Survey of Hybrid Encryption Algorithm for Mobile Communication
Ishita Bhatia¹ Nishit Mishra²
¹,²B. E. (C. S. E.)
¹,²Sanghvi Institute of Science & Management, Indore

Abstract— To enhance the security of data transmission in Mobile communication, a hybrid encryption algorithm based on DES and RSA is proposed. The currently used encryption algorithm employed to protect the confidentiality of data during transport between two or more devices is a 128-bit symmetric block cipher. In the proposed hybrid encryption algorithm, DES algorithm is used for data transmission because of its higher efficiency in block encryption, encryption speed of DES algorithm is faster than RSA algorithm for long plaintext, and RSA algorithm distribute key safely and easily also RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission in mobile communication system will be more secure. Meanwhile, it is clear that the procedure of the entire encryption is still simple and efficient. Digital abstract algorithm MD5 is adopted in this mechanism. Through comparing the digital signature which is transmitted by dispatcher and digital signature result of plaintext which is got by receiver through MD5 algorithm, data security can be guaranteed. This mechanism realizes the confidentiality, completeness, authentication and non-repudiation.

Key words: DES; RSA; MD5; digital signature; hybrid encryption

I. INTRODUCTION
Communication is one of the integral parts of science that has always been a focus point for exchanging information among parties at locations physically apart. After its discovery, telephones have replaced the telegrams and letters. Similarly, the term ‘mobile’ has completely revolutionized the communication by opening up innovative applications that are limited to one’s imagination. Today, mobile communication has become the backbone of the society. All the mobile system technologies have improved the way of living. Its main plus point is that it has privileged a common mass of society. As mobile communication has become essential part of our society, it is very necessary to secure the mobile communication. To secure the mobile communication we are proposing a hybrid encryption algorithm which is based on DES and RSA encryption algorithm. It also includes MD5 and digital signature for secure mobile communication.

A. Hybrid Encryption
A method of encryption that combines two or more encryption schemes and includes a combination of symmetric and asymmetric encryption to take advantage of the strengths of each type of encryption is known as Hybrid Encryption.

We are using an algorithm which is combination of DES (data encryption standard) and RSA (Rivest Shamir Adleman) algorithms. Digital abstract algorithm MD5 is also included in this mechanism to protect safe transmission of information.

B. Need of Hybrid Encryption
In our research we are proposing a combination of both DES and RSA as a hybrid link for both protocols. This is done to enhance the hardness in security by combining the RSA and DES encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing so we will put our efforts into encryption area for RSA algorithm with DES along with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm.

II. BACKGROUND & RELATED WORK
A. RSA Algorithm
The RSA public key cryptosystem was invented by R. Rivest, A. Shamir and L. Adleman. The RSA cryptosystem is based on the dramatic difference between the ease of finding large primes and the difficulty of factoring the product of two large prime numbers (the integer factorization problem). For the RSA cryptosystem, we first start off by generating two large prime numbers, ‘p’ and ‘q’, of about the same size in bits. Next, compute ‘n’ where n = pq, and ‘x’ such that, x = (p -1)(q-1). We select a small odd integer less than x, which is relatively prime to it i.e. gcd (e, x) = 1. Finally we find out the unique multiplicative inverse of e modulo x, and name it ‘d’. In other words, ed = 1 (mod x), and of course, 1 < d < x. Now, the public key is the pair (e, n) and the private key is d. Suppose Bob wishes to send a message (say ‘m’) to Alice. To encrypt the message using the RSA encryption scheme, Bob must obtain Alice’s public key pair (e, n). The message to send must now be encrypted using this pair (e, n). However, the message ‘m’ must be represented as an integer in the interval [0,n-1]. To encrypt it, Bob simply computes the number ‘c’ where c = m ^ e mod n. Bob sends the cipher text c to Alice. To decrypt the cipher text c, Alice needs to use her own private key d (the decryption exponent) and the modulus n. simply computing the value of c ^ d mod n yields back the decrypted message (m).

B. DES Algorithm
DES algorithm synthetically makes use of many cryptography technologies which include replacement, alternation and data input. It is a product cryptogram. Plaintext is divided into many blocks when encryption begins. Each block has 64 bits and the length of key is 64 bits. The valid length is 56 bits and the rest 8 bits are used for parity checking. First, 64 bits data is divided into two parts after initial replacement. Each part includes 32 bits. Then iterative process began. Right half 32 bits are extended to 48 bits. The result exclusive or with 48 bits sub-key
which is got from 64 bits keys. The result is compressed as 32 bits through s box. After replacement, the 32 bits data exclusive or with left 32 bit data which is got from the beginning of replacement. Right half part of the new round is got. At the same time, the result is regard as the parameter of new round. After 16 round replacements, a new 64 bits data is generated. There is one step we must pay attention to. The two results of last round do not exchange. The encryption and decryption can use the same algorithm through this process. To the last, the 64 bits result needs an inverse replacement. The 64 bits cipher text is got.

