RSA and Triple DES based Combined Secured Approach to Ensure Data Security

Ditee Yasmeen[1]

Abstract- Data security is a key concern of today's worlds. Data security is critical for most businesses and even home computer users. Client information, payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences. Cryptography techniques employ to ensure data security in this regard. For this, RSA and Triple DES technique has been studied, realized and implemented with strong authentication, confidentiality and message integrity. First, the key pairs have been generated for the users to perform the encryption and decryption. Public key pair (e, n) is used for encryption and for decryption corresponding private key pair (d, n) is used. For key generation, first select two large primes: p, q, and compute the modulo factor, n =p x q and, calculate the totient factor, Ω(n)= (p-1) x (q-1). All the co-primes are listed for this totient. Then two co-prime e and d are chosen with property that e d =1+k Ω(n). Generated key pair (e, n) is used as public key and (d, n) is used as private key. The plaintext message M is processed with a hash digest X, produced by X-OR, a hash function and appended it with M, which is then encrypted with the sender's own private key to generate cipher text C. Then C is further encrypted using triple DES encryption algorithm along with a secret key K_S. The secret key K_S is also encrypted with the receiver's public key. The encrypted secret key along with the encrypted data is sent to the destination. In the receiver end, the received encrypted secret key K_S is first decrypted using receiver's private key and then encrypted data is decrypted with K_S that generates cipher text C. C is now further decrypted using sender's public key to obtain original message M and a hash digest X. Then the receiver applies the X-OR function repeatedly to generate a hash digest X' and compare it with received digest X to ensure data integrity. The use of the secret key establishes the strong confidentiality and the uses of the sender's private key ensure the authentication by creating digital signature. The proposed system can be applied for many cryptographic applications like business transaction, small organization, file transaction etc. where strong security is highly demanded.

Keywords- Cryptography, Network Security, Modular Arithmetic, RSA, Triple DES, Hash Function, Message Digest, Data Breaches, and Data Security.

1 INTRODUCTION

Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users [6]. Data is an asset that has a value like any other asset. The requirements of data security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security information felt to be valuable to an organization was provided primarily by physical and administrative means. Until a few decades ago, the data collected by an organization was stored on physical files. The confidentiality of the files was achieved by restricting the access to a few authorized and trusted people in the organization. And only few people had authorized to modify the contents of the file Availability was achieved by permitting one person had an access to the files at all times. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is computer security. The introduction of distributed systems and the use of network and communications facilities for carrying data between terminal user and computer and between computer and computer also enhance the need of security. Network security [1][2] measures are needed to protect data during transmission.

2 DATA SECURITY

Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users. In 2013, there were 619 notable data breaches. Large organizations that manage retail, financial, health, legal, and government data are probably what come to mind first. However, a data breach can affect businesses of varying sizes and industry. Data breaches that happen to large organization are considered more newsworthy and are highly publicized. A report by Verizon paints a more accurate picture. According to the report, small businesses were victims of data breaches 54% of the time in 2012. The three important reasons to make data security a priority for a business is reputation is at stake, rebounding can be costly and the threats are only increasing [6]. Thorough data security begins with an overall strategy and risk assessment. This will enable us to

- *Ditee Yasmeen, Senior Lecturer, Institute of Science and Technology, Dhaka, Bangladesh. E-mail: ditee.yasmeen@yahoo.com*

identify the risks that are faced with and what could happen if valuable data is lost through theft, malware infection or a system crash. Other potential threats needed to identify include the following:

· Physical threats such as a fire, power outage, theft or malicious damage [5]

· Human error such as the mistaken processing of information, unintended disposal of data or input errors

· Exploits from corporate espionage and other malicious activity

Here are several aspects that need to be considered:

· Just who has access to what data

· Who uses the internet, email systems and how they access it

· Who will be allowed access and who will be restricted

· Whether or not to use passwords and how they will be maintained

· What type of firewalls and anti-malware solutions to put in place

· Properly training the staff and enforcing data security.

After the above analysis, one can then prioritize specific data along with more critical systems and determine those that require additional security measures. It is also a good idea to lay out a BCP (Business Continuity Plan) so that organization's staff is still able to work effectively if the systems happen to fail. Company risks and security implementations should be reviewed frequently to support changes such as the growth of business and other circumstances.

3 RSA

RSA is the most popular public-key cryptosystem. The algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters RSA are the initials of their surnames, listed in the same order as on the paper. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations [10]. RSA involves two keys: a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. RSA [9][11] uses exponentiation modulo a product of two large primes to encrypt and decrypt, performing both public key encryption and public key digital signature, and its security is connected to the presumed difficulty of factoring large integers, a problem for which there is no known efficient general technique.

