The Application of RSA Encryption Algorithm in the Hainan Rural Tourism Management Platform

Huijuan Xie[1,a]

[1]Hainan College of Economics and Business, Haikou, 571127, China
[a]360088369@qq.com

Keywords: RSA Algorithm; Prime; Data Security; Rural Tourism

Abstract: With the development of information technology, such as Big Data, O2O, Cloud Computing, the Internet of Things and Artificial Intelligence, the Hainan Rural Tourism Wisdom Management Platform should provide complete, safe and available information resources. How to make the information correctly generated, stored and transmitted has become very important. The Hainan Rural Tourism Wisdom Management Platform will use RSA encryption algorithm for data encryption to ensure data security. Because the RSA encryption algorithm is a public key encryption algorithm, if the keys are enough long, the information encrypted by RSA algorithm is unable to be cracked, which has been recommended as the public key data encryption standard by ISO.

1. Introduction

The RSA PublicKey Cryptography Algorithm is named after the first letter of three inventors (Rivest, Shamir, Adleman) in 1978, which is the only widely accepted and implemented by the general public key encryption algorithm[1]. With the construction of information infrastructure in Hainan Province, the Hainan Rural Tourism Cloud Computing Center, the Hainan Rural Tourism Big Data Platform, the Hainan Wisdom Tourism Public Service Platform and the Hainan Rural Tourism E-Commerce Platform Project is a major project of the Hainan Rural Tourism Construction, which can help realize the popularization and application of mobile payment in the tourism industry. With the integration of tourism services, management, marketing and the Internet, the encrypted information is everywhere in transmission, storage and exchange process, if the password was maliciously broken will bring serious results, The RSA Public Key Algorithm can secure for the Hainan Rural Tourism Wisdom Management Platform.

2. The Implementation of RSA Algorithm

The RSA public-key cryptosystem is an algorithm that converts a plaintext to its corresponding cipher-text, and then converts the cipher-text back into its corresponding plain-text[2]

RSA is a public-key cryptography algorithm developed based on the presumed difficulty of cracking the factorial of a large integer[3]. The plaintext space K=cipher text space C=Zm(The integer space which can mod M, its value range is 0 ~ n-1)

First, Generating Keys

(1) The two large enough and different prime numbers u and v, which should be kept secretly.

(2) Calculate the value of x and y, x=u×v, x is public. y=(u-1)×(v-1), y is secret.

(3) Select a public random integer s(0<s<y), and gcd (s,y) =1, s is generally a smaller integer. And {s,x} is the public key.

(4) Calculate the value of g,$g=s^{-1} \bmod y$, t is secret, {g,x} is private key.

Second, Encryption and decryption

If the plaintext space K≥x needs group the larger packet to ensure that each packet is satisfied by K<x. The public key {s, x} is used to encrypt, the cipher text is $C=K^s \bmod x$.Tthe private key{g,x} is used for the decryption, and $K=C^t \bmod y$.

3. Three Key Algorithms for effective Implementation of the RSA Algorithm

3.1 The Description of Extended Euclidean Algorithm

In the RSA algorithm, {g, x} is the private key, the value of g is the inverse of s and $g=s^{-1} \bmod y$. The extended Euclidean algorithm will be used to calculate the inverse element, the algorithm is as follows:

```
Function EEA=EEAalgorithm(EEA,M) {
   while(EEA<0)
      EEA=M+EEA;
   end
   l1=M;l2=EEA;o1=0;o2=1;
   q=l1/l2;      o=l1-q*l2;
  while(o>0)
     { temp=o1-q*o2;
       if(temp>0)    temp=temp%M;
       else              temp=(M+temp)%M;
       o1=o2;o2=temp;l1=l2; l2=o;
       q=l1/l2;          o=l1-q*l2;      }
     if(EEA==1)          n=1;
     else
          if(l2!=1)      waring('Nothing!')
          else      n=temp;
return n; }
```

3.2 The Description of the Fast Exponential Algorithm

In the RSA algorithm operation, the Fast Exponential Algorithm was used for the encryption and decryption. Because the number is relatively large and the algorithm is used for simulation, it is stored with long integer. In practical application, because the public key or the private key is so long that the overflow happens, error will occur in operation. The overflow could be solved if these data were stored in the BingInteger class of Java language.

