IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 6, Jun 2014, 143-150

UNIQUE INFORMATION BASED SECURE RSA

NEHA GUPTA[1], RAVI KUMAR GUPTA[2] & SHIPRA GUPTA[3]

[1,2]Research Scholar, Department of Computer Science & Engineering, Mewar University, Chittorgarh, Rajasthan, India

[3]Assistant Professor, Department of Computer Science & Engineering, WIT, Sohna, Haryana, India

ABSTRACT

Computer security is one of the most important parameters considered in any computer system to prevent any data misuse by an unauthorized/ outside intrusion. Cryptography is one technique for data/ computer security. In this paper, we have proposed a technique for a more secure data transfer which is a alteration to the classical public key crytogarphy method known as Unique Information Based Secure RSA. This method is based on public key cryptography scheme. In Unique Information Based Secure (UI SECURE) RSA public key of a user is derived from his/her unique identity such as email id, phone number. With the use of UI SECURE RSA, there is no need of public key certificates. It has a special entity called SEM. SEM is an on-line partially trusted server. For using services of SEM, a user needs to obtain an identity based token from SEM. A message cannot be encrypted or decrypted without this token. UI SECURE RSA divides the private key of the user in two parts: one part is given to the user and the other to the SEM. Both parts of the key are used to encrypt/decrypt the message. This technique is very secure as the key cannot be derived using half key.

KEYWORDS: Cryptography, Public Key, Private Key, Encryption, Decryption

INTRODUCTION

In today's world, almost every sector including banking, entertainment, education etc are online i.e. the customer/ user can access them through internet from anywhere according to their comfort. This is a great advantage of internet, but this advantage comes along with a drawbacks. As the data is available on the web so there are considerable chances of data loss, leakage of confidential data, misuse/ intrusion or alteration in the data. So, to overcome these drawbacks, it is important to protect our data by using proper data security schemes. Security services include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability.[1]

The NIST Computer Handbook [NIST95] defines the computer security as "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)".

The key principles of security can be summarized as:

- **Confidentiality:** Confidentiality is the principle that is based on maintaining the secrecy of data between the identified set of users, i.e. the intended sender and receiver. No other entity, i.e. an unauthorized entity or intruder, should be able to access the data.
- **Authentication:** Authentication is the principle that is based on identifying the authenticity of the entity which is interested in accessing the data.

- **Integrity:** Integrity is the principle that is based on ensuring that the data received by the receiver is exactly the same as sent by the sender. If the data is modified during the transit, integrity is violated or lost.
- **Non-Repudiation:** Non-repudiation principle is based on implying technologies such that the set of users, i.e. the sender and the receiver, cannot deny the transaction of data. The sender entity cannot refuse that it has sent the data as well as the receiver cannot deny the reception of data.
- **Access Control:** Access control principle is based on determining the restriction in data access by the receiver. If there are a number of receivers who can access the data, then the receiver control on the data can be controlled and different receivers can be provided with different controls on data.
- **Availability:** The principle of availability ensures that the data is available whenever it is needed. A high availability system is required to maintain a continuous data availability. It is quite obvious that to maintain data availability, a check on security attack is a key element.

SECURITY ATTACK

Security attack can be defined as an intruder attack on the system with the intention of destroying, exposing, altering, stealing or gaining of unauthorized access to an asset. In the worst case, security attack can lead to a condition where the organization's network devices or even the entire network is owned by the intruder or the attacker. Attacks can be broadly classified as:

- **Passive Attack:** Passive attack can be defined as a silent attack, where the intruder does not attempt to breakthrough or modify the original system. Instead, he keeps an eye on all the communication between the authorized parties. In passive attacks, the sender and the receiver are not even aware that their confidential data is exposed to a third person. This way the intruder can easily misuse the data without even being in knowledge of the data owner.
- **Active Attack:** In contrast to passive attacks, in active attacks the original message or data is modified. The intruder tries to breakthrough the original data or message. Active attacks can affect the availability, integrity, confidentiality and authenticity of the system.[2]

CRYPTOGRAPHY

Expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Attacks are of two types-

- Passive Attack
- Active Attack

Passive Attacks: Passive attacks do not involve any modification to the contents of the original message. The main aim is to monitor data transmission.

Active Attacks: In active attacks, the contents of the original message are modified in some way.

Cryptography

It is the art and science of achieving security by encoding messages to make them non-readable.

Symmetric Encryption

It is also known as conventional, secret-key, single-key

- Sender and recipient share a common key
- Was the only type of cryptography, prior to invention of public-key in 1970's [1]

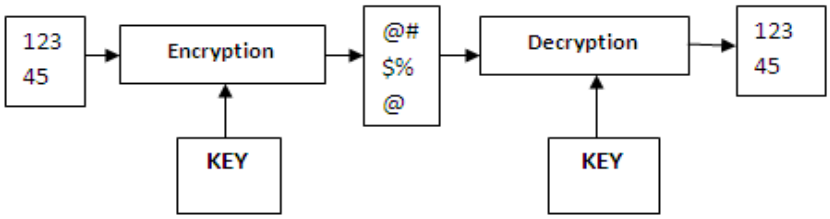

Figure 1: Symmetric Key Encryption

Public-Key Cryptography

Also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both [1].