For example, two persons, X and Y, send a secret message through the public mail. X wants to send a secret message to Y, and expects a secret reply from Y. Y and X have separate padlocks. First, X asks Y to send her open padlock to him through regular mail, keeping her key to himself. When X receives it he uses it to lock a box containing his message, and sends the locked box to Y. Y can then unlock the box with her key and read the message from X. To reply, Y must similarly get X's open padlock to lock the box before sending it back to him. Suppose X uses Y's public key to send her an encrypted message. In the message, he can claim to be X but Y has no way of verifying that the message was actually from X since anyone can use Y's public key to send her encrypted messages. So, in order to verify the origin of a message, RSA can also be used to sign a message. Suppose X wishes to send a signed message to Y. He can use his own private key to do so. He produces a hash value of the message, raises it to the power of d mod n (as he does when decrypting a message), and attaches it as a "signature" to the message. When Y receives the signed message, she uses the same hash algorithm in conjunction with X's public key. She raises the signature to the power of e mod n (as she does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, she knows that the author of the message was in possession of X's private key, and that the message has not been tampered with since.

4 RSA Algorithm

The RSA algorithm involves three steps: key-pair generation, encryption and decryption process [12].

4.1 Key-pair Generation for Conventional RSA

a. Choose two distinct prime numbers p and q

b. Compute $n \leftarrow p \times q$

- n is used as the modulus for both the public and private keys

c. Compute the totient: $\varphi(n) \leftarrow (p-1) \times (q-1)$

d. Choose an integer e such that, $1<e<\varphi(n)$ and e and $\varphi(n)$ share no factors other than 1 (i.e. e and $\varphi(n)$ are co-prime)

- e is released as the public key exponent

e. Determine d (using modular arithmetic) which satisfies the congruence relation:

$$de \equiv 1 \pmod{\varphi(n)}$$

- Stated differently, ed − 1 can be evenly divided by the totient (p − 1) × (q − 1)

- This is often computed using the Extended Euclidean Algorithm

- d is kept as the private key exponent

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret

4.2 Encryption Process

X transmits his public key (e, n) to Y and keeps the private key (d, n) secret. Y then wishes to send message M to X. She first turns M into an integer 0 < m < n by using an agreed-upon reversible protocol known as a padding scheme. She then computes the cipher text c corresponding to c ≡ me (mod n). This can be done quickly using the method of exponentiation by squaring. Y then transmits c to X.

4.3 Decryption Process

X can recover m from c by using his private key exponent d using the equation m ≡ cd(mod n)

Given m, she can recover the original message M by reversing the padding scheme. The above decryption procedure works because cd≡ (me)d≡ med(mod n). Now, since ed = 1+ k φ (n),
med≡ m1+ k φ(n) ≡ m(mk) φ(n)≡ m (mod n). The last congruence directly follows from Euler's theorem when m is relatively prime to n. By using the Chinese remainder theorem it can be shown that the equations hold for all m. This shows that we get the original message back cd≡ m (mod n).

4.4 Process Explanation with an Example

Here is an example of RSA encryption and decryption process. The parameters used here are artificially small,

a. Choose two prime numbers p = 61 and q = 53

b. Compute n = p x q

= 61 x 53 = 3233

c. Compute the totient φ (n) = (p-1) x (q-1)

Φ (n) = (61-1) x (53-1)
= 3120

d. Choose e > 1 co-prime to 3120, so e = 17

e. Compute d such that de ≡ 1 (mod φ (n)) e.g., by computing the modular multiplicative inverse of e modulo φ (n) we get, d = 2753.

Since 17 x 2753 = 46801= 1 + 15 x 3120.

The public key is (n = 3233, e = 17). For a padded message m the encryption function is:

c ≡ me (mod n) = m 17 (mod 3233)

The private key is (n = 3233, d = 2753). The decryption function is:

m ≡ cd (mod n) = c 2753 (mod 3233)

For example, to encrypt m = 123, calculating c= 123 17 (mod 3233) = 855

To decrypt c = 855, calculating m= 855 2753 (mod 3233) = 123

5 Triple DES

The Data Encryption Standard (DES) is a secret key encryption scheme adopted as standard in the USA in 1977. It uses a 56-bit key, which is today considered by many to be insufficient as it can with moderate effort be cracked by brute force. A variant called Triple-DES (TDES or 3DES) uses a longer key and is more secure, but has never become popular. The Advanced Encryption Standard (AES) is expected to supersede DES (and 3DES) as the standard encryption algorithm [3]. The Triple-DES variant was developed after it became clear that DES by itself was too easy to crack. It uses three 56-bit DES keys, giving a total key length of 168 bits. Encryption using Triple-DES is simply encryption using DES with the first 56-bit key, decryption using DES with the second 56-bit key, encryption using DES with the third 56-bit key. Because Triple-DES applies the DES algorithm three times (hence the name), Triple-DES takes three times as long as standard DES. Decryption using Triple-DES is the same as the encryption, except it is executed in reverse.

