Secure Digital Certificate Design Based on the RSA Algorithm

Yunsheng Zhong
Department of State-owned Assets
Sichuan university of Arts and Science
Dazhou 635000
China
ashunjz@sohu.com

Journal of Digital
Information Management

ABSTRACT: *With the popularity of the Internet, people can purchase and sell goods and services online just staying at home, and this trend is becoming increasingly apparent. The Internet, as a global computer network, has to provide the following five services: security, data integrity, authentication, usability, and reliable information. In case of lack of safety measures, Internet trading risk is very high. Digital certificates can provide proof of identity in Internet transactions, so that we can greatly reduce transaction risk. This paper describes an approach based on the X.509 standard for digital certificates, using the C language generate public key algorithm RSA, enabling digital certificate generation and signature verification process, the identity of certification users can be verified.*

Categories and Subject Descriptors:
K.6.5 [Security and Protection]: Authentication

General Terms:
Video Frame Processing, Content Processing

Keywords: Internet, Authentication, Digital Certificates, RSA

Received: 28 July 2013, Revised 3 September 2013, 9 September 2013

1. Introduction

With the rapid development of the Internet, e-commerce and network information services have been more widely used. There are a great amount of information on the computer and network, some of which are important and privacy. However, network open and 0 interaction will affect the security of such information. Secure authentication can ensure that the information is accessed and visited only by authorized users, and thus it is extremely necessary to establish a set of authentication system to protect the information. Authentication system as the first hurdle can provide users and systems a strong safety performance. Digital certificate is a digital ID to show identity in the network. Encryption technology as the core of digital certificates can do encryption and decryption, and digital signature and signature verification for the information transmitted on the network to ensure confidentiality integrity and security of the information transmitted online[1]. This requires that the buyer and seller participating in e-commerce must have their legal status, which can be able to effectively verified effectively and correctly.

Currently the definition and use of certificates are very different, but the public key certificate used most is X.509V3 certificate. Object of this paper is digital certificate based on the X.509 V3 format.

2. The Overall Design Scheme

2.1 RSA Digital Signature Scheme

Combined with RSA algorithm, IT can achieve a digital signature. Digital signatures are usually attached behind the message as an encrypted message digest as to confirm the sender's identity and the integrity of the information. For example, if *A* send a message to *B*, the steps are as follows:

1. Take advantage of the RSA algorithm to calculate the original message summary[2].

2. Use their own private key to encrypt the abstract and summary attached to the back of the original message. *B* receives the message[2].

Verifying the digital signature, follows these steps:

(1) Separate the original message from the encrypted message summary[2].

(2) Make use of the RSA public key to decrypt the encrypted summary[2]].

(3) Use the RSA algorithm to recalculate the original

message summary [2].

(4) Compare the decrypted summary and a summary of their recalculated, if they are equal, it means that the message has not been tampered in the transfer process, otherwise, the message is credible [2].

RSA digital signature technology brings the following three aspects of security:

1. **Information integrity:** it is concluded from the characteristics of RSA algorithm that if the message has been tampered with during transmission, the summary B get is different from the one decrypted by A's public key in order to determine whether the information issued by A bas been tampered [2].

2. **Information confirm:** as the relationship of one to one between the public and private, if the value of B via public key to decrypt and that of A are the same, it can be confirmed that the information is sent by A [2].

3. **Non-repudiation:** because only A holds its own private key, A can not deny its send-off information [2].

CA can digitally sign the digital certificate., In the RSA cryptosystem, we can get the private key d and the public key e and n, then the field m of the digital certificate is: $r = (H(m))^d \bmod n \ (m < n)$.

Here $H(m)$ m is a message digest of the calculated field, obtained from the MD5 hash function, and r is the signature of the message. When verifying the digital signature, it is only need to verify that: $H(m) = re \bmod n$.

