Optimization of Encryption Algorithm for Administrative Examination and Approval Data

Xihua Shen, Zhiding Liu, Qian Hu

Renhe Hospital of China Three Gorges University, Yichang 443000, Hubei, China

Abstract
The application of the standard RSA encryption algorithm in administrative examination and approval data encryption is inefficiency and the encryption result is not ideal. This paper presents an administrative examination and approval data encryption model based on real-time and efficiency optimization RSA algorithm. First it USES the modulus algorithm to reduce the number of nonzero elements and binary length of index to reduce the iteration number; After Lehmann test prime failure, it uses random search method to plus 2 on the original, instead of generating a random number again for the next cycle to improve the speed of prime number detection. The simulation experiments show that the proposed RSA algorithm based on real-time and efficiency optimization is superior to the traditional AES algorithm and the RSA algorithm in terms of efficiency and encryption performance.
Key words: RSA ENCRYPTION, ADMINISTRATIVE EXAMINATION AND APPROVAL, DATA ENCRYPTION, MODULUS OPERATION, INCREASING RANDOMLY.

1. Introduction

As the rapid development of world economy, the quality and efficiency has become an important factor in competition, so to strengthen quality control, improve the work efficiency is also gradually become the main part of management. Increase the degree of office automation has been the target of everyone, whether enterprises, schools, or the party and government organs are looking forward to the office automation [1]. We can take advantage of the network communication foundation and advanced network application platform to build a safe, reliable, open and efficient information, network and office automation, electronic information management system for medium-sized enterprises and institutions. With the popularity of online office system in various enterprises and institutions, people pay more and more attention to security problem, especially the potential safety hazard of online office system. Only by understanding the current security problems of the online office system, can we take remedial measures to strengthen security when designing OA system [2].

As a basic data encryption technology is the foundation of all communication security, data encryption process is the implementation of all kinds of encryption algorithms, and it provides a lot of security at the expense of a little. Montgomery put forward the rapid mould power operation method [3], many scholars proposed many algorithms to improve the encryption speed of RSA, for example Chung - Hsien Wu reduced the size of cipher text and the power based on the improved algorithm of Chinese remainder theorem, and then used the Chinese remainder theorem for decryption [4]. Yunfei Li put forward an improved RSA algorithm of fast decryption, the algorithm improved the signing and decryption speed mainly for multiple prime decryption RSA algorithm [5]. M. Frunza put forward a fast RSA algorithm encryption method, which improved the encryption key generation to enhance the security of the algorithm [6]. The earli-

est knapsack encryption algorithm is put forward by Merkle - Hellman, which transfers super increasing sequence algorithm into a general sequence of backpack through certain transformation, based on easy solution of super increasing sequence and the intractability of backpack. Lagarias - Odlyzko and Brickell respectively puts forward the algorithm to solve the problem of low density backpack. If a backpack sequence's density is lower than 0.645 according to the algorithm, Lattice Reduction Algorithm may be used for decoding [7]. Afterward Coster put the density value up to 0.9408, and at the same time pointed out that only the density of a safe knapsack algorithm is higher than 0.9408, can the algorithm resist low density algorithm, but if the density of a knapsack algorithm is higher than 1 , the solution is not the only. Weidong Zhang designs an easy solution, but not the super increasing knapsack sequence and then converted it into general sequence with high density [8]. Based on RSA and MH algorithm thought, more public key cryptography system is put forward, such as the Rabin algorithm based on quadratic residue problem, ElGamal algorithm based on discrete logarithm, based on elliptic curve discrete logarithm problem on the ECC algorithm [10]. In order to give full play to the symmetric key algorithm and public key algorithm their, Guo encrypted plaintext with triple DES first, and then delivered the key using the RSA public key algorithm [11]. This combination of the two modes has become the main mode of encryption system. But in public key cryptography system, because anyone can use the public key, gave an attacker useful information, thus to protect the public key will become very important. Denning proposed a new method to protect the public key and signature key, ensuring a more secure communication [12].