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

i.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.
Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

i.e., decrypt with K3, encrypt with K2, then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

6 Hash Function

A hash function is any well-defined procedures or mathematical functions which convert a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serves as an index into an array[13][14]. The values return by hash functions is known as hash values, hash codes, hash sums or simply hashes. A hash value h is generated by a function H of the form

$$h = H(M)$$

where M is a variable-length message and H(M) is the fixed-length hash value. The hash value is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by re-computing the hash value. Because the hash function itself is not considered to be secret, some means is required to protect the hash value. All hash functions operate using the following general principles. The input (message, file, etc.) is viewed as a sequence of n-bit blocks. The input is processed one block at a time in an iterative fashion to produce an n-bit hash function. One of the simplest hash functions is the bit-by-bit exclusive-OR (XOR) of every block[16].

7 Approach of the Proposed System

Let two user of the system are A and B. For better understanding we assume that A is sender of the message and B is the receiver. Both the user have given their key values by KDC (Key Distribution Center). Sender A has his own private key PRA and public key PUA, and B is also has his private key PRB and public key PUB. All the key values are generated by RSA algorithm. The system involves key pair generation, Encryption System and the Decryption System. "The proposed RSA and Triple DES based Combined Secured Approach to Ensure Data Security" is described in the following.

7.1 Key-pair Generation using RSA

a. Choose two distinct prime numbers p and q
b. Compute $n \leftarrow p \times q$
n is used as the modulus for both the public and private keys
c. Compute the totient: $\varphi(n) \leftarrow (p-1) \times (q-1)$
d. Choose an integer e such that, $1<e<\varphi(n)$ and e and $\varphi(n)$ share no factors other than 1 (i.e. e and $\varphi(n)$ are co-prime)
e is released as the public key exponent
e. Determine d (using modular arithmetic) which satisfies the congruence relation: $de \equiv 1 \pmod{\varphi(n)}$. d is released as the private key. So a user has one private key pair (d, n) and one public key pair (e, n).

7.2 Proposed Encryption System

Encryption of any message M which is also called plaintext involves creating ASCII table for each character of the message M. Then transform ASCII value of each character into its binary equivalent and apply a simple hash function X-OR repeatedly to all the binary values of each character. This produces a single binary string X, which is then appended with the original message, M. This appended message is now encrypted with sender's private key PR_A using RSA encryption algorithm that generates a cipher text C. A secret key K_S is now used to further encrypt the cipher text C along with the triple DES encryption algorithm, and this creates a cipher text C'. The secret key K_S is also encrypted by using receiver B's public key PU_B. The encrypted secret key and the encrypted data C' is now sent to the receiver B.