2.2 Certificate Request Program Based Business Platform

The process of generating a digital certificate must has the involvement of *RA* and *CA*. But here we can rely on the e-commerce platform to help us solve a lot of things. Here before applying for a certificate, the users must put their own public keys issued to *RA*, and *RA* must first determine the legitimacy of the public key. *RA* must do the digital signature verification of users' digital certificates originally used. If the validation passes, *RA* can trust this user [4].

Subsequently, *RA* randomly generate a random number to challenge the user. Use e to encrypt the random number to the user, allowing users to use their private key to decrypt and after decryption, it is returned to *RA*. *RA* compares it with the previous random numbers. If they are equal, then the user has the private key that corresponds with the e.

After verifying the user's private key's legality, *RA* puts the user's information and public key information to the *CA* Center. *CA* center will also produce a certificate to the user[5], which contains a public key and personal information. When issuing the certificate, *CA* center will use *CA* digital certificate's private key to do digital signature for the unique field of a digital certificate. Signature value is put into a digital certificate. When issuing to the user, the user decrypts the signature with the *CA*'s public key to decrypt the signature value. If they can get the original field, then it trusts the certificate, meaning that the certificate is signed by the *CA*. Otherwise, it does not accept the certificate. Certificate application model is shown in Figure 1.

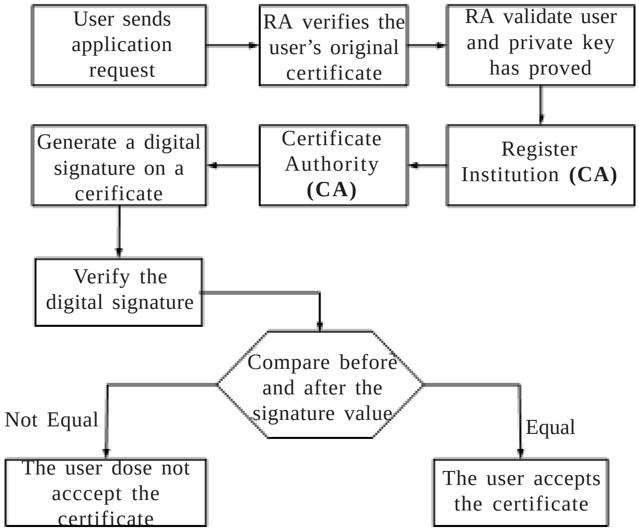

User sends application request
RA verifies the user's original certificate
RA validate user and private key has proved
Register Institution (CA)
Certificate Authority (CA)
Generate a digital signature on a cerificate
Verify the digital signature
Compare before and after the signature value
Not Equal
Equal
The user dose not acccept the certificate
The user accepts the certificate

Figure 1. Certificate Application Model Diagram

3. Secure Digital Certificate Design Based on the RSA Algorithm

Digital certificates generate based on asymmetric key cryptography as early as 1976 W.Diffie.Hellman and Merkle put forward the idea of public key system, which was a revolution of the traditional symmetric key cryptography. It required that the key pairs, one for the *public key* (e), the other is the *private key* (d), and required a secret key can not deduce to another secret key. Meanwhile it used a pair of mutually matching key for encryption and decryption. Individual user has a private key (private key) to decrypt and signature; public key makes public only by the owner for encryption and signature verification.

3.1 X.509 Digital Certificates

X.509 is the certification system standards that ITU established in 1988 in order to achieve the authentication of the remote network users in the opening network. X.509 is based on public key cryptography and digital signatures.

In X.509 the general format of digital certificates is as follows:

Version number: The version number indicates the X.509 version that the certificate data format followed. This article is designed for the current version the most widely used V3 [3].

Certificate serial number: A *CA*-signed certificate's serial number must be unique. Serial number is a long integer and the certificate users must be able to handle up to 20 octets certificate serial number [3].

Signature Algorithm Identifier: algorithm and the corresponding parameters when signing the certificate [3].

Validity: Valid describes the valid time of a certificate. In this period, *CA* guarantee it will maintain information about the status of the certificate.It includes the start time and end time of valid time [3].

