ISSN 2319 – 7595
Volume 4, No.1, January – February 2015
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/pdfs/2015/ijiscs01412015.pdf

An Efficient RSA-based and chaos-based Authentication Scheme

Chitra Solanki[1], Madhu Sharma[2]
[1] Mtech Student DIT University, India, chitrasnehlata@gmail.com
[2]Assistant Proffesor DIT University, India, madhuashishsharma@gmail.com

ABSTRACT

As we all know, security is an integral part of every technology and implementation today. In this IT driven society, cryptography is perhaps the most widespread form of secure communication. Authentication using RSA and chaotic map is basically the mechanism to help in establishing the proof of identities. The baker's map is used for generating random number. Chaos refers to a type of complex dynamical behavior that possesses some special features such as being extremely sensitive to small variations in initial conditions.

The project is to make a scheme based on RSA and chaotic map to show that a strong certificate less signature scheme not only keeps the original security properties of the signature, i.e., integrity, authentication and non-repudiation, but also can protect the signer even if the attacker has strong power. In 2014, Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang has given a simmilar designed certificateless-based signature scheme based on RSA operations; however, their scheme is modified and made more secure in this paper so that security level increases. This paper is an improved version to make the RSA-based certificateless scheme stronger and more secure [2].

Key words: Certificateless cryptography, digital signature, chaotic map, random number.

1. INTRODUCTION

Authentication is basically to ensure that the origin of an message is correct. Authentication of digital documents has aroused great interest due to their wide application areas such as legal documents, certificates, digital books and engineering drawings [5]. Internet is the most integral part of our daily life and the people who manages their work with internet like bank transaction, online shopping is also constantly growing. The websites which provide these services should be an authenticated one i.e., they should allow the user to create their own username and password with a reliable service. So only qualified people can access their account by password authentication. For a secure transaction another technique like Secure Socket Layer (SSL) is used. But some websites offers a poor authentication service which leads to password attacks.

Although many researchers have designed different authentication schemes with different requirements, like blind signatures. In the blind signature scheme, a user could get a signature for any message but the signer does not know the content of the message. Due to such properties, blind signature schemes are widely used in electronic voting, electronic payment and electronic cash [8]. All digital signatures are designed to save data from the following kind of attacks.

a) passive attacks
b) active attacks

Passive attacks do not involve any modification to the contents of an original message while in active attacks, the contents of the original message are modified in some way. It includes the following attacks [1].

The two main types of passive attacks are

(1) Release of message contents:

This type of attack means loss of confidentiality of message. When an unauthorized person is able to access the contents of the message.

(2) Traffic analysis:

We can prevent release of the message content by encoding the contents of the message in a form which can decoded by the desired parties because only they know the code language. However, if many such messages are passing through, a passive attacker can find simmilarities between them to come up with some sort of pattern. Such attempts of analyzing contents of messages that provides some clue to attacker regarding the communication that is taking place is known as traffic analysis attack.

The main types of active attacks are in the form of interruption attack such as masquerade, alteration or change in content of message such as modification, and denial of services to legitimate users such as fabrication [1].

(1) Masquerade:

It is a type of attack when an unauthorized user pretend to be an authorized user.

(2) Modification:

Alteration of messages is known as Modification. In this type of attack attacker changes the content of the messages like in an ongoing transaction it can change 500$ to 5000$.

(3) Fabrication:

Fabrication causes Denial Of Service (DOS). This attack make an attempt to prevent legitimate users from accessing some services, which they are authorized for [1].

We demonstrate these as follows:

In the proposed scheme, the authentication is done using chaotic map and RSA scheme. It is well known that RSA has been frequently used in the industry for years and many companies have invested in expensive hardware or software implementations of RSA [3]. Chaotic functions have certain properties which lend them directly to encryption schemes. In an attempt to use chaotic maps for the scheme we have used the random number which is generated from the baker's map. In a traditional digital signature system, the signer normally holds two keys, a private key and a public key. The private key can be used for signing important messages, and give the corresponding public key to the certificate authority and verifier. The certificate authority (CA) stores and manages every user's public key. Once the verifier receives a signature from a signer and wants to verify it, CA will give the corresponding certificate to the verifier which includes the signer's public key. Hence, the verifier can verify the certificate and the signer's public key immediately. It is secure and very convenient but places a heavy burden on CA because the CA has to store and manage many certificates. The users are allowed to use their identity information as their public key, and a private key generation center (PKGC) can generate user's private key which corresponds to the user's identity information. Unfortunately, some researchers have started to suspect the PKGC because people feel unsafe about the CA holding their private key and privacy information. This is called the "key escrow problem" to overcome "key escrow problem", researchers have started to focus on the issues of the certificateless-based signature scheme [2]. Earlier, a variety of "key escrow" and "trusted third party" encryption requirements was suggested by government agencies [6].