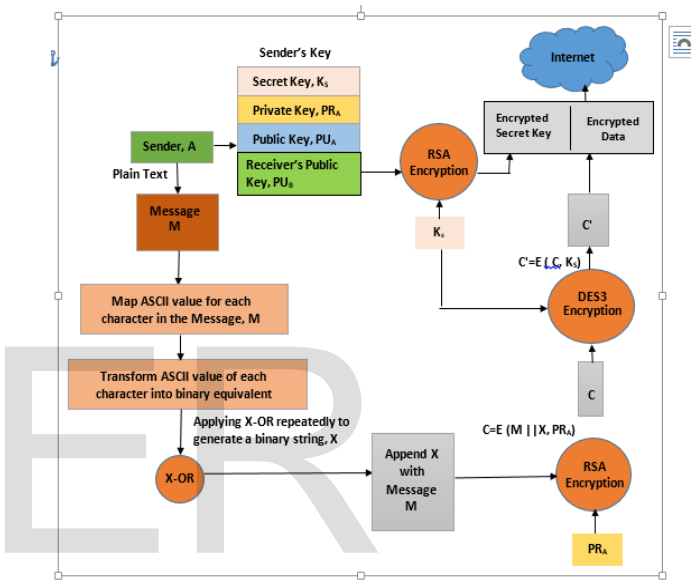

Figure 1: Proposed Encryption System

7.3 Proposed Decryption System

Receiver B now receives the encrypted secret key along with the encrypted data C'. At first B will decrypt the encrypted secret key by using his private key PR_B. Then the secret key K_S is used to decrypt the cipher text C' using triple DES algorithm to get C. This cipher text C is again decrypted using RSA algorithm along with the sender's public key PU_A. Thus we get appended message M and a hash digest X. The receiver B will repeatedly applying the hash function X-OR, just same process did by the sender to generate a hash digest X', which will compare with the received hash digest X. If the value of X and X' are same then it is ensured that the received message is altered. The use of the secret key establishes the strong confidentiality and the uses of the sender's private key ensure the authentication by creating digital signature. The proposed system can be applied for many cryptographic applications like business transaction, small organization, file transaction etc. where strong security is highly demanded.

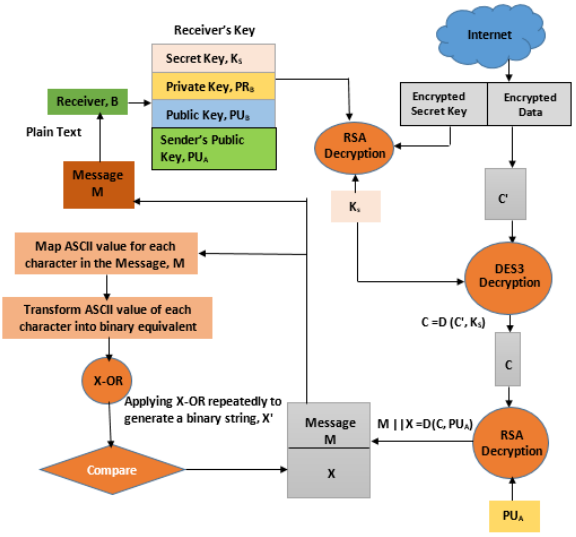

FIGURE 2: PROPOSED DECRYPTION SYSTEM

8 IMPLEMENTATION

Implementation of proposed RSA and Hash Based Secured Short Message Transactions contains rich source of codes for primality test, key-pair generation, and hash operation and for encryption-decryption process. Hence, object oriented approach is used to develop the proposed system. JAVA programming language is used to implement the system and hence improve the efficiency of the program. JAVA is mostly uses and popular language to implement object oriented concept. Another important advantage of JAVA is that it is platform independent. So, this implemented software able to run on any operating system where Java Virtual Machine (JVM) exists.

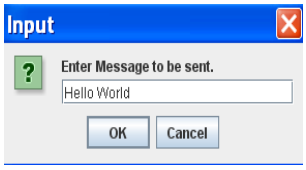

FIGURE 3: SAMPLE INPUT

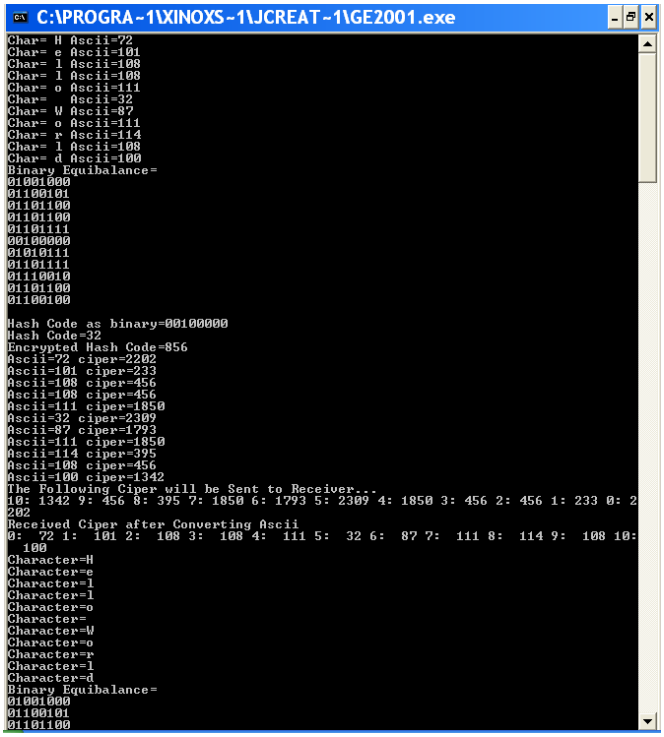

FIGURE 4: SAMPLE OUTPUT

9 COMPARISON OF THE PROPOSED SYSTEM WITH CONVENTIONAL RSA AND TRIPLE DES SYSTEM

After studying other related topics, algorithm, application of private and public key cryptography it is clear to me that one security approach can't be able to provide all the security service like data confidentiality, integrity checking, user authentication, data verification, authorization services, non-repudiation etc. To ensure strong security services a better most secures system is thus obvious. So this paper presents a combined approach based on symmetric and asymmetric key cryptography like Triple DES and RSA respectively. The comparison between proposed System with conventional RSA and Triple DES system is given below.