Issuer Name: The issuer name describes the information about the certificate issuer *CA*. The institution's name of *CA* that issued the certificate points out the trusted source for sign ing certificates [3].

Subject Name: Subject name describes the entity corresponding to the public key in the main public keys. It means the user's name the certificate belongs to, which is used to prove that the private key is used corresponding to the public key. Each subject distinguished name certified by *CA* must be unique [3].

Subject Public Key Info: Including the subject public key, the algorithm identifier and the corresponding parameters of the used public key [3].

Publisher unique identifier: This data is optional. When the issuer (*CA*) name is re-used for other entities, then use this identifier to uniquely identify the body [3].

This data is also an optional. When the subject's name is re-used in other subjects, then use this identifier to uniquely identify the subject.

3.2 Open the Secret Key Algorithm RSA

The difficulty of a large number of decomposition determines the security of the RSA cryptosystem and multiply a pair of large prime numbers, which easily get the outcome [6]. But it is very difficult to do factorization of most of tarsus. Based on this theory, we can put a pair of primes public as the public key, private key as the prime number. It has gone through a variety of attacks and has not been completely broken. Its algorithm can be expressed as:

Randomly select two large prime numbers p and q (generally about 10 decimal about 100);

In the process of selecting large prime numbers, we must find a method to verify the prime number and here it uses Fermat's Little Theorem. If a number C may be a prime number, then select a base (assumed to be 2), check whether $2p - 1 \bmod p = 1$ is established. Fermat's theorem puts forward if a number is prime, it certainly satisfies the above equation, but it making the establishment of the above equation is not always a prime number.

$$\text{Calculate } n = p * q; \text{ (open) and}$$
$$\varphi(n)\ (p-1) * (q-1) \text{ (keep secret)}$$

Apply program to generate randomly large prime numbers, then use the Tarsus multiplication function to calculate the value of public key n. Large prime numbers p and q respectively are minus 1 and then participate in the multiplication to obtain the Euler function value $\varphi(n)$.

Find a prime number e as the public key (public);

In the above we've got the Euler function value $\varphi(n)$. In the design process, I made the following some settings. When determining whether two numbers are mutually prime, when one number is a prime number, if another is not its multiple, both are coprime numbers. Thus, choose e as a prime number. As long as $\varphi(n)/e$ exists remainder, then the e and $\varphi(n)$ are prime.

Calculate d so as to satisfy and $e * d = 1 \bmod \varphi(n)$ and d as a private public key.

From the above we can see the values of e and $\varphi(n)$. Making use of equation relationship, we naturally can get the value of the *private key d*.

The advantages of RSA algorithm is the following:

1. Security

Security of the RSA algorithm is based on the difficulty of integer factorization in number theory. An n-bit binary number factorization takes $\exp\{[\ln(x) * \ln(\ln(x))]\ 1/2\}$ machine cycles. So it is difficult for the decomposition of large numbers. RSA algorithm is relatively safe.

2. Easy to use and easy to manage keys

Using RSA, even if multiple users communicate secretly, it is unnecessary to exchange keys before communication. But in the asymmetric key cryptosystem, each user need only to protect their own decryption key, while the encryption key is put in the common storage area rather than managed by users.

The inadequacies of the RSA algorithm is mainly inefficient and slow. When implementing it by software, it is slower than DES nearly 100 times. In addition, RSA Security has been seriously challenged. In order to improve the security of RSA, the longer keys must be used.

3.3 Certificate Generation Step

Step of generating a digital certificate is shown in Figure 2.

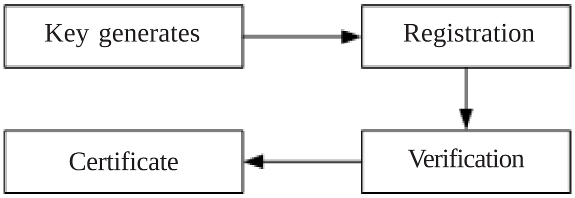


Figure 2. The Digital Certificate Generation Step

3.3.1 Key generation

Users to use some software to generate a pair of public / private keys. The user keeps the generated private key confidential and non-disclose the private key, and then sends the public key and the identity and other information to registered institutions.

