Modification of Symmetric-Key DES into Efficient Asymmetric-Key DES using RSA

Prerna Mohit
Indian school of mines
Dhanbad
Jharkhand, 826004
prernamohit@outlook.com

G.P. Biswas
Indian school of mines
Dhanbad
Jharkhand, 826004
gpbiswas@gmail.com.com

ABSTRACT

In this paper, we propose a new approach for DES based on public key cryptography called Asymmetric-DES. Where hybrid of DES and RSA algorithm are combine and found to be secure for only two rounds, whereas symmetric DES is secure for sixteen rounds with different combination of key. Thus, we modified the structure of DES and applies RSA encryption on plaintext with the public key of receiver to obtain the cipher text. Similarly the modification is performed in decryption algorithm. As a result breaking of two-round asymmetric DES is hard problem, as its security depend on RSA algorithm.

Keywords

DES; RSA; symmetric key; public key; cryptography

1. INTRODUCTION

With the rapid development of the computer and network technology, the security of information transmitted on the Internet will become more challenging, therefore a new branch of science is introduced called cryptography. Which mainly consist of two type: symmetric key cryptography and asymmetric key cryptography. In addition the requirements for cryptography are: confidentiality, data integrity, authentication and Non-repudiation. Confidentiality is the process of protecting the message from the unauthorized user and maintained by encryption/decryption. Similarly, the integrity of data insure that alteration of data is impossible and provided by digital signature.

The symmetric cryptography is very efficient for encrypting informations, as it is faster and is not being subjected to choose-ciphertext attacks, But the management of key ia always a crucial problem [1]. The Public-key cryptography, solves the problem of symmetric-key, as it is effective for key management. In addition data authentication is one of the feature of public-key, where key are paired one for encryption (public key) and one for decryption (private key) [2]. In practical symmetric and asymmetric cryptosystem are united to get the advantage of each other. Here, a different concept is proposed to convert the symmetric-key DES into Asymmetric-key DES.

There are several methods have been proposed in order to modify the original DES. In 1996 Seung-Jo Han [15] increases the digits of DES from 64-bit to 96-bit and divides the input block into 3 sub-blocks of 32-bits, with increase size of key from 64-bits to 128-bits for showing that improved DES is stronger than original DES but the performance of improved DES is not enhanced as compare to growth in its computational cost. After several years in 2010 Mohammed and Alani design DES variant with 96-bits key, in which the system has inbuilt S-box in the key generation algorithm which can oppose brute-force attack. On the other hand the Hardware implementation of DES is shown by Shahid and Arich [5] [8]. In 2004 Song and Zhang [9] presented an attack on four-round DES using Genetic Algorithm (GA) for the cryptanalysis of substitution cipher. In 2013 [3] Sombir proposed a scheme in which he combine transposition technique with DES and perform comparison between DES and RSA cryptosystem [7]. However, there are many variations of DES are shown in [4] [10] [17].

Some of the security attacks on DES is being found. In 1997 for the first time breaks a message encrypted with DES is performed [11]. After one year a U.S based organization Electronic Frontier Foundation (EFF) built a machine which performs brute force on DES key and breaks DES key in 56 hours [12]. Similarly, in 1999 with the joint effort of EFF and distributed.net breaking of DES key is performed in 22 hours and 15 minutes [13]. Hence DES is considered as insecure cryptography and is not being, use for encryption/decryption of data.

In this paper, we proposed the hybrid of DES and RSA cryptosystem to convert symmetric DES into the asymmetric DES system for short message of 64-bits. The RSA key is use in the structure of DES by dropping the DES key generation. The detail of scheme is describe in section 3.

The rest of the paper is organized in this way: Section 2 will give brief introduction to the existing symmetric DES and RSA public key cryptography. Section 3 introduces the proposed symmetric DES modification to asymmetric DES followed by section 4 presents the security analysis of the new scheme over existing scheme and finale the conclusion in section 5.

2. PRELIMINARY

In this section, we define the existing symmetric DES and asymmetric RSA cryptosystem in detail, as the basic module

ICTCS '16, March 04-05, 2016, Udaipur, India
 ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905352

for the construction of new asymmetric DES.