1.1 Chaos and Baker's Map

Baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one another, and compressed. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion [10]. Now, to consider the two-dimensional baker map, refer to (1)

$$\begin{aligned} B(x_n; y_n) = {} & (c x_n; 2y_n) \quad 0 \le y \le 0.5 \\ & (1 + c(x_n - 1),\ 2y_n - 1) \quad 0 < y \le 1 \end{aligned} \tag{1}$$

where, $0 < c \le 0.5$

Chaos means as iterates of functions and stable and unstable fixed points. Chaos is a word we all know usually meaning a lack of order or predictability. Chaotic behavior is the delicate behavior of a nonlinear system, which apparently random [10]. The weather is indeed one example of a chaotic system. A weather reporter might make nearly identical forecasts for two different areas, meaning that the initial conditions of the system are quite similar, while by the next week the weather patterns are completely different. Because of this sensitive dependence on initial conditions, weather forecasters have a very difficult time predicting the weather far in advance. Chaotic systems are not predictable over a long period of time and are also associated with fractal structures [9].

2. PROPOSED ALGORITHM

In this section, we propose an algorithm. There are three participants in our scheme: key generator center (KGC), signer, and verifier [2]. Our scheme consists of eight algorithms and the details are described as follows.

Algorithm

Step1. Apply R.S.A scheme by taking two large number's p and q and N = p*q and then generate public key e and private key d.

Step 2. Take two variables h and h' as cryptographic hash functions such that h has MD5 hash value and h' has SHA-1 hash value.

Step3. Setup → (MPK, MSK) such that KGC sets parameter d to be the master secret key (MSK) and parameters {e, N, h, and h'} to be the master public key (MPK).

Step4. In the blinding phase, the signer chooses a random number R first which is derived from baker's map, and then computes R^{-1} that satisfies $R.R^{-1} = 1$ that satisfies. Set UID users identity as any constant number and random number as secret value x_{UID}.

Step5. Signer chooses a random number r, and compute $R_r = UID^r.\ x_{UID}^{2r}$, H = h ($R_r$, UID , m), where m is the message and h is a hash function MD5. Then compute $u_1 = x_{UID}^{H+r}$ and $u_2 = ((x_{UID}.UID)^d)^{r-H}$ and generate the signature delta = (H, u_1, u_2)

Step6. Now verifier calculate $R_r' = (u_2)^e.(UID)^H (u_1)$ by using e, UID and then, the verifier can use R_r', signer's public key e, UID and the message m to generate $H' = h\ (R_r', UID\ , m)$, and verifies whether H is equal to H' . If the equation holds, then the verifier can believe that the signature is correct authentication. Otherwise go to step 7

Step7. H' not equal to H. Hence, fabrication.

3. RELATED WORK

We propose a strong RSA-based and chaotic map based certificateless scheme to improve authentication scheme. There are three participants in our scheme:

(A) key generator center (KGC)

(B) signer and

(C) verifier.

Our proposed scheme can be divided into three phases: 1) setup phase, 2) signing phase and 3) verifying phase. The details are described as follows:

(1) Setup Phase:

In this step we use RSA scheme [7]. The KGC randomly take two prime numbers numbers p and q, and compute its product which is N = p*q. Then KGC can choose public key (e) that satisfy (gcd e, Φ(N)) = 1. Here, Φ(N) denotes Eular's totient function. After that, KGC can find one private key (d) from computing ed=1 mod Φ(N) and selects two cryptographic hash functions MD5 and SHA-1. Finally, KGC sets parameter d to be the master secret key (MSK) and parameters e, MD5, and SHA-1 to be the master public key (MPK). MD5 is simple and easy to implement while SHA-1 chances of collision are less as compared to MD5 because of larger sized message digest [4].

