http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (9): 1818-1824, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1818.1824

Analysis and Research of the RSA Algorithm

[1]NaQi, [2]Wei Wei, [2]Jing Zhang, [2]Wei Wang, [2]Jinwei Zhao, [2]Junhuai Li, [3]Peiyi Shen,
[4]Xiaoyan Yin, [5]Xiangrong Xiao and [2]Jie Hu
[1]Department of Information Engineering, Shaanxi Polytechnic Institute,
Shaanxi, Xian'yang, 712000, China
[2]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[3]National School of Software, Xidian University, 710071, Xi'an, Shaanxi, China
[4]Department of Computer Science and Technology, Northwest University, Xi'an 710127, China
[5]School of Information Engineering, Zhejiang Agriculture and Forest University, China

Abstract: With the continuous development of society and the prevalence of computer and network technology. How to ensure the security of information in the course of transmission have become the most important things for people at present. With this background, we studied how to realize encryption and decryption of the RSA (Initials of Ron Rivest, Adi Shamirh, LenAdleman) encryption technology. This study mainly introduces the application of RSA algorithm in encryption and decryption, mentions the technology of digital signature. Also introduces in the process of implementation of RSA algorithm in Visual Studios environment and operation results. Using this system for encryption and decryption of information, theoretically, good results were obtained in safety and reliability.

Key words: RSA algorithm, encryption, decrypt, digital signature, application, security

INTRODUCTION

Encryption technology does not appear now that originated in 2000 BC (centuries), although the name is different (even not call encryption ago), but the concept as a kind of encryption, it was born in the early centuries ago, their idea is the same. In order to protect the information in the transmission process, prevent important or private information is intercepted and steal. Even if the access by third parties, not decrypt the corresponding method, the information has no value in use, it will not cause any loss.

The origin of the encryption technology what we now use, is proposed by Diffie and Hellman in the paper of "New Direction in Cryptography" in 1976 (Kahata, 2005). R. Rivest, A. Shamir and L. Adleman realize a public key cryptosystem that now called RSA public cryptosystem (Chen, 2012). The algorithm is considered to be the most perfect and the most mature public-key cryptosystem that is widely used in various fields.

This study focuses on algorithm principle, application, security and analysis and researches of the problem that existed in the algorithm. And the encryption and decryption of RSA technology is implemented in Visual Studios environment.

Basis of cryptography: Cryptography has a long history, but in general it is still very strange, because it is only in a small area, such as the military, intelligence, diplomatic and other sensitive sectors (Wei *et al*., 2011). Computer cryptography is the study of computer information encryption, decryption and transform scientific, interdisciplinary mathematics and computer, is an emerging discipline (Shi, 2007).

Cryptographic techniques are used to ensure the confidentiality, integrity and authenticity of electronic data. Confidentiality is to encrypt the data, so that the illegal user can not read data information read-out information to the legitimate user can use key. The integrity of data integrity, authentication and to determine whether the data is illegal tampering, correct and complete information to ensure that legitimate users. Authenticity is the authenticity of the data sources, the authenticity of the identification of the data itself, can ensure that legitimate users are not deceived (Shi, 2007). Simple process is shown in Fig. 1.

Encryption description: The encryption algorithm is divided into two kinds, symmetric and asymmetric encryption. Using symmetric encryption, the two parties communicate with the common key that needing the only one. Regardless of the sender or receiver of encryption

Corresponding Author: NaQi, Department of Information Engineering, Shaanxi Polytechnic Institute, Shaanxi, Xian'yang, 712000, China