2.1 Data Encryption Standard (DES)

The Data Encryption Standard is the first and most widely known symmetric key cryptography, developed by the joint work of the National Bureau of Standards (NBS), National Security Agency (NSA) and IBM in 1977 [5] [6]. The structure of DES is a block cipher, which divide the plaintext message into groups of 64-bits input-text with same numbers of keys and among 64-bit key eight bits are removed as parity bits. Hence, efficiently key size is 56-bits. Which would take a maximum of 256, approximately 7.6×10^6 attempts to find the correct key [6]. Hence brute-force attack is easy with limited numbers of keys. The basic model of Feistel structure is used, which divides the plaintext message into two halves of 32-bit left (L_i), right (R_i) and perform 16 rounds of identical operation with different keys K_i where $i \in \{1, 2...16\}$, as it is found that less than sixteen rounds makes it insecure and more than 16 rounds increase its computation cost. Fig 1 show one round of DES and the encryption operation can be formulated as:

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

$L_i = R_{i-1}$

Similarly the decryption operation with reverse order of key can be formalized as:

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus F(L_i, K_i)$

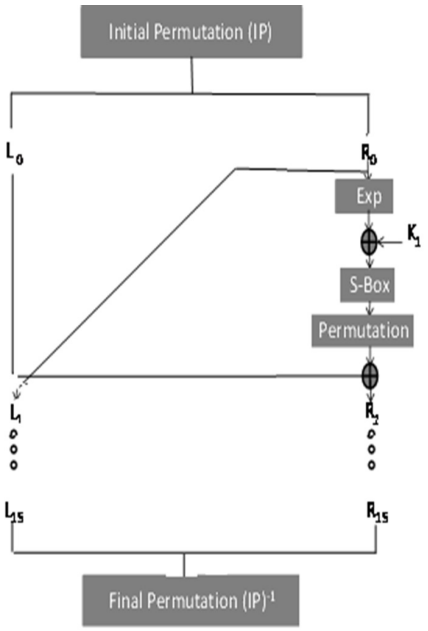

Figure 1: One round of DES Encryption.

2.2 RSA algorithm

One of the useful public key cryptosystem, RSA was named after its inventor Ron Rivest, Adi Shamir and Len Adleman in the year 1977 [14] is most wide known cryptographic scheme and based on the fact that it is easy to find large prime numbers and multiply it but difficult to factorization semi prime numbers. Therefore, RSA algorithm is based on factorization problem. In addition, RSA cryptography uses large numbers and considered as secure for 512-bit. There are some of the variations of RSA such as Batch RSA, Multifactor RSA, Rebalanced RSA was designed to speed up the RSA decryption and to provide strength in the existing system [16]. The RSA algorithm has three stages: key generation, encryption and decryption, described below:

1. Key Generation
   (a) Select two prime number p and q and compute $n = p \times q$.
   (b) Calculate the EulerâĂŹs function $\phi(n) = (p-1) \times (q-1)$
   (c) Choose e such that e is relatively prime to $\phi(n)$.
   (d) d is determined as multiplicative inverse of e with respect to $\phi(n)$
2. Encryption
   By getting public-key $\{e, n\}$ from key generation, the sender encrypts the message as $C = M^e$ mod n, where $M < n$,
3. Decryption
   After getting cipher-text C and its private key $\{d, n\}$ receiver can decrypt the cipher-text as $M = C^d$ mod n.

3. PROPOSED ASYMMETRIC-KEY DES

As we know the symmetric structure of DES is used between two remote parties to share a secret key for encryption/decryption of messages, where common secret key is shared via secure channel. On the other hand RSA public key cryptosystem generates public, private key pair for encryption, decryption of messages. Hence, we propose a new technique to incorporate both the scheme for generation of a new scheme, which consist of DES structure and RSA key generation in place of DES round key generation and named as asymmetric DES. As our scheme convert the symmetric DES structure to asymmetric DES structure using RSA algorithm and found to be secure for two rounds. The detail is described below and shown in fig 2, 3.