Reducing way can effectively be realized with the exponential operation, but it will need a great amount of memory. Reduced-order can be realized by mod before each execution of the multiplication, which was named fast exponential algorithm. The description of the fast exponential algorithm is that the binary of p is $z_k z_{k-1} \ldots z_0$, and zi={0,1}(i=0,1,...,k), m= $\sum_{i=0}^{k} z_i 2^i = \sum_{z_i=1} 2^i$,then

$$e^p \bmod n = e^{\sum_{z_i=1} 2^i} \bmod n = \left[\prod_{z_i=1} e^{(2^i)}\right] \bmod n = \left(\prod_{z_i=1} [e^{(2^i)} \bmod n]\right) \bmod n$$

```
function FEAalgorithm(int z,int x,int y)
{ m=0;
   t=1;
 for(int i=z;i=0;i--)
   { t=t*t(mod n);
      m=2*m;
      if(x==1)
        { m=m+1; t=t*a; } }
   return t;}
```

3.3 The Two Big Prime Numbers were automatically generated

The RSA algorithm is a popular public key algorithm, which is not only used for encryption, but also for digital signature. Over the past three decades, the RSA algorithm has come through various attacks, which can neither prove nor deny the security of RSA, and been considered as one of the best public key schemes. At critical security areas which are prone to attacks a key management technique is absolutely compulsory [4]. Generating two large prime u and v is the core algorithm of RSA. In order to enhance the operability and applicability of the algorithm, the algorithm is as follows:

```
int bp1,bp2;
function int IsPrime(int num)
{/*Is the data Prime?*/
  int k,t;
     if (num==2)
                return 1;
       else
              if (num<2||num%2==0)       return 0;
              else {
                    t=(int)sqrt(num+1);
                    for (k=3;k<=t;k=k+2)
                          if (num%k==0) return 0;    }
          return 1;}
function int BigPrime()
{int i=0,k1,k2;
  srand((unsigned)time(NULL));
  for(i=0;i<=1000;i++)
    {k1=rand()%1000+1;
    if( Primes(k1)==0)
       continue;
    k2=rand()%1000+1;
    if( Primes(k2)==0)
          continue;
     if(k1!=k2)          break;         }
     bp1=k1;    bp2=k2;}
```

2.4 The Result of the Experiment

The two big prime numbers such as 19 and 23 are selected, the value of s and g is 5 and 317, so the public key is {5,437} and the private key is {317,437}.

4. The Application of RSA Encryption Algorithm in the Hainan Rural Tourism Management Platform

The platform has the functions of transmitting data, storing data, processing data and exchanging data, which should be more secure. Whether the encryption algorithm is used properly, is an important symbol of the platform security. Whether the users use it also depends on its security. The password mechanism of the combination of the application of the platform and service with efficient key management method can solve the cloud data security to a certain extent[5]. Hainan Rural Tourism Management Platform will store data in the cloud, and the cloud service providers will be responsible for data storage, data management and data security, as shown in Figure 1.