As there are problems in the application of the standard RSA encryption algorithm in administrative examination and approval data encryption, this paper proposes a optimization of RSA algorithm based on real time and efficiency of administrative examination and approval data encryption model, and a simulation experiment was carried out, verifying the validity of the improvement strategy.

2. Encryption performance analysis of RSA algorithm

RSA algorithm is representative among the public key encryption algorithm. The algorithm can resist all known password attacks so far based on the knowledge of number theory; the security is based on the large integer factorization mathematical problem. Compared to Symmetric key encryption algorithm, the algorithm increased the digital signature function. RSA has the fundamental characteristics of public key systems, such as:

(1)Use PK (public key) to encrypt P (plaintext), and then use SK (secret key) decrypt P ,

$$P = D_{SK}[E_{PK}(P)] \quad (1)$$

(2) Encryption key PK can only be used to encrypt but not to decrypt,

$$D_{SK}[E_{PK}(P)] \neq P \quad (2)$$

(3) SK cannot be deduced from the known PK .

(4) Encryption and decryption operations can be interchanged,

$$E_{PK}[D_{SK}(P)] = P \quad (3)$$

From these characteristics, in public-key encryption system PK can be delivered to users. If sender A wants to send plaintext to receiver B, he can search the public key PKB from receiver B, encrypt the plaintext P with encryption algorithm, and then the ciphertext $C = E_{PKB}(P)$ can be obtained. After the recipient B receives the ciphertext C, decryption can be finished with decryption key known only by him, and then plaintext $P = D_{SKB}[E_{PKB}(P)]$ can be restored. Eavesdropper cannot restore the plaintext although he intercepted ciphertext because of the lacking of SKB .

Theoretical of RSA system depends on the famous Euler's theorem: Two positive integers a and n are relatively prime, then $a^{\phi(n)} = 1(\mathrm{mod}\, n)$, where $\phi(n)$ is positive integer number, $\phi(n)$ and n are coprime, $\phi(n)$ is less than n. The core idea of RSA public key technology is:

(1) p and q are two sufficiently large primes(decimal number with larger than 100 bits), p and q are confidential.

(2)Calculate $n = pq$, n is public (solve p and q is a waste of time by factorization).

(3)Solve the Euler function of n : $z = \phi(n) = (p-1)(q-1)$ 。

(4)Select integral e under the condition $[e, z] = 1$, that is e and $\phi(n)$ are coprime, e is a public.

(5)Calculate d to meet: $de = 1(\mathrm{mod}\, z)$, d is confidential.

To understand the performance of RSA password, this article will compare it with the AES key analysis.

AES algorithm uses a symmetric block cipher system, encryption and decryption keys are the same. The encrypt method is:

$$s'(x) = c(x) \cdot s(x) \bmod (x^4 + 1) \quad (1)$$

$$c(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\} \quad (2)$$

Among them, $s(x)$ is original state, $s'(x)$ is the transformed state, $\{\}$ is the number of byte.

$$s'(x) = s'_{0,c} + s'_{1,c} \cdot x + s'_{2,c} \cdot x^2 + s'_{3,c} \cdot x^3 \quad (3)$$

$$s(x) = s_{0,c} + s_{1,c} \cdot x + s_{2,c} \cdot x^2 + s_{3,c} \cdot x^3 \quad (4)$$

Multiplied $c(x)$ and $s(x)$ then $\mathrm{mod}(x^4 + 1)$, $s'_{0,c}$ is the coefficient of constant term, use $x^i \bmod (x^4 + 1) = x^{i \bmod 4}$:

$$s'(x) = \{02\}s_{0,c} + \{03\}s_{1,c} + \{01\}s_{2,c} + \{01\}s_{3,c} \quad (5)$$

The remaining items may be obtained similarly, and then formula (1) can be represented with matrix as:

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} \quad (6)$$

That is, mix columns transformation is equal to intermediate state data left multiplying a constant matrix according to column.