Assume two party's, where A and B are respectively encrypting and decrypting for communication of secure messages between them. The Asymmetric-Key DES algorithm works as:

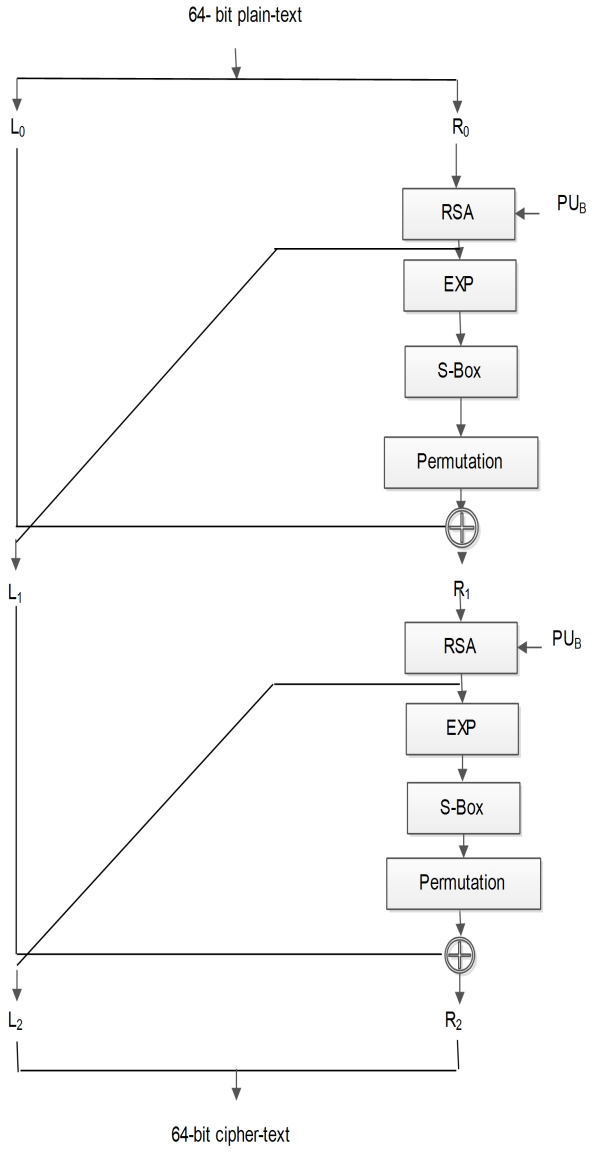

Figure 2: Proposed Encryption of Asymmetric-Key DES.