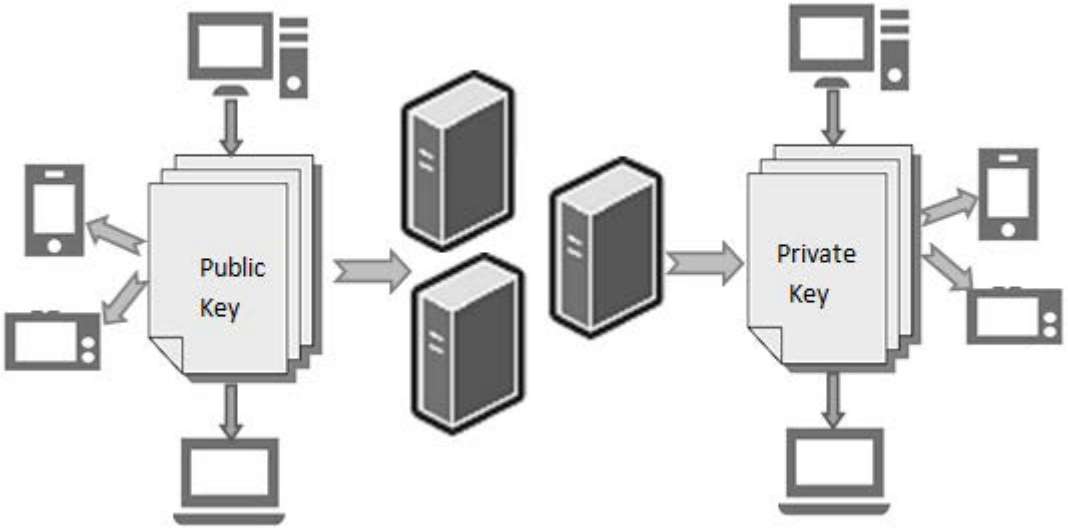

Figure 1

The RSA encryption algorithm is widely used, such as some fragmentation-aware RSA algorithms currently that was found in the literature and can analyze their performance when implemented alone or in tandem [5]. We propose a novel security scheme, called the security system for a 4G environment (Se4GE for short), which as an LTE-A-based system integrates the RSA and Diffie–Hellman algorithms to solve some of LTE-A's security drawbacks where LTE-A stands for LTE-Advance which is a 4G system[7]. a novel RSA hardware implementation with TTA - like architecture. Montgomery modular multiplication based on RNS is adopted[8].

The RSA encryption algorithm is applied to encrypt data in the cloud, because the RSA security depends on intractability of the integer factorization problem, or in other words the difficulty of restoring a public key and cipher text to the plaintext is like the difficulty of decomposing the product of two prime numbers, which is a recognized mathematical problem. RSA and Elliptic Curve Cryptosystems (ECC) are consider as the most popular public key cryptography, In 2009 the IEEE considered the NTRU algorithm as a public key algorithm [9]. RSA algorithm starts with generating a pair of RSA keys, one is kept by users, and the other is available for the public or even registered in a cloud server. In order to improve the intensity of data storage on the Hainan Rural Tourism Management Platform, The RSA key should be longer than 500 bits, which is recommended 1024 bit. Usually combining traditional encryption method with the public key encryption method is used to encrypt during transferring information to reduce the computations. The evaluation of the computational efforts of the four public-key cryptosystems showed that the improvements suggested in this manuscript lessen the performance gaps between RSA and Dickson, LUC and Williams considerably. Still the RSA system remains, as expected, the most efficient[10]

5. Conclusion

The application of big data in the rural tourism is favored, but the data security is considered to be the biggest obstacle for data applications. The application of RSA encryption algorithm provides the guarantee for the tourism information service, effectively enhances the level of internationalization level of tourism services in Hainan province.

Acknowledgement

In this paper, the research was sponsored by the Construction of Evaluation Index System of Hainan Rural Tourism Intelligent Management Platform (Project No.HNSK(JD)16-24).

References

[1] Xiangdong Hu, Qinfang Wei. Applied Cryptography[M].Beijing: Publishing House of Electronics Industry, 2010,25:43-46.

[2] Weng-Long Chang, Kawuu Weicheng Lin. Molecular solutions of the RSA public-key cryptosystem on a DNA-based computer[J], Journal of Supercomputing, 2012(61): 642-672.

[3] Factorial (2013) Wikipedia. http://en.wikipedia.org/wiki/Factorial,2013.

[4] Megha Nema,Shalini Stalin.RSA Algorithm based Encryption on Secure Intelligent Traffic System for VANET using Wi-Fi IEEE 802.11p, Department of Electronics & communication Engineering,2015.

[5] Chen Zhang. the Application of RSA Algorithm in the Cloud Computing[J]. Information Technology and Standardization, 2013(11):11-14.

[6] Joana Sócrates-Dantas* +, Regina Melo Silveira*, Davide Careglio +, José Roberto Amazonas*, Josep Solè-Pareta + , and Wilson Vicente Ruggiero*.Abstracts from the 4th World Congress of the International Dermoscopy Society[J]. Dermatology Practical & Conceptual,2015(5): 137–270.

[7] Yi-Li Huang, Fang-Yie Leu , Ilsun You, Yao-Kuo Sun , Cheng-Chung Chu. A secure wireless communication system integrating RSA, Diffie–Hellman PKDS, intelligent protection-key chains and a Data Connection Core in a 4G environment. The Journal of Supercomputing,2014(67): 635-652.

[8] Wei Guo, Yaling Liu, Songhui Bai, Jizeng Wei,Dazhi Sun. Hardware architecture for RSA cryptography based on residue number system[J]. Transactions of Tianjin University, 2012(18): 237-242.

[9] IEEE Std 1363.1 - IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4800404&contentType=Standards,2009.

[10] Günther Brandner. RSA, Dickson, LUC and Williams: a study on four polynomial-type public-key cryptosystems [J]. Applicable Algebra in Engineering, Communication and Computing,2013(24): 17-36.