The encryption performance comparison results of RSA algorithm and AES key is shown below:

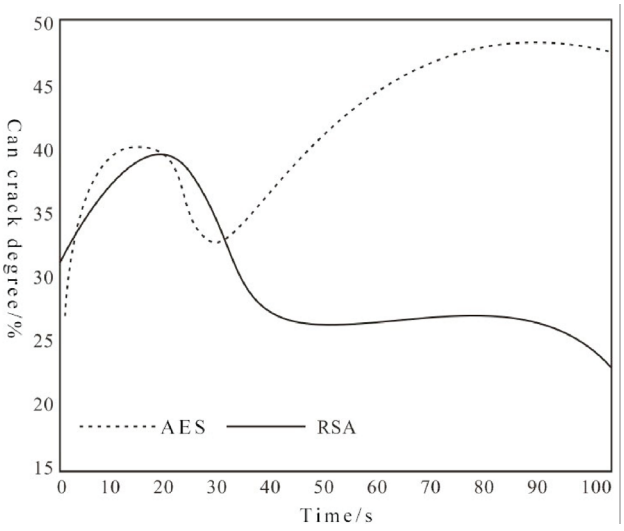

Figure 1. RSA encryption algorithm AES algorithm performance comparison

From Figure 1, Compare to AES encryption algorithm, RSA algorithm has a better encryption performance, but still cannot to achieve the high accuracy encryption requirement.

3. Instantaneity and efficiency optimization of RSA Encryption Algorithm

3.1. Real-time optimization based on modular arithmetic

Let be i、 $j \in \left\{0,1...,\frac{M-1}{2},\frac{M+1}{2},...,M-1\right\}$, by multiply congruence peace the rest of the symmetry:

$$(M-i)^2 = i^2 (\mathrm{mod}\, M) \quad (7)$$

$$(M-i)(M-j) = ij (\mathrm{mod}\, M) \quad (8)$$

$$i(M-i) = (M-i)j = -ij (\mathrm{mod}\, M) \quad (9)$$

Make A_i the intermediate result after the i iteration, x is the encrypt plaintext, then

$$A_i、\ x \in \left\{0,1...,\frac{M-1}{2},\frac{M+1}{2},...,M-1\right\} \quad (10)$$

Two basic operations are respectively $A_i^2 (\mathrm{mod}\, M)$ and $A_i^2 (\mathrm{mod}\, M), i = 1,2,...,1$.

Substitution principle is: if A_i、 $x > \frac{m-1}{2}$, then A_i or x multiply congruence calculation is replaced by $M - A_i$ or $M - x$ for square remaining. According to formula (7) ~ (9), the final results does not change, but as we reduce the modulus processing time and multiplication, the whole algorithm computation speed is up by more than 20% on average.

Iterations depend on its hamming weight, that is, the number of nonzero elements and index of the length of the binary. If we can effectively lower the hamming weight of index of binary, iteration steps must also go to reduce.

A binary "1" can be represented as the follow, we use "1" to present "-1",

$$\begin{cases} (11)_2 = (100)_2 - (1)_2 = 10\bar{1} \\ (111)_2 = (1000)_2 - (1)_2 = 100\bar{1} \\ (11111)_2 = (10000)_2 - (1)_2 = 1000\bar{1} \\ (11...1)_2 = (100...)_2 - (1)_2 = 10...\bar{1} \end{cases} \quad (11)$$

If there are k ($k \geq 2$) "1" after "110" and "1110", we also undertake the following quadratic substitution

$$\begin{cases} (11011)_2 = (100000)_2 - (1)_2 - (100)_2 = 10000\bar{1} - (100)_2 = 100\bar{1}0\bar{1} \\ (11101...1)_2 = 1000\bar{1}0...0\bar{1} \end{cases} \quad (12)$$

The consists of 1, 0, 1 on the right of formula (11) and (12) is called binary redundancy.

Thus it is not hard to see, when the number of "1" after "110" and "1110" ≧ 2, or even "1" ≧ 3, hamming weight of a binary number is higher than the number of redundant binary hamming weight.

Replace the binary sequence of three above even the "1" and "110" and "1110" after more than two types "1" by formula (11) and (12). Such as $e = (101110101111)_2$, If $R(e)$ represents the binary redundancy corresponds to e, then $R(e) = (11000\bar{1}0\bar{1}000\bar{1})_2$. It is easy to verify $e = R(e)$. But the hamming weight of e is 9, and $R(e)$ is only 5, significantly less than e.