3.3.2 Registration

User sends the public key and related registration information as well as all their supporting materials to the registry and sometimes, these materials can also be a paper document. However, in this process, it should be paid attention that users can not put private key to registered institutions but rather to its confidentiality. In fact, the private key is best not to leave the user's computer.

3.3.3 Authentication of data and private key

After the registration process is complete, the registries should make the corresponding authentication to users' materials, mainly from the following two aspects to validate.

First, *RA* needs to validate users' materials, such as the evidence provided, to ensure that they can accept. If the user is an organization, *RA* need to examine business records, historical documents and credit references. If the user is an individual, then it needs the simple proof such as postal address, e-mail address, phone numbers, driver's license, etc..

The second check is to ensure that the user holds the corresponding private key to the public key of the certificate, which is very important. We must prove that this user has the private key, otherwise it will cause legal problems. *RA* can first get a random number to challenge. It takes the user's public key to encrypt and sends the encrypted result to the user. If the user can use their private key to decrypt, it can be confident that the user owns the private key. Chapter 3 describes in detail the whole process of this algorithm.

3.3.4 Certificate generation

After all of the above steps are successful, *RA* passes the user's details to the certificate authority. Certificate authority verifies it and uses the program to generate a digital certificate. Then it sends the certificate to the user while it would keep a record of that certificate.

3.4 RA Authenticates Users' Private Key

In the application for a certificate, the user needs to send their identify to registered institutions, while at this time registered institutions need to verify the user's identity and whether the user has a corresponding private key. It is better to verify the user's identity through the information. This step is very important to check whether the user has a private key corresponding to public key. *RA* tends to generate a random number at this time, which we assume k. *RA* uses the public key to encrypt and the encryption formula is:

$$ke \bmod n = c \ (k < n)$$

After encryption, *RA* sends the value of k to the user [8]. In advance *RA* will inform the user encryption algorithms, allowing users to use their private key to decrypt.

Decryption formula is: $cd \bmod n = b$.

The user sends the value of Y to *RA*. *RA* decides whether the value of k and b are equal. If equal, it means the user has a private key corresponding to the public key. *RA* verifies user's private key process is shown in Figure 3.

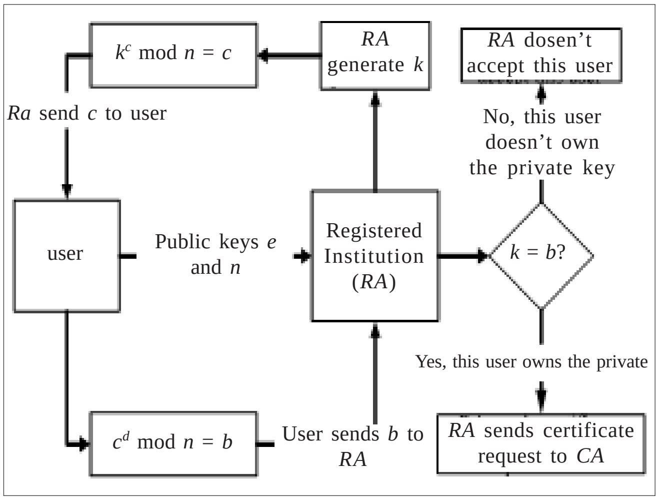

k^c mod n = c
RA generate k
RA dosen't accept this user
Ra send c to user
No, this user doesn't own the private key
user
Public keys e and n
Registered Institution (RA)
k = b?
Yes, this user owns the private
c^d mod n = b
User sends b to RA
RA sends certificate request to CA

Figure 3. The Process of RA Validating User's Private Ke

In order to prevent from replaying attacks, in the program I use function to get the current system time. RA sends number generated to the user to get the current system time T1. When a user decrypts the random number with the private key, he would later return the decrypted number to RA and then get the current system time T2. Set a reasonable time interval, if the time difference between T2 and T1 is over this time interval, it will not accept the returned information of the user.

