ENCRYPTION TECHNIQUE FOR RELIABLE DATA TRANSMISSION IN MULTINODE NETWORK

Ajay Kakkar*

Abstract

Efficient encryption algorithm should consist of two factors; (i) fast response and ii) reduced complexity. Key selection techniques and analysis for security provision of multi-node network have attracted significant interests recently. The keys used for encryption/decryption process must be generated very carefully, if these keys are lost then the probability of recovering the data is very less. To enhance the security of the network and e-systems, this paper presents dynamic ID-based and ID based remote user authentication schemes which solves double-spending effectively along with the problem of loss of key during the transmission. The protocol's efficiency and security are also analyzed.

Key Words: *Encryption, Security, S-Boxes, Passwords.*

*Assistant Professor,Thapar University,Patiala

INTRODUCTION:

To achieve security various techniques are used such as passwords, encryption techniques, biometrics and many more, but out of all these cryptography with good encryption algorithm having large key length is used [1-3]. It is also important to calculate the number of bits required for the encryption; basically they provide the knowledge about the key length. Moreover in case of multiple S-Boxes different keys are used, although it creates a burden over the model but at the same time increases the security level. At present it is possible to break key having1028 word length (bits) with in 10 minutes that means increasing the length of key is just a time consuming process for the designer, not a reliable technique. So instead of increasing the key, multiple techniques are used where more then two functions are used to make the system optimized and reliable. i.e the output of first operation is given to the second and output of the second to the third and so on. Depending upon the requirement the numbers of levels (Round Functions) are taken. Combination of Public and private key cryptography results in modern key cryptography, widely used in abroad [4-5]. Security of electronic transaction protocol is an important research towards pushing electronic commerce, but the double-spending problem of off-line system will cause a great loss to the organizations. We know that user authentication mechanism is an important part of the network security to protect unauthorized access of a networked system. System-wide security is always required to make sure that data is safe. By using the information about timing, power consumption, and radiation of a device during the execution of a cryptographic algorithm; cryptanalysts have been able to break the system. So motive should be to make the combination secure [6-7]. Practical model consists of transmitters and other processing units capable to encrypt which is further transmitted over the channel (guided or unguided). The data rate is dependent on the bandwidth further affected by the noise and signal strength. Let us a take a model having User A and multiple intermediate stations $S_1, S_2 .... S_n$ and a receiver (User B) as shown in fig 1.

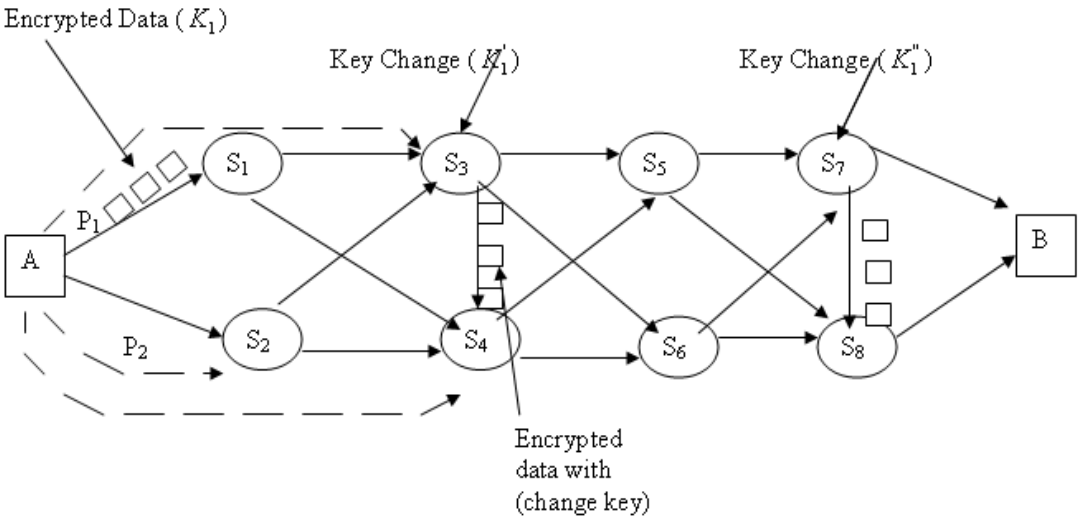

Figure 1: Multinode network having various stations

If K users transmitting the data (binary) simultaneously in a common band with a centre frequency f_c. Then the transmitted signal from the Kth user is:

$s_k(t) = \sqrt{2P} b_k(t) a_k(t) \cos(2\pi f_c t + \theta_k)$ .Where $P =$ the total power is available to each user, $b_k(t)$ is the data signal of the Kth user, consist of a rectangular pulse in the interval of $(rt, (r+1)T)$, The nth bit, $b_{k,n}$ in the Kth user is assumed to be ± 1 with equal probability and independent of all the bits, $b_{i,j}$. Then we can write the data signal for the Kth user:

$$b_k(t) = \sum_{r=\infty}^{\infty} b_{k,r}\, p(t - rt)$$

$$p(t) = 1, \quad 0 \le t \le T$$
$$= 0 \quad otherwise$$

The signal a_k is the periodic coded rectangular pulse having T second duration. The signal a_k is used to spread to the data signal b_k. The receiver for Kth user of station S_1 receives the signal

$$r_k(t) = \sqrt{2P} \sum_{q=1}^{L} \sum_{k=1}^{M} \beta_{kq}(t - \tau_{kq}) a_{kq}(t - \tau_{kq})$$
$$b_{kq}(t - \tau_{kq}) \cos(2\pi f_c t + \phi_{kq}) + n_k(t)$$

θ_k is the carrier phase uniformly spread over random variable $(0, 2\pi)$.

The output distribution function $F_o(y)$ of a station having different keys is given as $F_o(y) = \sum_{i=1}^{N} P(Y = X_{(i)} F_i(y)$, where X_i is the input to substation and $F_i(y)$ is the function of that particular substation having continuous and discrete input random variables.

Proof: $F_o(y) = P(Y \leq y, m_k)$ Where m_k is the mutually exclusive event $1 \leq k \leq N!$

$$F_o(y) = \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{k=1}^{N!} P(Y = X_{(i)}, Y = X_{(j)}, Y \leq y, m_k)$$

$Y = X_{(i)}$ & $Y \leq y$ are statically independent.

$$F_o(y) = \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{m_k \in m_{i,j}}^{N!} P(X_{(i)} \leq y, m_k)$$

$$F_o(y) = \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{m_k \in m_{i,j}}^{N!} P(m_k \left| X_{(i)} \leq y \right\rangle P(X_{(i)} \leq y)$$

$$F_o(y) = \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{m_k \in m_{i,j}}^{N!} \frac{1}{N!} P(X_{(i)} \leq y)$$

$$F_o(y) = \sum_{i=1}^{N} \sum_{j}^{N} \frac{P_{i,j}}{N!} P(X_{(i)} \leq y)$$

$$F_o(y) = \sum_{i=1}^{N} P(Y = X_{(i)} F_i(y)$$

Finally S-Boxes are used to encrypt the sequences obtained from both sections, leads to 32 bit encrypted data [8-10]. The only way this will make sense is if the same key is used to encipher/decipher multiple blocks.

1. If S_1=3 mod 5
2. Then output $a^{(m+1)/4}$mod k
3. Else $k_1 \in K_n$ (chosen randomly)
4. $k \leftarrow (P-1)/2; i \leftarrow 0, j \leftarrow \propto$
5. Repeat
6. $i \leftarrow j \bmod 5; j \leftarrow i \bmod 5$
7. If $a^i.b^j = 10 \bmod q$
8. Then $j \leftarrow j + (q+1)/5$

9. until $i \leftarrow j/10$

10. output = $a^{(i+1)/(j-1)} \bmod p$

The algorithm results in the multiple S-boxes which are given as:

The failure rate of 1st key high and the failure rate of second key is less. In the last attempt optimized and reliable combination is shown. In this combination the secured S-5 has been achieved.

