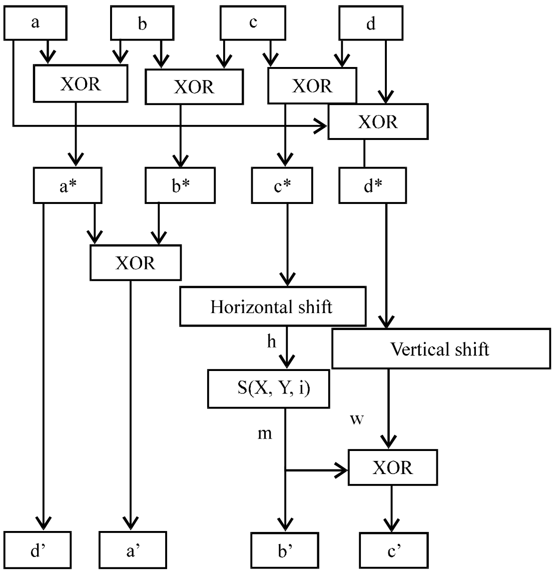

Fig. 3: Key generation process

16 keys are generated during 16 rounds. Originally the key is divided into four parts a-d of 128 bits each as shown in Fig. 3. Round key consist of a'-d' Algorithm 1.

New system algorithm:

```
1)  Divide the initial key into 4 parts : a, b, c, d of 128 bits each
2)  a* = a XOR b = d'
3)  b* = b XOR c
4)  c*= c XOR d
5)  d*=a XOR d
6)  a' = a* XOR b*
7)  Horizontal shift of c* part = h, in this left shifting will be done
8)  Result in step 7 will apply on  S-box = m = b'
9)  Vertical shift of d* = w in this up shifting will be done
10)  m and w will be XORed = c'
```

Here plaintext of 512 bits will get encrypted with the help of 512 bits key during 16 rounds as shown in Fig. 4.

Algorithm 2:

```
1)  $K_v = K_f \oplus R_i$
            $R_i$ = Round key
                    i = Number of rounds
             $K_f$ = Feedback value
2)  $K_{ni} = S_i| X*Y$  (Kv)
             $K_{ni}$ = Updated key
3)  $M_s$ = Si| X*Y(M)
4)  $M_p = R(M_s)$
5)  $M_n = M_p \oplus K_{ni}$
6)  $M* = S_i|X*Y(M_n)$
```

Decryption process is the reverse process of encryption. In horizontal shift, right-shift will be done instead of left-shift. In vertical shift, down-shift will be done instead of upper-shift (Pakshwar *et al*., 2013).

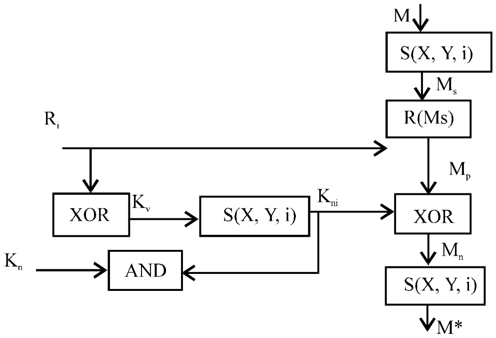

Fig. 4: Encryption process

CONCLUSION

This study has present two different cryptography algorithms. The message becomes more secure as different keys are used for every message. The hacker cannot determine the key if he knows the plaintext. It is simple and the delay time will be less than DES, 3DES, AES and RC6 algorithms because of no multiple functions used. The outsider attacks cannot know the key even if they have the plaintext and the cipher text. The algorithm will help the authentication protocols to reduce the delay taken by them and provide the channel the data security wanted.

REFERENCES

Amador, J.J. and R.W. Green, 2005. Symmetric key block cipher for image and text cryptography. Intl. J. Imaging Syst. Technol., 15: 178-188.

Daemen, J. and V. Rijmen, 2001. Rijndael the advanced encryption standard. Dobb=s J., 26: 137-139.

Pakshwar, R., V.K. Trivedi and V. Richhariya, 2013. A survey on different image encryption and decryption techniques. Intl. J. Comput. Sci. Inf. Technol., 4: 113-116.

Raj, R.M. and S. Anbu, 2014. Quantification of network security situational based awareness on neural networks. Asian J. Inf. Technol., 13: 755-760.

Ramesh, G. and R. Umarani, 2010. Data security in local area network based on fast encryption algorithm. Intl. J. Comput. Commun. Inf. Syst., 1: 85-90.

Ramesh, G. and R. Umarani, 2012. UR5: A novel symmetrical encryption algorithm with fast flexible and high security based on key updation. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 16-22.

Singh, G., 2013. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Intl. J. Comput. Appl., Vol. 67,.

Stallings, W., 2007. Network Security Essentials: Applications and Standards. Pearson Education India, London, UK., ISBN-13: 9788131716649, Pages: 432.