4. Run Results

4.1 Digital Certificate Application Interface

E-commerce platform is Inseparable from digital certificates. In the commodity trading online, authentication will need to use digital certificates. Before the use of e-commerce trading, it is an essential component to apply for a digital certificate. It is Shown in Figure 4.

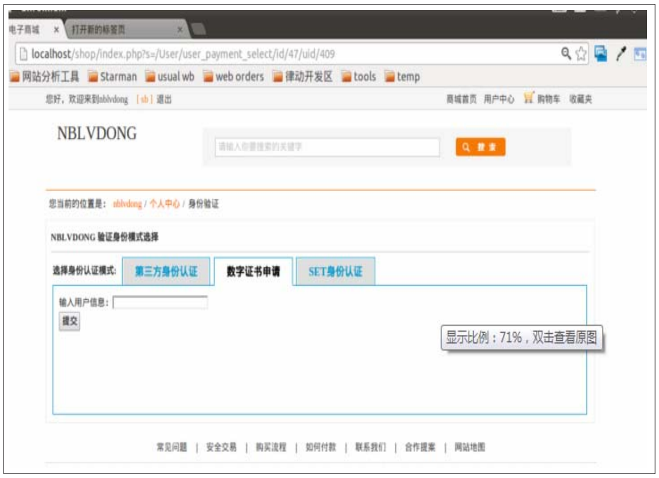
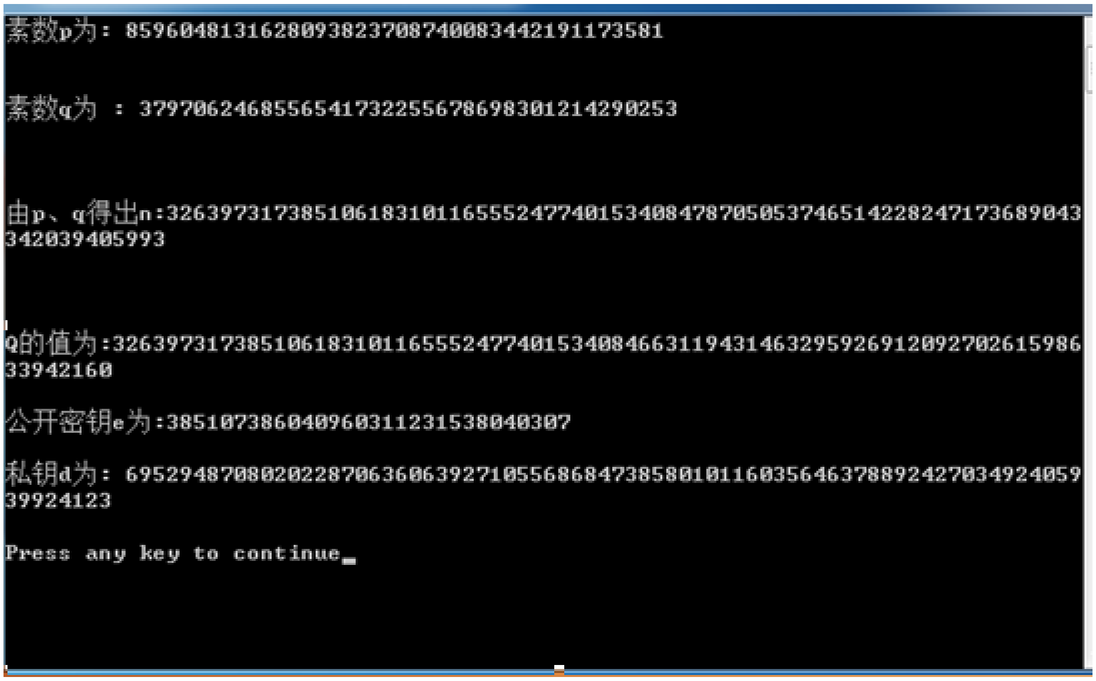