Use $R(e)$ instead of e, the x encryption can be expressed as:

$$y \equiv x^{R(x)} (\mathrm{mod}\, M) \quad (13)$$

Among then $R(e) = \sum_{i=0}^{k} e_i 2^i \quad k = n$ or $n = 1, e_i \in \left\{0,1,\bar{1}\right\}$ (14)

Iterative calculation of formula (14), it contains three kinds of basic operation, $A_{ix} (\mathrm{mod}\, M)$, $A_i^2 (\mathrm{mod}\, M)$ and $Aix^{-1} (\mathrm{mod}\, M)$. x^{-1} is the inverse multiply of mold M:

$$xx^{-1} = 1 \mathrm{mod}\, M \quad (15)$$

Known Euler function $\phi(M)$ of modulus $M = pq$ represents the number less than M and relatively prime with M, then $\phi(M) = (p-1)(q-1)$.

The ratio of Euler function and modulus is:

$$\frac{\phi(M)}{M}=\frac{(p-1)(q-1)}{pq}=1-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq} \quad (16)$$

When the value of M is 200 - bit decimal data, the expression of the ratio of formula (16) tends to be 1.

So we say expression (16) shows x that as long as meet $x\in\{0,1,...,M-1\}$ is relatively prime with M, which is satisfied

$$(x,M)=1 \quad (17)$$

x satisfied formula (17), then $x-1$ the inverse multiply of M must exist. Starting from this, we can construct a new fast RSA algorithm, the operation steps are as follows:

(1)First of all, we turn the encrypted index of binary format to binary redundant data, then $R(e)$. Based on the theory, starting from the highest level of encryption index e, if encryption index e has n ($n\geq 3$) "1", the "1" is replaced by $10...0\overline{1}$. If a sequence of "110" or "1110" has two or more even after digital "1", it also can replace in succession, such as (11011). First time $11101\overline{1}$, the second time $100\overline{1}0\overline{1}$ .Such as (111011), of course, can also replace continuously.

(2)Using Euclidean algorithm, we can get the multiplicative inverses x^{-1} of M with x.

(3)Let be

$$x=\begin{cases}X & x\leq\dfrac{M-1}{2}\\ M-x & x>\dfrac{M-1}{2}\end{cases} \quad (18)$$

$$x^{-1}=\begin{cases}x^{-1} & x^{-1}\leq\dfrac{M-1}{2}\\ M-x^{-1} & x^{-1}>\dfrac{M-1}{2}\end{cases} \quad (19)$$

We begin from the first of $R(e)$, computing power surplus y. If A_i is the i step to calculate the intermediate results, it can get a specific algorithm:

$$A_i=\begin{cases}A_i & A_i\leq\dfrac{M-1}{2}\\ M-A_i & A_i>\dfrac{M-1}{2}\end{cases} \quad (20)$$

$$A_{i+1}=A_i^2(\mathrm{mod}\,M) \quad (21)$$

$$A_{i+1}=A_i x(\mathrm{mod}\,M) \quad (22)$$

$$A_{i+1}=A_i x^{-1}(\mathrm{mod}\,M) \quad (23)$$

From which it is easy to infer that the new algorithm iteration number is:

$$l'=n+h[R(e)]-2 \quad (24)$$

$h[R(e)]$ is the hamming weight of $R(e)$.

3.2. The efficiency of search optimization based on random increasing

In the RSA algorithm, the commonly used search methods are random search method and increasing random search method.

(1)Random search method

Randomly generate an odd number p_1 for primality testing. If it's a prime number is over; Otherwise to randomly generate an odd p_2 for primality test, until you find a prime number p_t.

Obviously, for a m binary number, the average per d (length m for the density $1/2d$ of the binary number of primes) random odd number can find a prime number.

(2)Increasing random search method

Randomly generate an odd number for primality testing. If it's a prime number is over, otherwise test the next odd number at the start of this number, until you find a prime number.

Assuming that prime distribution is uniform, produce a m prime numbers, use increasing random search method, the average number of search is

$$d\times 1/d+(d-1)\times 1/d+...+1\times 1/d=(d+1)/2 \quad (25)$$

Far less than the time of random search d.