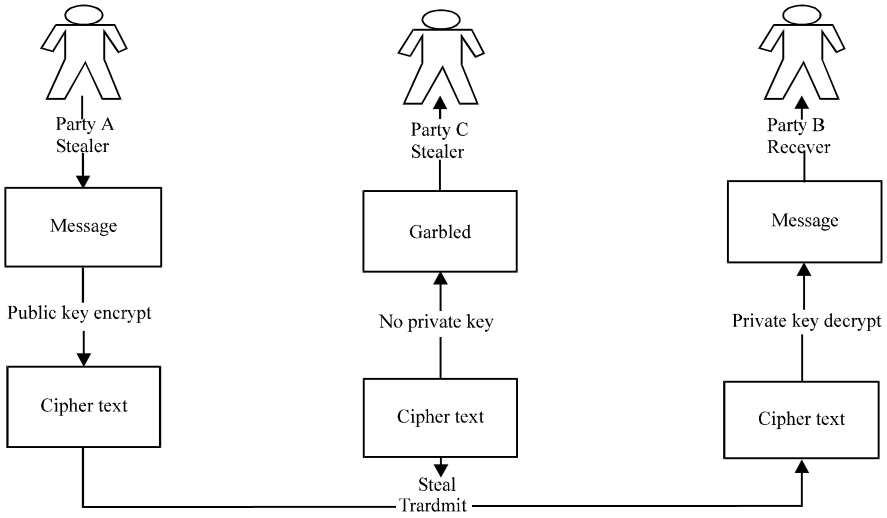

Fig. 1: Process of RSA encryption and decryption

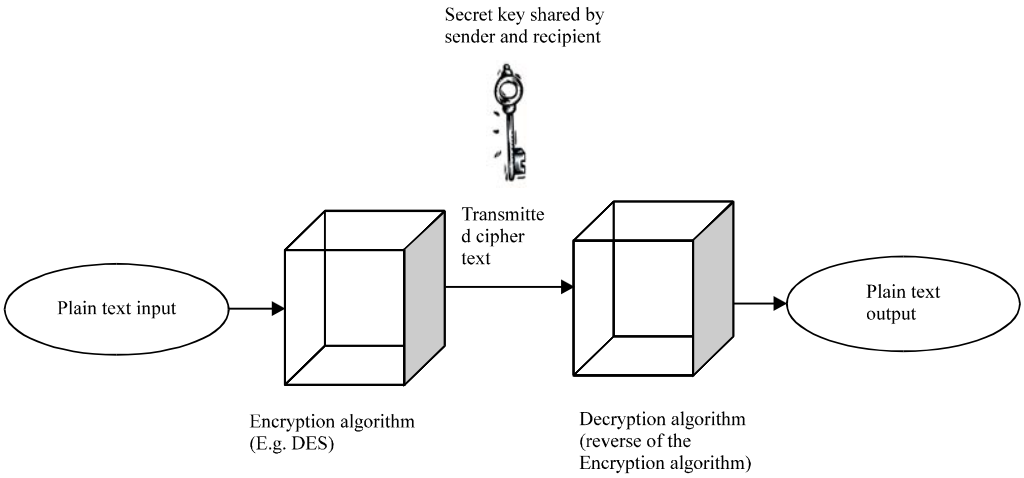

Fig. 2: Symmetric cipher model

and decryption use the key. If the key access by third parties in the process of transmission, Plus on the key has no meaning. How to put the key to each other's hands is the shortcoming of the algorithm. The algorithm of the model is shown in Fig. 2.

Asymmetric encryption algorithm of RSA that is different from symmetric encryption algorithm needs two keys, a public key, a secret key. The two of them appear in pairs, if the public key to encrypt data, only with the corresponding private key can decrypt; if the private key to encrypt data, so only with the public key can decrypt the corresponding. Because the encryption and decryption using two different keys, so this algorithm is called asymmetric encryption algorithm (Cai and Lu, 2011). Party A generates a pair of keys and one of them as a public key open to the other side, Party B use the key which from the party A to encrypt the confidential information and then sends the information to the party A; party A decrypt the encrypted information using the dedicated key that he preserved. Party A can only decrypt any information that encrypt by its public-key by a dedicated key. The algorithm of the model is shown in Fig. 3.

RSA algorithm: The RSA algorithm is a kind of asymmetric encryption algorithm which appeared in 1978. The algorithm is public key encryption algorithm which is a widely accepted and implemented by public. It is a kind