(2) Signing Phase:

In this phase signer chooses a random number R generated by BAKER'S MAP (the baker's map is a chaotic map from the unit square into itself) and then compute its inverse R^{-1} that satisfies $R.R^{-1} = 1$. After that, he or she uses, secret value x_{UID} and KGC's master public key e to compute $C=R^e.x_{UID}$ and sends his identity UID and C to KGC. When KGC receives UID and C, KGC will use its master private key d to sign the received UID and C. After that, KGC sends UID^d and C^d back to the signer. When the signer receives UID^d and C^d, he or she can compute $C^d.R^{-1}$ to get x_{UID}^d. Finally, the signer can compute $x_{UID}^d.UID^d = (x_{UID}.UID)^d$ and sets $(x_{UID}.UID)^d$ as the private key. At the same time, signer can directly set her/his identity UID as the public key. In this phase signer chooses a random number r, and uses r to compute $R_r = UID^r.x_{UID}^{2r}$. After that, the signer can compute $H = h\ (R_r, UID, m)$, where UID is the public key of signer and m is the message. Then, the signer computes and $u_1 = x_{UID}^{H+r}$ and $u_2 = ((x_{UID}.UID)^d\ )^{r-H}$ to generate the signature delta = (H, u_1, u_2) and send a message with the signature to the verifier.

(3) Veryfying Phase:

When the verifier receives the message m with signature delta, he or she can use signer's public key (UID) and KGC's master public key which is e to compute $R_r' = (u_2)^e.(UID)^H (u_1)$. Then, the verifier can use R_r', signer's public key UID and the message m to generate $H' = h\ (R_r', UID, m)$, and verifies whether H is equal to H'. If the equation holds, then the verifier can believe that the signature is correct [2].

3.1 The details of the equation are shown as follows:

$$H' = h(R_r', UID, m) \tag{2}$$

Now, from verifying phase

$$(R_r)' = (u_2)^e (UID)^H (u_1) \tag{3}$$

Refer to (2) and (3)

$$H' = h[\{(u_2)^e . (UID)^H (u_1)\}, UID, m] \tag{4}$$

From signing phase

$$u_2 = ((x_{UID}. UID)^d)^{r-H} \tag{5}$$

Now, refer to (4) and (5)

$$H' = h[\{(((x_{UID}. UID)^d)^{r-H})^e . (UID)^H (u_1)\}, UID, m]$$

$$H' = h[\{((x_{UID})^{ed} (UID)^{ed})^{r-H} . (UID)^H (u_1)\}, UID, m]$$

$$H' = h[\{(x_{UID})^{r-H} (UID)^{r-H} . (UID)^H (u_1)\}, UID, m]$$

$$H' = h[\{(x_{UID})^{r-H} (UID)^{r-H+H} . (u_1)\}, UID, m] \tag{6}$$

Again from signing phase

$$u_1 = (x_{UID})^{r+H} \tag{7}$$

Now, refer to (6) and (7)

$$H' = h[\{(x_{UID})^{r-H} (UID)^r (x_{UID})^{r+H}\}, UID, m]$$

$$H' = h[\{(x_{UID})^{r-H+r+H} (UID)^r\}, UID, m]$$

$$H' = h\{(x_{UID})^{2r} (UID)^r, UID, m\} \tag{8}$$

From signing phase

$$R_r = (\text{UID})^r (x_{UID})^{2r} \tag{9}$$

Now, refer to (8) and (9)

$$\text{H}' = \text{h}(R_r, \text{UID}, \text{m})$$

$$\text{H} = \text{h}(R_r, \text{UID}, \text{m})$$

$$\text{H}' = \text{H}$$

4. RESULT

Table 1: Attributes

Abbreviation	Full form
RSA	Ron Rivest, Adi Shamir and Len Adleman
MPK	Master Public Key
gcd	Greatest Common Divisor
UID	User's Identity
KGC	Key Generation Center
MSK	Master Secret Key
MD5	Message Digest
SHA-1	Secure Hash Algorithm
e	Public Key
d	Private Key

Table 2: Proposed Scheme Module

	Proposed Scheme
algorithm	7 steps
phases	3 phases

Table 3: Proposed Scheme Variation

	For Message shivji	For Message jesus	For Message Hebrew
R random number generated by Baker's map length	1.075570e+ 02	7.074899e+ 01	8.623785e+ 01
Signer's private key length	5.049970e+ 132	9.351639e+ 200	2.941348e+ 104

For three different messages we have shown the variation in R length and signer private key length as shown in Table 3. The given e in Table 3 is exponentiation operator.