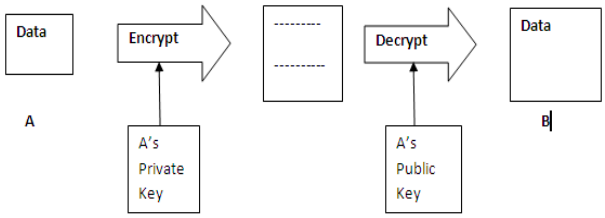

Figure 2: Public Key Cryptography

RSA Algorithm

RSA was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm [10].

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

- Choose two different large random prime numbers p and q
- Calculate n=pq

- Calculate the totient: $\phi(n) = (p-1)(q-1)$.
- Choose an integer e such that $1 < e < \phi(n)$, and e is coprime to $\phi(n)$ ie: e and $\phi(n)$ share no factors other than 1; gcd $(e, \phi(n) = 1$.
    - e is released as the public key exponent
- Compute d such that de mod $\phi(n)=1$.
    - d is kept as the private key exponent

Suppose, there are two users Alice and Bob, who wish to communicate with each other in a secure manner. The methods for encrypting and decrypting the messages using RSA algorithm are explained below-

Encrypting Messages

Alice gives her public key (n & e) to Bob and keeps her private key secret. Bob wants to send message M to Alice.

First he encrypts the message m-

$C= m^e \bmod n$

Bob then sends c to Alice [7].

Decrypting Messages

Alice can recover m from c by using her private key d in the following procedure [7]:

$m=c^d \bmod n$

Problem Statement

Using secret key and an encryption algorithm, the sender encrypts the message. The receiver using the same secret key and the corresponding decryption algorithm decrypts the message. However, the Public Key Cryptography (PKC) Scheme introduced by Diffie and Hellman (1976) gave the concept that the sender and receiver need not use the same secret key for encryption and decryption. In fact, the sender uses a key called public key to encrypt and the receiver uses a different key called private key, for decryption. This concept revolutionized the cryptography research. This also introduced the concept of Digital Signature (Rivest *et al.*, 1978). Though there are number of algorithms available to implement the PKC, the main problem lies in the distribution of the Public key. This is done by a Certification Authority (CA), which distributes the Public Key of a user in the form of a signed certificate. This leads to the issues of certificate management like revocation, distribution, storage and verification.

Unique Information Based Public Key Encryption is a solution to these problems.

UI Secure RSA

This is a scheme, in which, an entity's public key is derived directly from certain aspects of its identity, for example, an IP address belonging to a network host, or an e-mail address associated with a user.

In this scheme, a simple identity based cryptosystem developed atop some Mediated RSA (mRSA) (Boneh *et al*., 2002) has been proposed.

Algorithm for key generation-

Let w (even) be the security parameter

1.) Generate random w/2 it primes x and y

Such that p = 2x + 1, and
q = 2y+1 are also prime

2.) n = pq

3.) $\varphi(n) = (p-1)(q-1)$

4.) For each user 'A'

a.) $e_A = ff(ID_A)$

b.) $d_A = 1/e_A \bmod \varphi(n)$

c.) $d_{Au} = Z_n$

d.) $d_{A,SEM} = (d - d_{Au}) \bmod \varphi(n)$

Algorithm for key generation is described above. Certificate Authority (CA), chooses two large prime numbers x and y randomly such that p = 2x + 1 and q = 2y+1 are also primes. Then n = pq and $\varphi(n) = (p-1)(q-1)$ are computed. The public key of user A is generated by as the output of $ff(ID_A)$. ff must be set beforehand. It is an efficient mapping hash function. The function must be a one to one mapping from identity strings to public keys. Z_n is a randomly chosen odd number relatively prime to $\varphi(n)$.

Algorithm for encryption

1.) n, k and ff are retrieved from the domain certificate.

2.) $e = ff(ID_A)$

3.) Encrypt the input message m with (e,n) using standard RSA.

The algorithm for encrypting a message m is given above. For encrypting a message m, a used only needs receiver's unique information such as email id, phone number and the domain certificate. After this the message encrypted using RSA algorithm as described above. The decryption is also same as encryption and the decryption algorithm is given below-

Decryption algorithm

1.) USER: m'←Encrypted Message

2.) m' is send to SEM

3.) In parallel:

(i) SEM:

(a) $HD_{sem} \leftarrow m'^{d_{sem}} \bmod n$

(b) Send HD_{sem} to USER

(ii) USER:

(a) $HD_u \leftarrow m'^{d_u} \bmod n$

4.) USER: $M \leftarrow (HD_{sem} * HD_u) \bmod n$

5.) USER: m← RSA decoding of M

Mapping Function FF

MD-5 or SHA-1, any of the hash functions can be safely used as mapping function ff. MD-5 and SHA-1 both are cryptographic hash functions. MD-5 produces a 128 bit hash value and SHA-1 produces a 160 bit hash value [9].