Encryption equation

$$Li = E_{RSA}(R_{i-1})$$
$$Ri = L_{i-1} \oplus F(R_{i-1}, e)$$

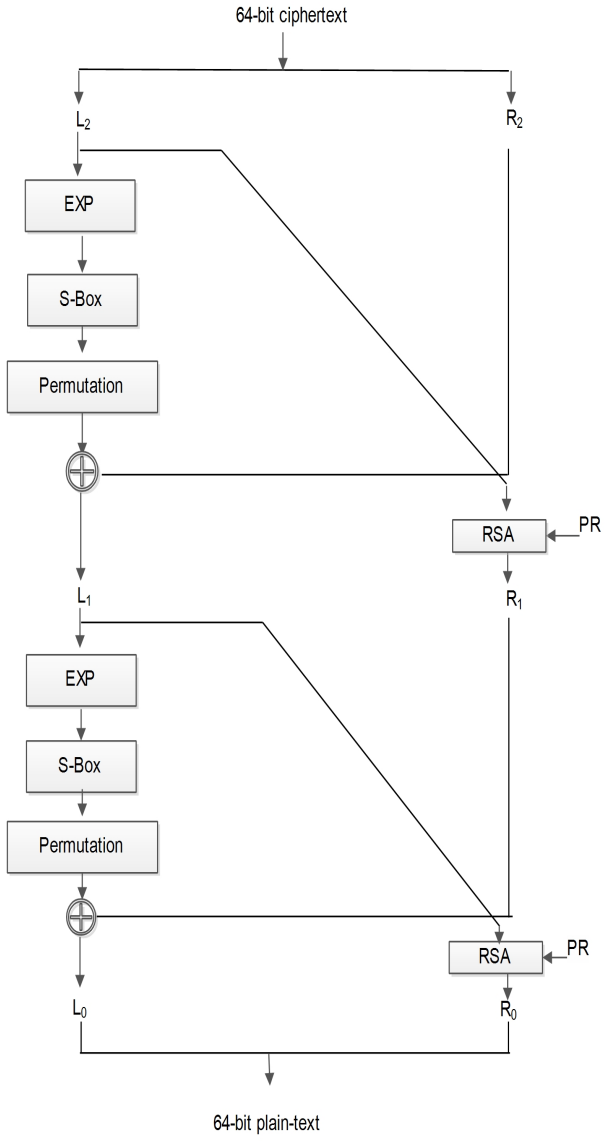

Figure 3: Proposed Decryption of Asymmetric-Key DES.

Decryption equation:

$$L_{i-1} = R_i \oplus F(L_i)$$
$$R_{i-1} = D_{RSA}(L_i)$$

Encryption by User A	**Decryption by User B**
1. Divide the input it into two parts L_0R_0 2. Compute $C_1 = R_0^e mod\ n$ 3. Apply function (Expansion, S-box, Permutation) on C_1 4. The next round input (R_1, L_1) are computed as Right half is $R_1 = L_0 \oplus F(C_1)$ and Left half is $L_1 = C_1$ 5. Again repeat step (2) to (4) to get C_2, R_2, and L_2. 6. Concatenate $L_2 \| R_2$ to get final cipher text C.	
$\xrightarrow{\langle C \rangle}$	
	1. Divide the cipher text C into two parts L_2, R_2 2.The next round right half is computed as $R_1 = L_2^d mod n$ 3.Apply function (Expansion, S-box, and Permutation) on L_2 4. Compute $L_1 = R_2 \oplus F(L_2)$ 5.Again repeat step (2) to (4) to get R_0, and L_0. 6.Concatinate $L_0 \| R_0$ to get plaintext.

As shown the public and private key pair (e, d) are used to provide confidentiality in data. In the same way digital signature can be applied to provide authentication (using private and public key pair) for signature generation and verification. Hence, Asymmetric- DES can be used to implement digital signature as well. whereas the same is not supported in symmetric DES. In order to perform digital signature, the signature is perform by the receiver and verification is performed by sender, whereas the process are same as in the case of confidentiality. But, private key d is use for signature generation and public key e is use for verification operation.

4. SECURITY ANALYSIS

As stated in the previous section, there are many attempts to break the security of existing DES is found, and to prevent it from different attack. We modify the structure and integrate the existing DES with RSA algorithm, to form a secure cryptosystem. It is known that DES with short key of 56/64-bits are not secure, however RSA with modulous $n \geqslant 512-$bits made the system secure where n is product of two prime number. The hardness of RSA cryptography depends on following parameter:

- Factorization problem where factorization of n into prime p, q
- Determination of $\phi(n)$ directly without knowing p, q.
- Determination of d directly

It is known that the processing overhead of public-key is higher then symmetric-key. However we are encrypting only 64-bit messages which is very small and instead of sixteen rounds only two rounds are used. Thus, processing overhead of Asymmetric-key DES is relatively same with the existing DES. The computation of right half involves:

$$R_1 = L_0 \oplus S - Box(Exp(E_{PU_B}(R_0)))$$

$$R_2 = E_{PU_B}(R_0) \oplus S - Box(Exp(E_{PU_B}(R_1)))$$

From these equation it is clear that R_2 involves seven encryption/security operations to obtain plaintext R_0. The first operation is encryption of R_0 with the public key of B, in addition expansion operation provide recombination of encrypted bits. The second secure process involve *S-Box* operation, followed by XOR with L_0. Where S-Box provide similar operation like in symmetric encryption and act as a non-linear operate in asymmetric-key DES. After that the obtain value of R_1 is encrypted with public key of B, again the *S-Box* operation and XOR with encrypted R_0 is applied. Hence to break seven security protection to obtain R_0 is not feasible. Similarly the left half operation includes:

$$L_1 = E_{PU_B}(R_0)$$

$$L_2 = E_{PU_B}(R_1)$$

During the computation of L_2 four security operations are performed where three encryption is involved in the computation of R_1 and fourth encryption is performed on the obtained value of R_1. Where R_1 and L_1 are intermediate values and not known to the third party.Thus, the proposed Asymmetric-DES as a whole is secured.
On the other hand the detail encryption equation of traditional DES for right and left halves are:

$$R_i = L_{i-1} \oplus S - Box(DES_{key} \oplus Exp(R_{i-1}))$$

$$L_i = R_{i-1}$$

In this the previous round right half directly, become the next rounds left half without any change. Where the right half performs two XOR operations, one S-box computation and the DES key encrypt. The brute force attack on DES make the system weaker. In addition, expansion operation is the re-use of the same bits in a different order.

5. CONCLUSION

In this paper, an improved and secure version of DES has been developed. Which inclusion conversion of symmetric DES to asymmetric DES using RSA cryptosystem. That will provide greater security to the existing DES structure with two rounds of identical operations under RSA encryption/decryption which increase slight computation with great increase in the security of asymmetric DES structure. The same idea (symmetric DES + RSA) can be use to provide authentication as well. The structure can further be modified to provide confidentiality with authentication for secure communication.

6. REFERENCES

[1] B. Schneier. Applied Cryptography, (third ed.)Wiley, New York 1996.

[2] P. Mohit, G. P. Biswas. Design of ElGamal PKC for Encryption of Large Messages. 2nd IEEE International Conference on Computing for Sustainable Global Development,2015.

[3] S. Singh, S. K. Maakar, S. Kumar. Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques. International Journal of Advanced Research in Computer Science and Software Engineering 3(6), pp. 464-471. 2013.

[4] A. M. Sisin, B.T. Tanguilig, D. Bobby, B. D. Gerardo, Y. Byun. An improved Data Encryption Standard to Secure Data using Smart Cards. Ninth International Conference on Software Engineering Research, Management and Applications 2011.

[5] B. Shahid, H. Tauqeer, M.S. Ilyas. Hardware Implementation of DES Encryption Cracker. Student Conference on Engineering Sciences and Technology, 2005.

[6] M.E. Smid, D. K. Branstad. The Data Encryption Standard: Past and Future. Proc. of the IEEE. Vol. 76, No. 5, pp. 550-559, 1988.

[7] S. Singh, K. Sunil , S. K. Maakar, S. Kumar. A Performance Analysis of DES and RSA Cryptography. International Journal of Emerging Trends and Technology in Computer Science, volume 2, Issue 3, 2013.

[8] T. Arich, M.Eleuldj. Hardware implementations of the Data Encryption Standard. 14th IEEE International Conference on Microelectronics 2002.

[9] J. Song, H. Zhang, Q. Meng, Z. Wang. Cryptanalysis of Four-Round DES Based on Genetic Algorithm. International Conference on Wireless Communications Networking and Mobile Computing, Issue 21-25, pp. 2326-2329, 2007.

[10] M. M. Alani. DES96 - Improved DES Security. 7th International Multi-Conference on Systems, Signals and Devices, 2010.

[11] M. Curtin, J. Dolske. A Brute Force Search of DES Keyspace. 1998.

[12] Electronic Frontier Foundation: Cracking DES : Secrets of Encryption Research, Wiretap Politics and Chip Design. OâĂŹReilly. (May 1998)

[13] R.Clayton, M. Bond. Experience Using a Low-Cost FPGA Design to Crack DES Keys. Cryptographic Hardware and Embedded Systems - CHES, Volume 2523 of the series LNCS pp. 579-592 2002.

[14] R.L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21, pp.120-126, 1978.

[15] S. Han, H. Heang-Soo Oh, J. Park. The improved Data Encryption Standard (DES) Algorithm. 4th IEEE International Symposium on Spread Spectrum Techniques and Applications Proceedings, 1996.

[16] Y. Lu, R. Zhang, D. Lin. Factoring multi-power RSA modulus $N = p^r q$ with partial known bits. In: Information Security and Privacy, pages 57-71. Springer, 2013.

[17] W. Ren. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication.In: Second International Conference on Modeling, Simulation and Visuali-zation Methods WMSVM, 2010.