	A	b	T_1	T_2		a	B	T_1	T_2		A	b	T_1	T_2
S_1	0.01	0.1	10	50	S_1	0.12	0.1	10	50	S_1	0.11	0.1	10	50
S_2	0.01	0.2	10	50	S_2	0.12	0.2	10	50	S_2	0.11	0.2	10	50
S_3	0.01	0.3	10	50	S_3	0.12	0.3	10	50	S_3	0.11	0.3	10	50
S_4	0.01	0.4	10	50	S_4	0.12	0.4	10	50	S_4	0.11	0.4	10	50
S_6	0.01	0.5	10	50	S_6	0.12	0.5	10	50	S_6	0.11	0.5	10	50
S_7	0.01	0.6	10	50	S_7	0.12	0.6	10	50	S_7	0.11	0.6	10	50
S_8	0.01	0.7	10	50	S_8	0.12	0.7	10	50	S_8	0.11	0.7	10	50

Table1: Failure Rate of 1st key is varied from (0.01-0.13); FR of 2nd key decreases (0.8-0.11)

	A	B	T_1	T_2		a	B	T_1	T_2		A	b	T_1	T_2
S_1	0.14	0.1	10	50	S_1	0.15	0.1	10	50	S_1	0.1	0.5	10	50
S_2	0.14	0.2	10	50	S_2	0.15	0.2	10	50	S_2	0.1	0.4	10	50
S_3	0.14	0.3	10	50	S_3	0.15	0.3	10	50	S_3	0.1	0.3	10	50
S_4	0.14	0.4	10	50	S_4	0.15	0.4	10	50	S_4	0.1	0.4	10	50
S_6	0.14	0.5	10	50	S_6	0.15	0.5	10	50	S_6	0.1	0.4	10	50
S_7	0.14	0.6	10	50	S_7	0.15	0.6	10	50	S_7	0.1	0.3	10	50
S_8	0.14	0.7	10	50	S_8	0.15	0.7	10	50	S_8	0.1	0.4	10	50

Table 2: Failure Rate of 1st key is varied from (0.01-0.13); FR of 2nd key decreases (0.8-0.11)

	A	b	T_1	T_2		a	b	T_1	T_2		A	b	T_1	T_2

S_1	0.11	0.8	10	50	S_1	0.12	0.8	10	50	S_1	0.11	0.8	10	50
S_2	0.11	0.7	10	50	S_2	0.12	0.7	10	50	S_2	0.11	0.7	10	50
S_3	0.11	0.6	10	50	S_3	0.12	0.6	10	50	S_3	0.11	0.6	10	50
S_4	0.11	0.5	10	50	S_4	0.12	0.5	10	50	S_4	0.11	0.5	10	50
S_6	0.11	0.3	10	50	S_6	0.12	0.3	10	50	S_6	0.11	0.3	10	50
S_7	0.11	0.2	10	50	S_7	0.12	0.2	10	50	S_7	0.11	0.2	10	50
S_8	0.11	0.1	10	50	S_8	0.12	0.1	10	50	S_8	0.11	0.1	10	50

Table 3: Failure Rate of 1st key is varied from (0.11-0.13); FR of 2nd key decreases (0.8-0.11)

	A	B	T_1	T_2		a	b	T_1	T_2		A	b	T_1	T_2
S_1	0.11	0.8	10	50	S_1	0.15	0.8	10	50	S_1	0.21	0.5	10	50
S_2	0.11	0.7	10	50	S_2	0.15	0.7	10	50	S_2	0.21	0.4	10	50
S_3	0.11	0.6	10	50	S_3	0.15	0.6	10	50	S_3	0.21	0.3	10	50
S_4	0.11	0.5	10	50	S_4	0.15	0.5	10	50	S_4	0.21	0.4	10	50
S_6	0.11	0.3	10	50	S_6	0.15	0.3	10	50	S_6	0.21	0.4	10	50
S_7	0.11	0.2	10	50	S_7	0.15	0.2	10	50	S_7	0.21	0.3	10	50
S_8	0.11	0.1	10	50	S_8	0.15	0.1	10	50	S_8	0.21	0.4	10	50