Table 1: Comparison of MD-5 and SHA-1

MD5	SHA-1
• Message digest is 128 bits in length.	• Message digest is 160 bits in length.
• It requires 2^{128} attacks to compute the original message.	• It requires 2^{160} attacks to compute the original message.
• Attack to try and find two message producing the same message digest requires 2^{64} operations.	• Attack to try and find two message producing the same message digest requires 2^{80} Operations
• It is faster with 64 iterations and 128 bit buffer.	• It is slower as compared to MD5 with 80 iterations and 160 bit buffer.

Properties of Hash Functions

- It is easy to compute the hash value of any given message.
- It is infeasible to generate a message that has a given hash.
- It is infeasible to modify a message without changing the hash.
- It is infeasible to find two different messages with the same hash.

Performance Comparison

Performance comparison of different encryption keys are given below-

Table 2

Keys	RSA Mod 1kb	RSA Mod 2kb	RSA Mod 3kb
128 bit key	6 ms	19 ms	53 ms
160 bit key	7 ms	24 ms	72 ms

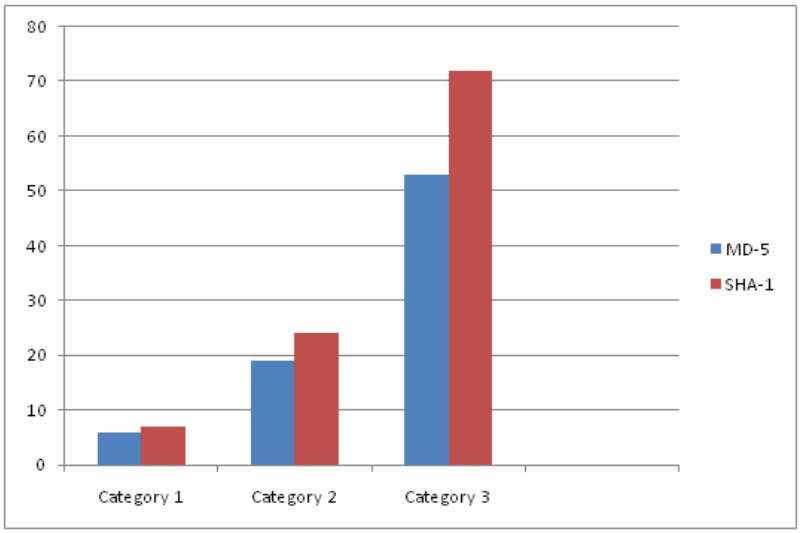

Figure 3

MD-5 hash function produces a key of 128 bits and SHA-1 produces a key of 160 bits. Described above is a performance comparison of the algorithm using both when 128 bit key (MD-5) is used and when 160 bit key is used (SHA-1). Since, MD-5 produces a 128 bit key, its execution time is faster than compared to SHA-1 but SHA-1 is more secure.

CONCLUSIONS

Unique Information Based Secure RSA can be implemented easily because in the present scenario RSA is widely accepted and implemented cryptographic algorithm. It provides high security to the clients and can be used to transmit confidential data from one end to another with proper authentication. It provides better performance. Less than 1ms time is required for private key generation. Time taken by the algorithm to encrypt the data is around 7ms and decryption time reaches approximately 35ms. SEM, the third party, used is a fully trusted third party, since its collision with any other can result in compromise of all other user's secret key due to shared RSA modulus.

FUTURE WORK

Here, hash function is used for public key mapping, which makes this algorithm expensive to implement than RSA since the public exponent is random. We need to search upon alternate mapping functions that can produce more efficient RSA components.

REFERENCES

1. W. Stallings, "*Cryptography and Network Security: Principles and Practice*" Prentice Hall Fifth Edition.
2. "*Ethical Hacking and Countermeasures Attack Phases*", EC Council Press
3. K. Santoshi, K. Imamoto, K. Sakurai, *Enhancing Security of Security-mediated PKI by one-time ID*, in: Proc., the 4th Annual PKI R&D Workshop, USA, April 19-21.
4. K. Bicakci, N. Baykal, *Improved server assisted signatures*, Computer Networks 47 (2005) 351-366.
5. http://www.ijert.org/view.php?id=2147&title=secure-transaction-in-online-banking-system-using-ib-mrsa
6. J. Cleens, V. Dem, J. Vandewalle, *On the security of today's online electronic banking systems*, Journals of Computers & Security 21(3) (2002) 257-269.
7. W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, 22(1976), pp. 644-654
8. Thai Duong and Juliano Rizzo, "Cryptography in the web: The case of cryptographic Design Flaws in ASP.NET", IEEE symposium on Security and Privacy 2011.
9. Vishwa Gupta, Gajendra Singh, and Ravindra Gupta, "Advance Crytography Algorithm for improving Data Security", International Journal of Advanced research in Computer Science and Software Engineering Jan '2012.
10. http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29