After in-depth research, we can prove the following theorem.

Increasing random search method is better than that of random search method. Set a m bit prime number, the average search times for using random search method, increasing use of random search method is r, the average number of search is s, then $r=d$, $d/2<s<d$.

A m odd number has n prime numbers, from small to large the order is $p_1,p_2,...,p_n$, the n prime numbers space will be divided into n ranges $(p_1,p_2),(p_2,p_3),...,(p_{n-1},p_n),(p_n,2^m)$, $(p_n,2^m)\cup[2^{m-1},p_1]$. The length of the n ranges are respectively $T_1,T_2,...,T_n$, overall length is T, then $\sum T_i=T$, $T/n=d$.

Obviously, the average search times of random search method is d, $r=d$.

Consider increasing random search method. First of all, the probability that each m bit odd is elected as the starting point of the search is $1/T$. Inspection the number in range T_1, if p_1+1 is chosen as a starting point, the next prime p_2 needs T_1 times search; If p_1+2 is chosen as a starting point, the next prime p_2 needs T_1-1 times search...; If p_2 is chosen as a starting point, the next prime need once search. Other interval is also the same. Therefore, the average search times of increasing random search method is:

$$s=[(T_1+T_2+...+T_n)^2-2\sum_{i=1,i<j}^{n-1}T_iT_j]/2T \quad (26)$$

Because

$$2\sum_{i=1,i<j}^{n-1} T_iT_j \le \sum_{i=1,i<j}^{n-1} (T_i^2+T_j^2) = (n-1)\sum_{i=1}^{n} T_i^2 = (n-1)X \quad (27)$$

So $X/2T > [T^2-(n-1)X]/2T$, $X > T^2/n$

So

$$s > (1/2T)(T^2/n) = T/2n = d/2 \quad (28)$$

Also because $s < d$, then

$$n\left(\sum_{i=1}^{n} T_i^2 + T\right) < 2T^2 = 2\left(\sum_{i=1}^{n} T_i^2 + 2\sum_{i=1,i<j}^{n-1} T_iT_j\right) \quad (29)$$

Which is

$$n(X+T) < 2X + 2\sum_{i=1,i<j}^{n-1} T_iT_j \quad (30)$$

Because

$$2\sum_{i=1,i<j}^{n-1} T_iT_j \le (n-1)X \quad (31)$$

So $n(X+T) < 2(X+(n-1)X)$, which is $X > T$.

Also because

$$X = \sum_{i=1}^{n} T_i^2 > \sum_{i=1}^{n} T_i = T \quad (32)$$

always holds, so

$$\lfloor T_1(T_1+1)+T_2(T_2+1)+\ldots+T_n(T_n+1)\rfloor/2T < T/n \quad (33)$$

always holds, so

$$d/2 < s < d \quad (34)$$

After Lehmann test prime failure, use increasing random search method to plus 2 on the original instead of generating a random number for the next cycle test, in order to improve the speed of prime number detection.

4. Algorithm performance simulation

In order to verify the performance of the improved algorithm proposed in this paper, we use different size on the administrative examination and approval data encryption and decryption speed test, which is shown in the table below:

Table 1. Encrypt / decrypt files processing speed test

Algorithm	AES		RSA		Improved-RSA	
Speed(Mbps)	1	2	1	2	1	2
	31.23	31.23	23.32	21.44	17.79	22.25
	16.94	22.35	21.33	24.23	20.55	21.29
	25.56	27.56	25.34	24.23	13.36	20.31
	26.87	22.87	24.33	24.77	12.56	21.71
Mean	23.23	24.44	24.23	23.66	14.45	16.54

PS:"1" represents encryption, "2" represents decryption in table.

According to the data in table 1, the improved RSA algorithm in this paper in the face of large amount of information, has maintained a relatively ideal processing speed. Judging from this, the encryption algorithm has good performance of encryption, and can quickly handle all kinds of administrative examination and approval data.

Then do encrypt the test on AES, RSA, and improve the performance of RSA algorithm put forward in this paper, the result is shown in the following figure.