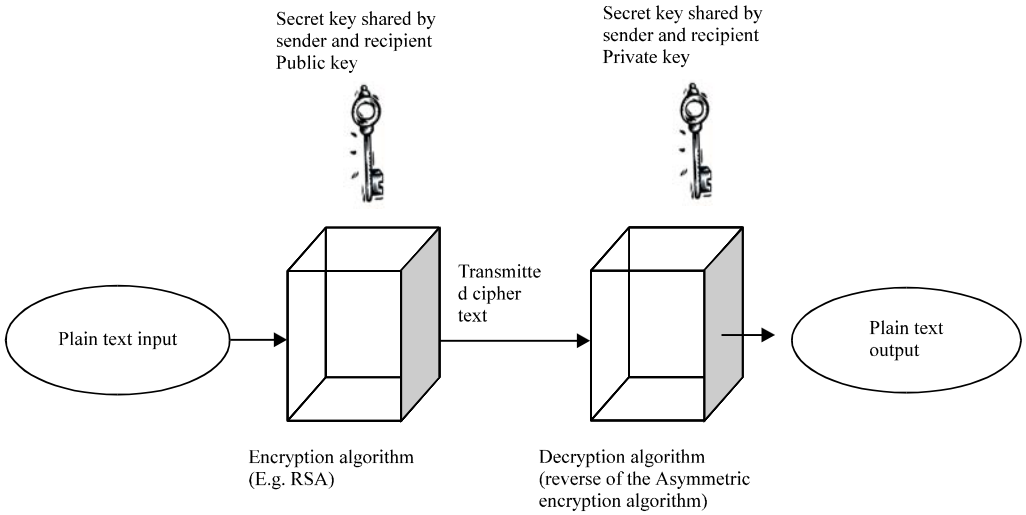

Fig. 3: Symmetric cipher model

of algorithm that can be used for not only data encryption but also digital signature. Nearly forty years, has experienced all kinds of attacks and the test, has been gradually accepted by the people and is considered to be one of the best public key schemes.

The algorithm is based on large integers and prime testing; its mathematical basis is the Euler theorem.

In the Elementary number theory; its security is based on the difficulty of factoring large integer (He and Wu, 2004; Buchmann, 2001).

Key generation: First, we select two big prime number of the same length randomly: p, q, n = p*q, t = (p-1)*(q-1), then we select the number e, its range is more than 0 and less than t. we usually use the value of e is 3, 17, 65537 (216 plus 1) and e must meet the Condition is d*e %t = =1, then we can get the value of d. The result is we get the four numbers n, t, e, d; the e is the encryption key, the d is the Decryption key, open n and d to public, keep p, q and e to anybody.

Although, the transformation of encryption and decryption is the inverse, the private key system handles the data as a bit, but the public key system handles the data as a number that perform function operation and the mathematical function is one-way. It is to say, it can easily come true from one side, but very difficult to another side, so simple steps unable to decrypt the cipher text (Wang and Song, 2011).

Encryption algorithm: The known-plaintext x(x<n) and group x into character blocks, the length of each plaintext message Xi must meet 0<xi<k (where k is the length of n) and calculate the cipher text C = xe (MOD n).

Decryption algorithm: The known cipher text c and the private key (n,d), can calculate the plaintext x = Cd (mod n)?

The example of RSA algorithm: Known p = 11, q = 19, gotten n = 209, t = 180. Select the number e randomly e = 7, meet 0<e<t, According to the formula of d*e%t = =1 d = 103 can be obtained, d is a private key. Open (n, e), keep (n, d). If we need to seed the information x = 65, using (n, e) = (209, 7) to calculate the encrypted values: C = xe(mod n) = 657 mod 209 = 56, When received c = 56, using (n,d) = (209,103) , calculate x = Cd(mod n) = 56103 mod 209 = 65.

Exchange the key of the symmetric encryption algorithm (Chen and Zhu, 2006): Because of asymmetric encryption algorithm is t more slowly than symmetric encryption algorithm, so asymmetric encryption algorithm is usually used to secure encryption key of the symmetric encryption algorithm in the practice, but symmetric encryption algorithm is usually used to secure the Communication of message. It is also to say, Asymmetric encryption algorithm is mainly used for the encryption key of the symmetric encryption algorithm.

The process of exchange the session key:

- A uses RSA algorithm to generate their own public key (n, e) and the private key (n, d) and sends the information to B that contains the public key (n, d) and ID of A
- B gets the session key k and uses the public key encrypt the message to A, Ke mod n