C. Digital Abstract algorithm MD5
Message-Digest refers to hash transformation of message. MD5 algorithm gets the remainder (64 bits) of the primitive plaintext through mod 2^64. The result is added to the end of Message. The MD5 code includes the length information of the message. Some message whose range of bits from 1 to 512 is added into the place which is between message and remainder. After filling, the total length is several times of entire 512. Then the whole message is divided into some data blocks. Each of them includes 512 bits. The data block is further divided into four small data blocks which include 128 bits. The small data block is input into hash function to perform four round calculations. In the end, MD5 message abstract is got. Digital signature can achieve following three points: receiver could check the signature of message which is sent by dispatcher. Dispatcher cannot deny the signature of message. Receiver cannot fake the signature. In our research we are proposing a combination of both DES and RSA as a hybrid link for both protocols. This is done to enhance the hardness in security by combining the RSA and DES encryption algorithms by adding some more security codes. Encryption is the vital part of information sharing so we will put our efforts into encryption area for RSA algorithm with DES along with digital abstract algorithm MD5 so that we can make security harder by giving a hybrid algorithm.

III. METHODOLOGY CONCEPT
We have implemented the Privately Protected Public key cryptosystem for the 128 bit data encryption with the help of the Combinational approach of the RSA and DES Algorithm and also as the supporting tool is like Message Digest. We focus on the console mode implementation here, and leave the GUI implementation for a later section of this report. The console application uses a 128 bit Data Encryption implementation, which is adequate for non-critical applications. By a simple modification of the source code, higher bit-strengths may be easily achieved, albeit with a slight performance hit. For that purpose we prepare the algorithm for the Implementation and their steps are below.

A. Algorithm

1) SENDING SIDE
   Step. 1 : Find MD of 128 bit of data which you want to send
   Step. 2 : Calculate 2’s complement of data which you want to send
   Step. 3 : Calculate XOR of 2’s complement of data and MD
   Step. 4 : Encrypt the resultant data of the above step through 128 RSA
   Step. 5 : Apply DES to Encrypt the MD of the data
   Step. 6 : Send 256 bit (send encrypted data using RSA[128] and encrypted MD[128] using MD5)
   (You can send 256 bit for every 128 bit data or send encrypted MD only ones for a session)

2) RECEIVING SIDE
   Step. 1 : Get 256 data for the decryption purpose
   Step. 2 : Decrypt MD using DES
   Step. 3 : Decrypt data through RSA
   Step. 4 : Take XOR with decrypted data and decrypted MD
   Step. 5 : Take 2’s Complement of resultant

B. Block Diagram of the System

C. Receiving Side

This algorithm applied on the both sending and the receiving side and then we get the efficient method for the encryption and decryption.
D. The advantages of hybrid encryption algorithm

1) Using RSA algorithm and the DES key for data transmission, so it is no need to transfer DES key secretly before communication;  
2) Management of RSA key is the same as RSA situation, only keeps one decryption key secret;  
3) Using RSA to send keys, so it can also use for digital signature;  
4) The speed of encryption and decryption is the same as DES. In other words, the time-consuming RSA just do with DES keys.

IV. CONCLUSIONS

Today, mobile communication has become the backbone of the society. All the mobile system technologies have improved the way of living and its main plus point is that it has privileged a common mass of society. Also mobile communication has completely revolutionized the communication by opening up innovative applications that are limited to one's imagination. Also mobile communication has not fully considerate security issues in the standardization process just because it uses wireless channel for transmission medium. Compared to fixed network mobile communication is more vulnerable to be attacked. For the applications that take data security as priori, achieving a high level of data security is essential. But currently, there exists no such encryption algorithm used for mobile communication so we are proposing the DES and RSA hybrid encryption algorithm that is more secure and easier to achieve, thus ensures safety and real time data transmission in mobile communication systems. It makes use of DES which has high encryption speed for plaintext. It also develops the merit of RSA which manages the key easily. The receiver can verify whether the information is tampered in network through using MD5 algorithm. This mechanism realizes the confidentiality, completeness, authentication and non-repudiation. It is an effective method to resolve the problem of secure mobile communication.

REFERENCES

[1] Elichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval and Jacques Stern, RSAOAEP is secure under the RSA assumption, Journal of Cryptology, 2002