Results show that the proposed improved RSA algorithm encryption performance is well, compared to the AES and standard RSA algorithm.

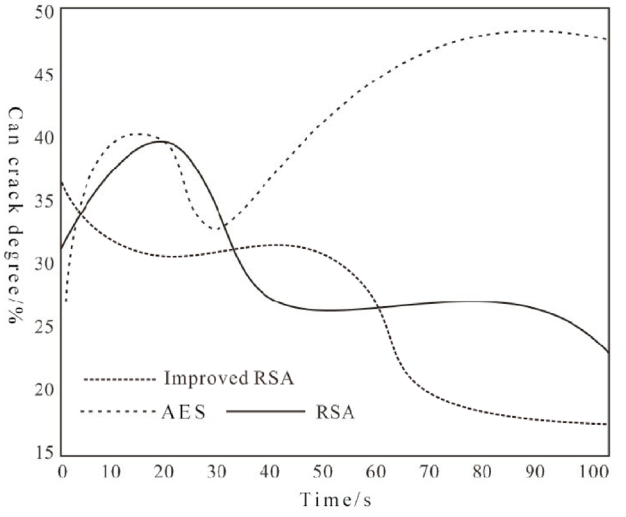

Figure 2. Encryption Performance comparison of three encryption algorithms

5. Conclusions

With the use of a variety of online office system of document transmission, online examination and approval of operation safety has aroused people's more and more attention, the researches and developments of digital signature provides a safe and effective solution for this new office online system. As there are problems in the application of the standard RSA encryption algorithm in administrative examination and approval data encryption, this paper proposes a optimization of RSA algorithm based on real time and efficiency of administrative examination and approval data encryption model. The experimental simulation

results show that the proposed RSA algorithm based on real-time and efficiency optimization is superior to the traditional AES algorithm and the RSA algorithm in terms of efficiency and encryption performance.

References

1. Zang J (2015) Modeling and evaluation of a dual chaotic encryption algorithm for WSN. *Journal of Shandong University*, p.p.1-5.
2. Wei H, Liu W Y (2015) Design of AES encryption of data recorder with Hamming code for error- check- correct. *Application of Electronic Technique*, p.p.118-121.
3. Wanf T C (2014)Fault-tolerant and privacy-preserving data aggregation algorithm in sensor networks. *Application Research of Computers*, p.p.1499-1502.
4. Hu F J (2013) A rapid eye-to-hand coordination method of industrial robots. *Journal of Information and Computational Science*, 10(5), p.p.1489-1496.
5. J Dean, S Ghemawat (2004) *MapReduce: Simplied data processing on large clusters*. Proceeding of the 6th Symposium on Operating System Design and Implementation, New York, p.p.137-150.
6. Randal E. Bryant (2007)Data-Intensive Supercomputing: the case for DISC. *CMU Technical Report CMU-CS-07-128*.
7. S Ghemawat, H Gobioff (2003) *The Google file system. Proceeding of the 19th Symposium on Operating Systems Principles*, New York, p.p.9-43.
8. Zhang Y X (2013)Research on Information Security Mechanism Used in Network Video Surveillance System. *Telecommunications Science*. p.p.69-73.
9. Zuo X H(2013) Study on Security of Logistics Information System. *Logistics Technology*, p.p.34-36.
10. Hu F J, Zhao Y W (2014) Chen Jian. SIFT Feature Points Detection and Extraction of Three-Dimensional Point Cloud. *WIT Transactions on Information and Communication Technologies*, p.p.603-611.
11. Yan Y J, Guo J F (2014) Approach to Selecting Hamming Weight Decision Function in Block Cipher's Differential Power Analysis Attacks. *Microelectronics*, p.p.690-693.
12. Fan Q S (2013) Application of Data Encryption Technology in Computer Security. *Coal Technology*, No. 7, p.p.171-172.

PolSAR Image Classification Based on Deep Convolutional Neural Network

YunyanWang

Hubei Collaborative Innovation Center for High-efficiency Utilization of Solar Energy, Hubei University of Technology, Wuhan 430068, China

Gaihua Wang*

Hubei Collaborative Innovation Center for