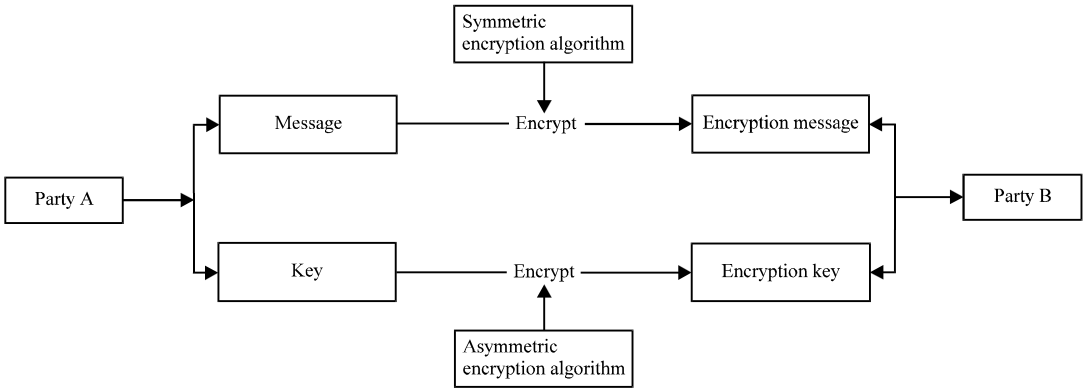

Fig. 4: Exchange of symmetric encryption algorithm key processes

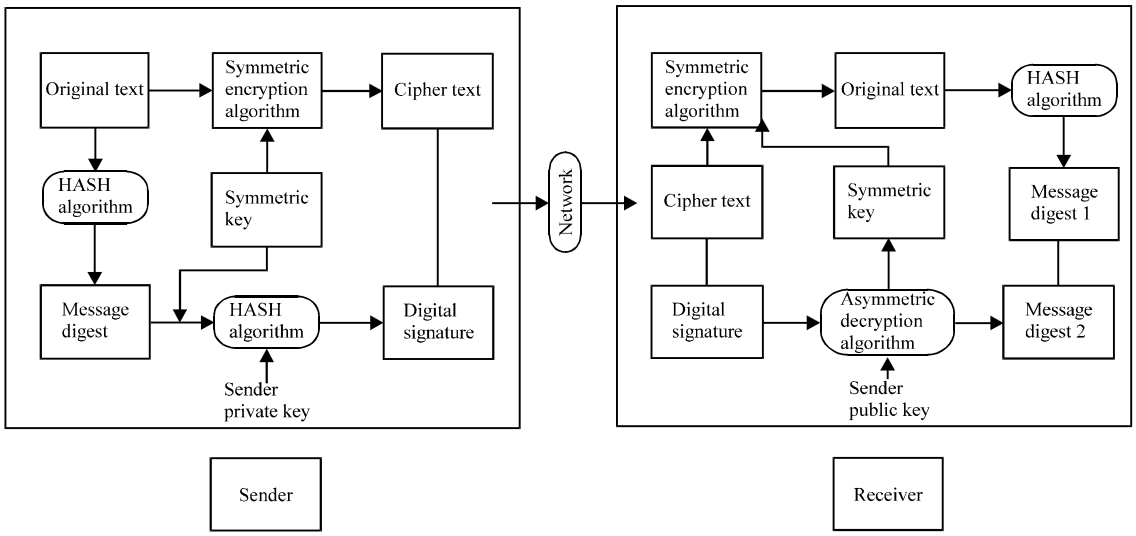

Fig. 5: RSA algorithms in the digital signature

- A uses his private key to decrypt the Ke mod n, then can get K. In this way, A and B can communicate with symmetric encryption algorithm and the session key K. Simple process is shown in Fig. 4

Digital signature: The RSA algorithm uses the public key to encrypt and the private key to decrypt in the encryption/decryption process. The private key is used to encrypt and the public key is used to decrypt in the digital signature. The sender using HASH algorithm to calculate the hash value of the file M, then generate the digital signature C from using the key to encrypt digital abstract and then M C together and sent to the receiver. The receiver receives the file M1 and digital signature C1, needs to verify that M and M1 are identical.

The verification process is to get hash value H1 of M1 using the HASH function and get the H2 from the decrypt digital signature of C1 by using the public key. Compare H1 to H2 is the same (Shi *et al*., 2008). Information transmission is security if the same. The specific process is as follows as shown in Fig. 5.

IMPLEMENTATION OF RSA ALGORITHM IN VISUAL STUDIOS

In the program, the user can encrypt and decrypt the digital, Chinese characters, letters and other information. In the encryption and decryption of digital information, the user directly inputs the encrypted and decrypted number according to the suggested of the procedure, then can get the encryption or decryption information of the

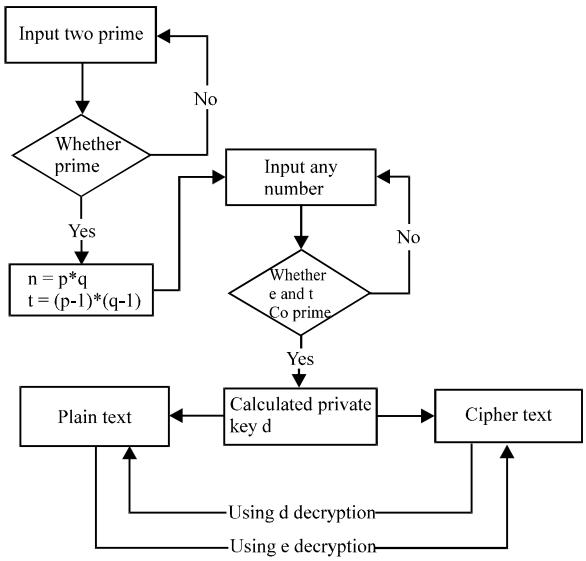

Fig. 6: Flow chart

```
Please enter the two prime numbers:p,q397 97
Calculated the n is38509
Calculated the t is38016
Enter a public key e: 5
Calculated d is30413
Encryption please input 1
Decryption please input 2
1
Please input the message m:57
27441
Ciphertext is 27441
Press any key to continue
```