电子商城
打开新的标签页
localhost/shop/index.php?s=/User/user_payment_select/id/47/uid/409
网站分析工具
Starman
usual wb
web orders
律动开发区
tools
temp
您好，欢迎来到nblvdong [sb] 退出
商城首页
用户中心
购物车
收藏夹
NBLVDONG
请输入你要搜索的关键字
搜索
您当前的位置是：nblvdong / 个人中心 / 身份验证
NBLVDONG 验证身份模式选择
选择身份认证模式:
第三方身份认证
数字证书申请
SET身份认证
输入用户信息：
提交
显示比例：71%，双击查看原图
常见问题 | 安全交易 | 购买流程 | 如何付款 | 联系我们 | 合作提案 | 网站地图

Figure 4. Digital Certificate Application Interface

In the real life, when the user request a digital certificate,he must have an original certificate expired, which has the user's public key. The private key corresponding to the public key is known only by the user. Here we make use of platform to generate an RSA key pair for the user. The generation of RSA key pair is basis of the digital certificate, so RSA key pair generation is essential. Here I choose



```
素数p为: 85960481316280938237087400834421911173581


素数q为 : 37970624685565417322556786983012142902553



由p、q得出n:32639731738510618310116555247740153408478705053746514228247173689043
342039405993



Q的值为:326397317385106183101165552477401534084663119431463295926912092702615986
33942160

公开密钥e为:385107386040960311231538040307

私钥d为: 69529487080202287063606392710556868473858010116035646378892427034924059
39924123

Press any key to continue_
```

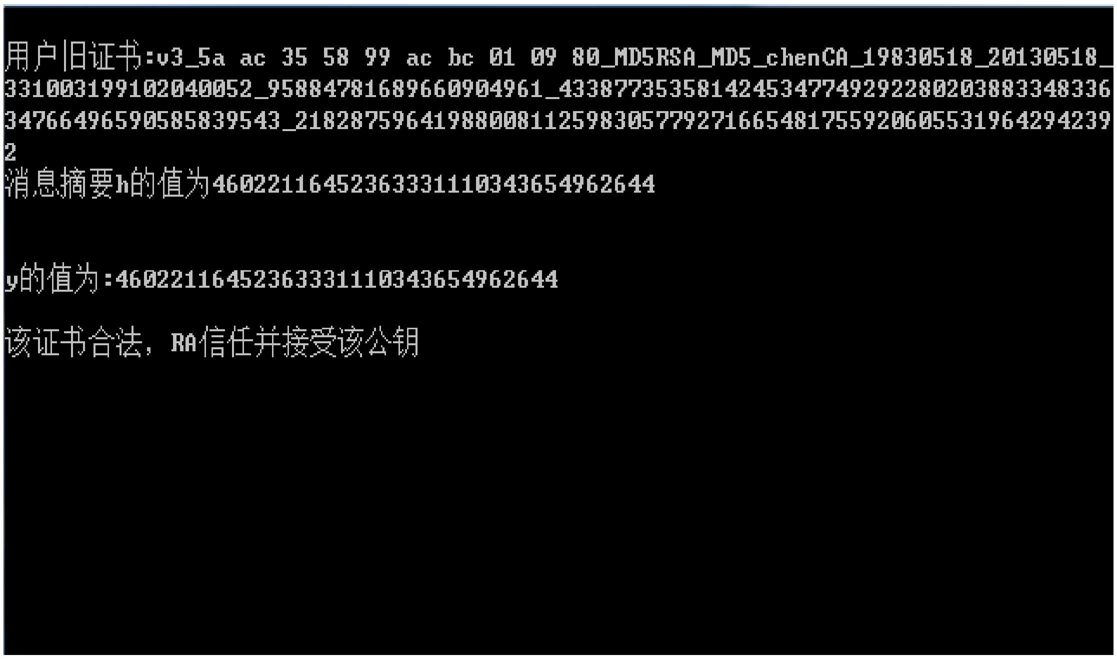
Figure 5. RSA Key Pair Generation Interface

the large prime numbers p and q generating 40 and calculate the values of n, $\varphi(n)$ and d according to the formula, as shown in Figure 5.