TABLE 1: COMPARISON OF PROPOSED SYSTEM WITH CONVENTIONAL SYSTEM

SYSTEM	AUTHENTICATION	CONFIDENTIALITY	DIGITAL SIGNATURE	INTEGRITY
TRIPLE DES	NO	YES	NO	NO
RSA	YES	YES	YES	NO
PROPOSED SYSTEM	YES	YES	YES	YES

10 CONCLUSIONS

RSA algorithm had been in use for the last 25 years and it's been one of the most successful cryptography algorithms that the security world ever had. But it is now less secure to ensure data security alone. Moreover DES or triple DES can't provide all the security services too. So this is very sure to have such a secured system that will provide strong data security as the way I have mentioned in this research paper. Though the proposed system imposed some processing overhead but the security services like data confidentially, integrity and user authentication it provides are very much demanded. This system is good for small message service (SMS), digital signature, M-commerce (WAP), smart card system (EMV), E-commerce and banking (SET), Internet based applications (SSL).

ACKNOWLEDGMENT

It is with a great sense of anticipation and trepidation that I begin to write, what I consider to be, one of the most important pieces of my dissertation. There are a great number of people who helped me over the years, and I know that it is impossible to thank all of them. But I will try my best to thank as many as I can, and sincerely apologize to those I missed.

I express my special thanks, sincere gratitude and deepest appreciation to Prof. Dr. Md. Ismail Jabiullah, Head of the Department, Department of Computer Science and Engineering, Hamdard University Bangladesh, for his excellent guidance, kind supervision and continued encouragement to organize the materials diligently. He was a constant source of ideas, motivation, and encouragement. His valuable time, inspiration and scholarly advice helped me to accomplish the work systematically.

I am very much thankful to my family members and friends for their continuous support and encourage through the task of the thesis creation. Most of all, I would like to thank my parents for whom I am a human in the society.

REFERENCES

[1] Andrew S. Tanenbaum, "Computer Network", Forth Edition, 2003, ISBN: 0-13-066102-3
[2] William Stallings, "Cryptography and Network Security- Principles and Practices", Fourth Edition, 2006, ISBN: 978-81-203-3018-4
[3] William Stallings, "Data and Computer Communication" Seventh Edition, July 2003, ISBN: 9971-51-431-1.
[4] "Standard Specifications for Public Key Cryptography", IEEEP1363/D10 (Draft Version 10), New York USA, 1999.
[5] https://en.wikipedia.org/wiki/Data_security
[6] "An Overview of Cryptography", Gary C. Kessler, May 1998, (22April, 2010). Web-site link: http://www.garykessler.net/library/crypto.html.
[7] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126. doi:10.1145/359340.359342. http://theory.lcs.mit.edu/~rivest/rsapaper.pdf.
[8] "Cryptography and Network Security", Behrouz A. Forouzan, Special Edition 2011, McGraw-Hill, ISBN-13: 978-0-07-066046-5 and ISBN-10: 0-07-066046-8
[9] "Data Communication and Networking",Behrouz A. Forouzan, Fourth Edition, McGraw-Hill, International Edition, 2007, ISBN-13: 978-007-125442-7 and ISBN-10: 007-125442-0.
[10] RSA Laboratories. RSA Laboratories frequently asked questions about today's cryptography, version 4.1.2000. Accessed on-http://www.rsasecurity.com.
[11] Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography, Chapter 9: "Hash functions and data integrity", pages 321-383. The CRC Press series on discrete mathematics and its applications. CRC Press, 1997.
[12] Ronald L. Rivest. Abelian square-free dithering for iterated hash functions. Accessed on-http://theory.lcs.mit.edu/~rivest/RivestAbelianSquareFreeDithering ForIteratedHashFunctions.pdf. Last accessed on 15th of December 2006.
[13]Wikipedia, the free encyclopaedia http://en.wikipedia.org/wiki/Cryptography, Accessed on November 15, 2014.
[14]http://en.wikipedia.org/wiki/Cryptographic_hash_function, Accessed on January 7, 2015.
[15] B. Preneel, R. Govaerts and J. Vandewalle. "Hash functions based on block ciphers". In Advances in Cryptology, CRYPTO' 93, Lecture Notes in Computer Science, pages 268-378. Springer-Verlag, 1994.