Fig. 7: Result of encryption

```
Please enter the two prime numbers:p,q397 97
Calculated the n is38509
Calculated the t is38016
Enter a public key e: 5
Calculated d is30413
Encryption please input 1
Decryption please input 2
2
Please input the ciphertext c:27441
57
The message is 57
Press any key to continue
```

Fig. 8: Result of decryption

number which inputted. We don't need to do any treatment to the digital information. If the user input the information that is made of Chinese characters, we turn the information into URL code. Finally we turn the URL code into ASCII code to encrypt and decrypt. If the user input the information is composed of string, the information is converted to ASCII code to encrypt and decrypt. If the information is a very long string, we need to first packet encryption information.

In the program, the main function gets the N and its Euler number T in according to the prime p and q that the user inputs and given by the user's public key e, calls the function fun (E and T) to determine whether the cop rime and got the private key D. user chooses the information is to be Encrypted or decrypted, calls the function my (encryption), realize the computation of exponentiation and multiplication. The specific process is shown in Fig. 6. The result of the Encryption is shown in Fig. 7. The result of the Decryption is shown in Fig. 8. And the code is as follow:

```
Unsigned long my encryption (unsigned long x, unsigned long y, unsigned long z)
  {Unsigned long r = 1;
  y =y+1;
  while(y! = 1)
  {
  r = r*x;
  r = r%z;
  y--;
  }
  printf("%d\n",r);
  return r;
  unsigned long fun(unsigned long a, unsigned long b)
  {
  unsigned long t;
  while(b)
  {
  t = a;
  a = b;
  b = t%b;
  }
  if(a = = 1)
  return 0;
  else
  return 1;
  }
```

The result of the Encryption is shown in Fig. 7. The result of the Decryption is shown in Fig. 8.

Safe of RSA algorithm: The system structure of RSA algorithm is based on the number theory of the ruler. It is the most security system in the key systems. The safe of RSA algorithm bases on difficulty in the factorization of the larger numbers (Zhang and Cao, 2011). If you want to break the information, you need to decompose a large number; it is also to say, it is difficult to get the private key through the factorization from a public key. For example, in order to decompose a large number of RSA-129 that factories a 129 bit decimal 425 bit on April 1994, more than 600 volunteers participated in the cracking activity, opened more than 1600 workstations, mainframes and supercomputers decomposition, spent 8 months time, finally decomposed RSA129 problem in public key.

But research shows that, since 1994 to complete the work to decipher and faster decomposition factor calculation method is proposed. Therefore, a large number of recent lower quartiles (512bit binary number) have been successfully decomposed, it tells people, the encrypted using the RSA algorithm, in the key generation, try to ask n is very big, so the attacker to break the success of t = (p-1) * (q-1), it is very difficult. In order to make the RSA safety, it must choose a large p and q; use a longer key is beneficial and harmless. Users' usually choice more than 100 decimal digits, so the attacker cannot decompose the N in polynomial time effective internal.

DISADVANTAGE OF RSA ALGORITHM:

- Fake public-key algorithms. The user should not worry if public key leak, but need to consider someone takes another's place by counterfeiting published false public key, so it should be possible to widely publish the right key to public to prevent counterfeiting
- Complexity of the key creation. Because of the RSA algorithm is limited by the prime and efficiency of generating primes is relatively low, so it is difficult to achieve a secret once (Internet Data Center, 2011)
- Security needs to be proofed. The RSA security depends on the difficulty of factoring large numbers, but is equivalent to factoring has not been proved theoretically, because there is no proof of cracked RSA will need factorization. If there is an algorithm can fast decompose a large number, so the RSA algorithm's security would be threatened. In addition, the computational ability of the computer to continuously improve, the cost of computer to reduce, the parallel technology of the computer to develop, then attack the RSA algorithm will get huge growth ability
- Slow of the speed. The RSA encryption and decryption algorithm need a lot of calculation and the speed is slowly, compared with the symmetric cryptographic algorithm thousands of times slower. With the development of large number of decomposition technique, key length would increase to ensure safety, so the computation will be greater

