International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 3 421 – 423

A Novel Approach for Improving Privacy of Data Using Dynamic Key Generation

RAJESH KUMAR J N

Head of the Department,
Computer Science and Engineering,
Sree Sastha Institute of Engineering and Technology

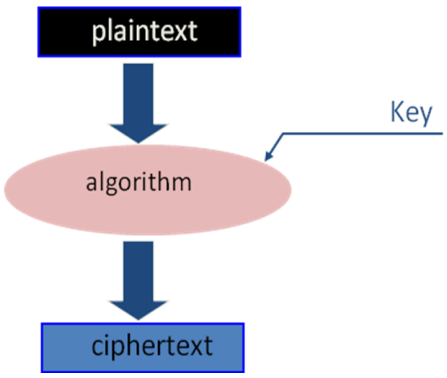
Abstract **-** In today's computer world security, integrity, confidentiality of the organization's data is the most important issue. This approach deals with the security of the data that organization manages and works with. It proposes a technique based on generating multiple numbers of keys to secure data using Data encryption standard (DES) and RSA algorithm. DES algorithm is used for encryption and decryption. RSA algorithm is used for key generation. The feature of such an approach includes high data security and high feasibility for practical implementation. This proposed methodology is helpful for hiding data in the applications like Online Transaction, Stock Maintenance, Payroll etc.

Keywords: *Dynamic Key Generation, RSA, Data Encryption Standard (DES)*

*****

I. INTRODUCTION

This proposed methodology is based on cryptography. In this a new technique in key generation using RSA algorithm is proposed. This technique is based on generating multiple numbers of keys. Initially it generate key for alphabets A-Z and numbers 0-9. Encryption is done by character wise for the given plain text using the key generated by RSA.



Then increase the number of the key which is almost equivalent to the number characters in the plain text. So that the key cannot be broken by any hackers and the data will be more secure.

II. PROPOSSED FRAMEWORK

Step 1: When the input is given, it orders the RSA to generate the key for alphabets A-Z and numbers 0-9.

Step 2: Key is automatically generated by RSA algorithm and stored in index.

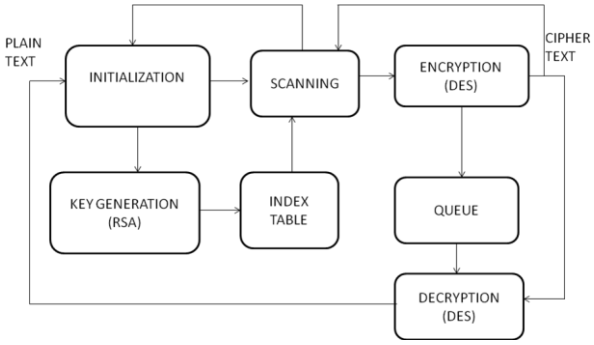
Step 3: Input is scanned by character wise and it fetch the corresponding key from index.

Step 4: Encryption is done by Data Encryption Standard (DES) algorithm by giving the scanned character and key from index has input.

Step 5: The key used in the DES are stored in the queue.

Step 6: Decryption is done by Data Encryption Standard (DES) algorithm by giving the scanned character and key from queue has input.

When a input (plain text) is given immediately key is generated for characters A-Z and numbers 0-9 using RSA key generation algorithm. The character and the corresponding keys are stored in the index table.



Now the plain text is start to scan in character wise. The scanned character and it corresponding key is fetched from the index, is given has a input for DES algorithm for encrypting the character. Similarly the next character is scanned and the process will goes on.

Based on the alphabetical order of the characters new keys are generated. For example: 'A' is the 1st alphabet, so for each appearance of 'a' new key is generated. 'B' is the 2nd alphabet,so for first two appearance of 'B' the key generated initially will be used then when 'B' appears 3rd time a new key will be generated and it will be used for 3rd and 4th appearance of 'B'. When 'B' appears 5th time new key will be generated. Similarly for the alphabet 'Z' after the 26 appearance of 'Z' a new key will be generated.

During the encryption process the key used for the encryption will be stored in the queue (FIFO).Because in decryption the first key will be used to decrypt the first character of the cipher text, and then next key will decrypt the next character and goes on.

Finally the cipher text (encrypted plain text) and the keys in the queue are sending to the receiver, where decrypt the cipher text to get back the plain text.

III. ALGORITHMS USED

RSA (Rivest,Shamnir,Adleman)

Rsa algorithm for key generation:

- Select two large prime numbers p, q
- Compute

  $n = p \times q$

  $v = (p-1) \times (q-1)$
- Select small odd integer k relatively prime to v gcd(k, v) = 1 Compute d such that

  $(d \times k)\%v = (k \times d)\%v = 1$
- Public key is (k, n)
- Private key is (d, n)

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

DES is a 64-bit block cipher. Both the plaintext and ciphertext are 64 bits wide.The key is 64-bits wide, but every eighth bit is a parity bit yielding a 54-bit key.

IV. CONCLUSSION

In this proposed a multiple numbers of keys are generated. Initially it generate key for alphabets A-Z and numbers 0-9. Encryption is done by character wise for the given plain text using the key generated by RSA. Therefore this proposed method of an encryption cannot be broken by brute force attack, timing attack and meet in middle attack. So the data is protected and improved the privacy of data.

V. REFERENCES

[1] William Stallings, "Cryptography and Network Securityprinciples and practices", Pearson / PHI.Third Edition.

[2] W.Mao,"Modern Cryptography-Theory and Practice", Pearson Education, Second Edition, 2007.

[3] Meiko Jensen, Jog Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society.

[4] C. Dubnicki, L. Gryz, L. Heldt, M. Kaczmarczyk, W.Kilian,P.Strzelczak,J.Szczepkowski, C. Ungurean, and M. Welnicki, "Hydrastor: A Scalable Secondary Storage," Proc. Seventh Conf. File and Storage Technologies (FAST), pp.197-210, 2009.

[5] Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04.

[6] M. Kiran Kumar, S. Mukthyar Azam, Shaik Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", International Journal of Network Security & its Applications, vol.2, No.4, Oct. 2010.

[7] Ateniese, S.Kamara, and J.Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc.15th Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp.319-333, 2009.

[8] A.Shamir, "How to Share a Secret," ACM Comm., vol.22,pp.612-613,1979.

[9] G.Ateniese, K.Benson, and S.Hohenberger, "Key-Private Proxy Re-Encryption," Proc. Topics in Cryptology (CT-RSA), pp.279-294, 2009.

[10] M.Mamboand E.Okamoto, "Proxy Crypto systems: Delegation of the Power to Decrypt Cipher texts," IEICE Trans. Fundamentals of Electronics, Comm. And Computer Sciences, vol.E80-A, no.1, pp.54 - 63, 1997.

RAJESH KUMAR J N received his BE and ME degrees in Computer Science and Engineering in the year 2002 and 2004. He published more than ten papers in various conferences. Currently he is doing research in JNTU, Kakinada, and Andhra Pradesh, India. He is working as Head In-charge of Computer Science and Engineering Department of Sree Sastha Institute of Engineering and Technology, Chennai, India.