Table 4: Failure Rate of 1st key is varied from (0.11-0.13); FR of 2nd key decreases (0.8-0.11)

Node = 5, S-Boxes= 16, for S_5

S. No.	Data Length	Key Length	S-Boxes	Processing time (ns)	Hacking Time (min)
1.	26	8	16	19.35	78.71
2.	56	8	16	23.43	81.40
3.	56	16	16	41.54	32.41
4.	124	8	16	43.25	76.09
5.	256	8	16	65.73	98.75

Table 5: processing and hacking time for station S_5

For the same parameters, the combination of 16 bit key length and 16 S-Boxes provides 19.95 minutes (table 3.5) to the hacker. It has been observed from the results of tables (3.2-3.5) that:

- By increasing number of nodes the processing time is increased.
- If numbers of nodes are increased then it takes more processing time.
- It also provides enough time to the hacker.
- If there is an increase in the data length then hacking and processing times are increased.
- By increasing key length the hacking time is reduced.
- Increase in the number of S- Boxes reduces the hacking time with nominal increase in processing time.

So, correct combination of key length and S- Boxes is selected in order to achieve optimized efficient results.

CONCLUSION AND FUTURE SCOPE

Design issues are not easy to adopt, depending upon the nature they are taken. We always design the system by keeping an eye on the worst case. The algorithm used in the paper shows that all the stages are mutually independent from each other, provides the facility to use compression and re-encryption techniques. From the table 1-4 it is quite clear that the less encryption time is obtained if multiple keys are used and they have different failure rates.

REFERENCES

[1] A. Banerjee, L. Drake, L. Lang, B. Turner, D. Awduche, L. Berger, K. Kompella, and Y. Rekhter (July 2001), "Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques," IEEE Communication Magazine, Vol. 39, No. 7, pp. 144-151.

[2] A. Bobbio and K.S. Trivedi (1990), "Computing Cumulative Measures of Stiff Markov Chains Using Aggregation," IEEE Transaction on Computers, Vol. 39, No. 10, pp. 1291-1297.

[3] A. Reibman and K.S. Trivedi (1988), "Numerical Transient Analysis of Markov Models," Computers and Operations Research, Vol. 15, No. 1, pp. 19-36.

[4] Alexander Chatzigeorgiou ,George Stephanides, Spyros T. Halkidis, Nikolaos Tsantalis (September 2008), "Architectural Risk Analysis of Software Systems Based on Security Patterns" IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 129-142.

[5]B. Livshits and M.S. Lam (Aug. 2005), "Finding Security Vulnerabilities in Java Applications with Static Analysis," Proceedings of 14th Usenix Security Symposium pp. 19-36.

[6] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K.S. Trivedi (March, 2004), "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems," Performance Evaluation, Vol. 56, No1, pp. 167-186.

[7]Blake, I.F. and Kolesnikov, V. (2004) 'Strong conditional oblivious transfer and computing on intervals', in P.J. Lee, (Ed). *ASIACRYPT'04*, Volume 3329 of *Lecture Notes in Computer Science*, Springer, pp.515–529.

[8]Blake, I.F. and Kolesnikov, V. (2006) 'Conditional encrypted mapping and comparing encrypted numbers', in G. Di Crescenzo and A. Rubin, (Eds). *FC 06*, Volume 4107 of *Lecture Notes in Computer Science*, Springer, pp.410–421.

[9] D. Liu and P. Ning (October 2003), "Establishing Pair-wise Keys in Distributed Sensor Networks," Proceedings of 10th ACM Conference on Computer and Communication Security (CCS '03), pp. 52-61.

[10] Elisa Bertino, Ning Shang, and Samuel S. Wagstaff Jr. (April 2008) "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp-65-70.