After the test of cap software, p and q are primes, e and d are one pair of corresponding public and private key pair. Before generating the certificate, the whole process of generating the key pair is done by the user or registered institution. If it is user-generated, the user needs to keep d secret, and then put the public key and the identity proof to registered institutions. If it is a key pair generated by registered institution, the registered institution need to distribute private key secretly to users without exposure. So the user has a private key and RA institution has a public key.

4.2 RA Verify the User's Public and Private Keys Interface

When users request a new certificate, they will send their own public key to the RA institutions. How RA can trust the correctness of public key? Users must send the certificate once used to RA when applying for a new certificate, let which verify the digital signature of the CA on the digital certificate. If past, RA believes that this public key is one the user ever used and then does related work as shown in Figure 6.

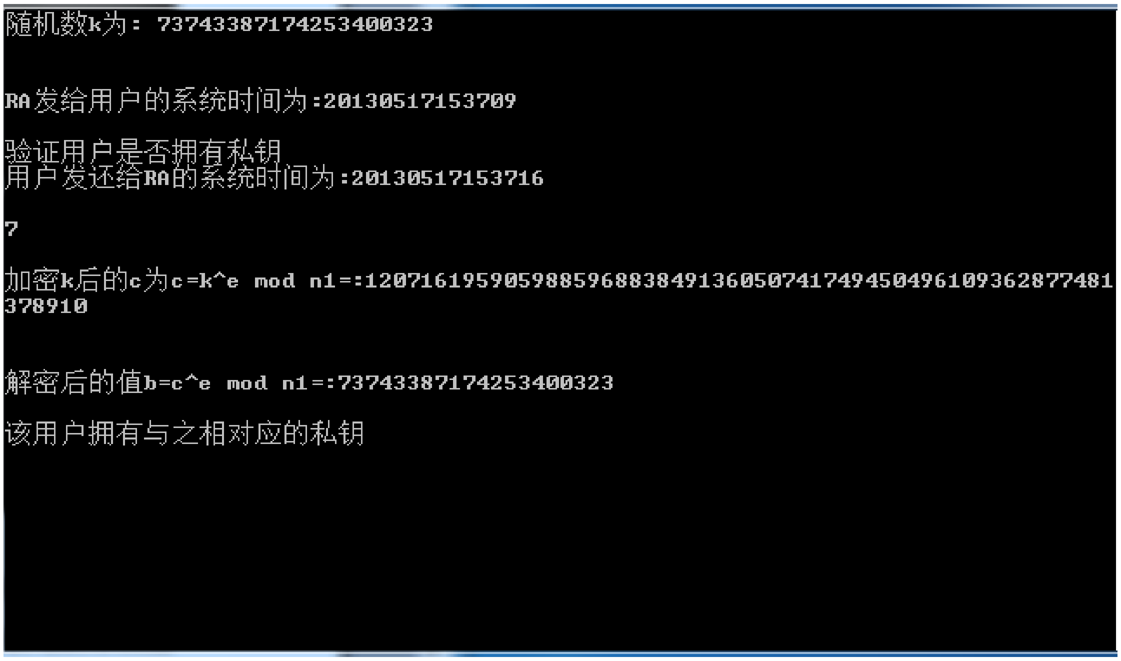


```
用户旧证书:v3_5a ac 35 58 99 ac bc 01 09 80_MD5RSA_MD5_chenCA_19830518_20130518_
331003199102040052_95884781689660904961_4338773535814245347749292280203883348336
34766496590585839543_21828759641988008112598305779271665481755920605531964294239
2
消息摘要h的值为46022116452363331110343654962644


y的值为:46022116452363331110343654962644

该证书合法，RA信任并接受该公钥
```