APPLICATION AND DEVELOPMENT PROSPECT OF RSA ALGORITHM

Since the proposed from the nineteen seventies, through the practice of 20 years, has been widely used, has become a most popular encryption standard. With the development of computer network and e-commerce technology, provides a broader space for the application of RSA technology. In many hardware, RSA software and library software product kernel, is convenient for people to use. For instance, in terms of hardware, the technology of IC is mature that used in all kinds of electronic products (Zhang *et al*., 2009); in terms of software, mainly used in the encryption connection, digital signatures and digital certification on the Internet, In addition, the household IE browser, integrates and uses RSA encryption technology, combined with the MD5 and SHA1 mainly used for digital certificates and digital signatures. For users accustom to using online shopping and online banking, almost use the RSA technology every day (Si and Tang, 2009).

With the year-on-year increase of the amount of data and the continuous improvement of people's needs, RSA faces various challenges, application security, data security and privacy, cloud security, denial of service attacks, Advanced Persistent Threats (APTs), mobile security and so on. There are the prospects of the development in the few years.

CONCLUSION

In this study, based on fully research and a deep understanding of the principle of tradition RSA algorithm, the RSA algorithm is implemented in VC environment and analyzes the security of RSA algorithm and its disadvantages. On the whole, the RSA algorithm is a good algorithm. But in the application of the RSA algorithm, RSA algorithm also has many problems, such as the public key is correct, the encryption and decryption speed is very slow and the key generation is very troublesome. We take into account the weaknesses while use the RSA algorithm and make an attack on the RSA. Widely used symmetric encryption algorithm and asymmetric cryptographic algorithm combines, advantages and disadvantages of complementary of two algorithm, Longer encrypted with a symmetric cipher encryption algorithm key file and then use the RSA algorithm to encrypt files, so an excellent solution to the symmetric key distribution problem (Guo, 2011).

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their valuable comments. This program is supported by Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No.2013JK1139). Our project is also supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No.

2012JM8047) and by Science and Technology Project of Xi'an (CX1262⑨). And this project is also partially supported by NSFC Grant (Program No. 61072105, 61007011, No. 61172018 81201179, 61100236, 61202393, 11226173) and Beilin District 2012 High-tech Plan, Xi'an, China.

REFERENCES

Buchmann, J., 2001. Einfuhrung in die Kryptographie [Introduction to Cryptography]. 2nd Edn., Springer, Berlin, Germany.

Cai, C. and Y. Lu, 2011. Asymmetric encryption JAVA and VC. Comput. Knowled. Technol., 18: 4306-4307.

Chen, C. and Z. Zhu, 2006. Application of RSA algorithm and implementation details. Comput. Eng. Sci., 9: 13-14.

Chen, Z., 2012. The encryption algorithm and security of RSA. J. Hengyang Normal Univ., 12: 69-69.

Guo, H., 2011. Efficient implementation of RSA algorithm based on C language. Mod. Comput., 8: 14-14.

He, C. and H. Wu, 2004. Public key RSA algorithm is applied to several problems. Mod. Comput., 178: 72-74.

Internet Data Center, 2011. Data encryption technology of [DB/OL]. http://zy.zhku.edu.cn/info/kcln/10/3.htm.

Kahata, A., 2005. Cryptography and Network Security. Tsinghua University Press, Beijing, China.

Shi, Z., 2007. Computer Network Security Tutorial. Tsinghua University Press, Beijing, China.

Shi, Z., Q. Tan and H. Duan, 2008. The research and application of the RSA algorithm in the digital signature. Microcomput. Appl., 6: 50-51.

Si, H. and B. Tang, 2009. Application of RSA and its application in an encrypted file. Comput. Telecommun., 6: 76-77.

Wang, H. and R. Song, 2011. The length of the key influences the degree of security of the RSA system. Comput. Knowledge Technol., 10: 7104-7105.

Wei, X., Z. Li and Y. Zhu, 2011. On the RSA algorithm and application. J. Honghe Univ., 4: 31-32.

Zhang, S., W. Wan and J. Zhang, 2009. Applied Cryptography. Xi'an Electronic and Science University Press, Xi'an, China.

Zhang, Y. and T. Cao, 2011. Application of encryption based on RSA algorithm. Sci. Technol. Advisory (Technol. Admin.), 25: 79-80.