5. PERFORMANCE ANALYSIS

Authentication and cryptography play a vital role in online transmission, off-line retrieval systems. It is therefore essential that in this information technology driven society, we make digital transmission as secure as possible. We have proposed a scheme which use random number generated by baker's map. The use of baker's map is used to create chaos so that this scheme became unpredictable.

Chaotic phenomena seems to be random, but have a precise mathematical formulation. Hence, given some other parameters they are repeatable and yet apparently random. The properties required by cryptography are readily satisfied by chaotic functions as function parameters have sensitive dependence on initial conditions. We have used RSA technique in the first step and then we have used random number generated by a baker's map which makes this scheme more secure and safe. In this paper, an authentication technique based on chaotic Baker map and RSA has been presented. The chaotic Baker map is used as a method to increase the security level [7]-[10].

The implementation of the proposed technique is simple, and achieves good authentication mechanisms in a reasonable time, which is a required property for communication applications. Moreover, the processing time is the time required to authenticate, encrypt or decrypt data. The smaller the processing time, the higher the speed of authentication. We have tested this proposed technique and estimated that the processing is very fast.

6. CONCLUSION

This efficient RSA-based scheme has been found to not only improve the security level but also solve the certificate management problem. In this paper, we proposed an efficient RSA-based certificateless signature scheme to improve the security of Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang scheme. Our proposed scheme makes the RSA-based certificateless signature system more powerful and secure. At the same time, use of chaotic map makes it unpredictable. Furthermore, it is easy to implement. For all of these reasons, our scheme is more suitable for an efficient certificateless-based signature systems.

REFERENCES

1. ATUL KAHATE. ***Cryptography and Network security***, 1st ed .Tata McGraw-Hill, 2003, ch. 1, pp. 8-10.
2. Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang, **A Strong RSA-based and Certificateless-based Signature Scheme,** *International Journal of Network Security*, Vol.0, No.0, pp. 2-4, Jan. 22, 2014.

3. Debiao He, Muhammad Khurram Khan, and Shuhua Wu, **On the Security of a RSA-based Certificateless Signature Scheme**, *International Journal of Network Security*, Vol.16, No.1, pp. 1-3, Jan. 2014.
4. Pragya Agarwal, Shilpi Gupta, Anu Mehra, **Transmission and Authentication of Text Messages through Image Steganography**, *International Journal of Computer Applications (0975 – 8887) 4th International IT Summit Confluence 2013 - The Next Generation Information Technology Summit*, 2013, pp.1-4.
5. Kondapalli Venkata Ramana, and K. Usha Rani, **Chaotic Cryptographic to Maintain Security and Authentication of Gray Scale Image by Secret Sharing,** *International Journal of Application or Innovation in Engineering & Management*, Volume 2, Issue 9, September 2013 ISSN, pp. 42-44.
6. H. Abelson, R. Anderson, S. Bellovin, J. Benalob, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier, **The risks of key recovery, key escrow, and trusted third-party encryption**, *The World Wide Web Journal–Special Issue: AMatter of Trust,* vol. 2, no. 3, pp.1-4, 27 may 1997.
7. R.L RIVEST, A.SHAMIR, L.ADLEMAN. **A method for obtaining digital signatures and public key cryptosystem**, Association of compting machinery(ACM), 21(1978), pp.2 -8.
8. GUOFAGN DONG, FEI GAO, WENBO SHI and PENG GONG, **An efficient certificateless blind signature scheme without bilinear pairing**, *Anais da Academia Brasileira de Ciênciasin*, vol.86, pp. 1003-1006, , Brasil, 2014.
9. Alireza Jolfaei, Abdolrasoul Mirghadri, **Image encryption using chaos and block cipher**, *Canadian center of science and education*, vol.4, No 1, pp. 1-3, January 2011.
10. George Makris , Ioannis Antoniou, **Cryptography with Chaos**, *Proceedings, 5th Chaotic Modeling and Simulation International Conference*, Athens Greece, June 2012, pp. 1-2.