Figure 6. RA Verify the Legality of User's Original Certificate



```
随机数k为： 737433871742534 00323

RA发给用户的系统时间为:20130517153709

验证用户是否拥有私钥
用户发还给RA的系统时间为:20130517153716

7

加密k后的c为c=k^e mod n1=:120716195905988596883849136050741749450496109362877481
378910


解密后的值b=c^e mod n1=:73743387174253400323

该用户拥有与之相对应的私钥
```

Figure 7. RA Validate User's Private Key

When the user sends the certificate request to registration authority, *RA* must verify the identity of the user, which must check the user's public key corresponding to the private key is correct in the request as shown in Figure 7.

It can see from the map, *RA* first generates a random number and *RA* organizations will acquire the current time. The public key encrypts the random number and the encrypted formula is shown above. The encrypted data and the access of the current time is sent to users, who decrypt it with the private key and the decrypted data back to the *RA*. At this time, *RA* will once again get the current system time. Compare whether before and after two system times is less than 60 seconds to prevent replay attacks. *RA* compare whether the data users decrypt and the random number generated previously are equal. If equal and the time difference is within the allowable range, it means the user has the private key corresponding to the public key. When the value of d the private key is arbitrarily changed, for example, the d-value plus one or minus one, the result will be that a decrypted number and the original random number is not the same. So, RA can use this method to verify the user's private key.

5. Conclusion

Digital certificate is an authoritative electronic document. It provides a way to verify your identity on the Internet to bind the certificate holder's identity to its public key bindings[7]. In order to ensure the integrity and non-distortion of the certificate, certificates also contain the certification authority CA's signature to the certificate. The certificate can provide security services, such as authentication, integrity, confidentiality and non-repudiation. The public key in certificate can be used for data encryption or authentication of signature corresponding private key[9].

This paper not only focuses on the structure and content of universal standard certificate X.509V3 in current world to analyze, but also analyze and describe in detail the whole process of how to generate a digital certificate currently. In *C* language as a tool, it makes the realization of the validation work of the digital certificate's private key and achieve authentication of the private key's digital signature.

References

[1] Xingyi, Li., Jie, Cui (2011). Authentication System's Design and Implementation Based Digital Certificate. *Computer Technology and Development*, 21 (12) 160-163.

[2] Jianye, Wang. (2002). X.509 PKI-depth Discussion and Analysis. 2, p. 97-99.

[3] Xilong, Qu (2006). Digital Signature System's Design and Implementation Based on Digital Certificates. *Computer Engineering and Applications*, 42 (15) 189-192.

[4] Yaohong, Ke., Jianhua, Yu . (2012). Constructed Digital Certificate of Video Security Access Gateway Based on RSA. Shanghai: Fudan university.

[5]Hardjono, T (2005). TCG Trusted Network Connect, TNC Architecture for Interoperability Specification Version 1.0.

[6] Ping, Xiao., Qian, Li. (2013). The Android Data Security Mechanism Based on RSA Digital Envelopes Technology. *Nitinfo Security*, (3) 37-39.

[7] Fubiao, Deng. (2013). The Design and Implementation of A digital Certificate Initialization and Unlocking System. *Nitinfo Security*, (3) 79-81.

[8] Bellare, Mihir., Namprempre, Chanathip., Neven, Gregory. (2009). Security Proofs for Identity-Based Identification and Signature Schemes. *Journal of Cryptology*, 22 (1) 1432-1378.

[9] Ping, Xu. (2011). CA Digital Certificate System's Design and Implementation Based on the X.509 Standard. *Computer and Mathematical Engineering*, 39 (9) 96-98.