Adaptive RSA Encryption Algorithm for Smart Grid

Fang Wang, Zhenyu Wang and Yan Zhu
State Grid Jiangsu Electric Power Limited Company, Suzhou Power Supply Branch
No. 555 Laodong Road, Suzhou Jiangsu 215004, China
Email: grammynow@aliyun.com
Email: gcxy6@hotmail.com
Email: 269166357@qq.com

Abstract. Information security has been paid more and more attention as it is a high-weight factor that affects many aspects in our life. Many technologies have been introduced to improve information security. Encryption algorithm is one of the most frequently used method. There are many encryption algorithms. RSA algorithm, which uses asymmetric encryption method, is a secure encryption algorithms. RSA’s encryption effect is pretty good due to difficulty in cracking its private key. Smart grid is the upgrade of power grid, which is based on integrated, high-speed two-way communication network. In smart grid, there are lots of data to be transferred along the network. In order to ensure that the data are not stolen or tampered with, it is necessary to encrypt the data during transferring. However, it is ineffective to use conventional RSA algorithm directly in smart grid. To solve the problem, we propose an adaptive RSA algorithm to generate primes, which modifies the application scope of RSA algorithm, so that the algorithm can be successfully applied in smart grid. According to the time limit of the encryption algorithm, the prime number is generated adaptively, so that the encryption time of the algorithm is reasonably controlled. The data is encrypted by generating the public key and the private key used for encryption through the generated prime number. The experiments verified the effectiveness of the algorithm.

1. Introduction
Putting forward the viewpoint of public key and private key system is a milestone in the development of cryptography\cite{1}. Compared with the traditional encryption method, the asymmetric encryption method\cite{2} can greatly improve the security index without revealing the private key. The RSA algorithm\cite{3} is an extremely important encryption algorithm in the asymmetric encryption algorithm. Because of the high security index of RSA algorithm and the digital signature of data\cite{4}, it is easy for the receiver to know whether the received data have been modified.

Smart grid is the intellectualization of power grid, also known as Power Grid 2.0. It is built on the basis of integrated, high-speed two-way communication network. Through the application of advanced sensing and measurement technology, advanced equipment technology, advanced control methods and advanced decision support system technology, it realizes the reliability, safety, economy, efficiency and environmental friendliness of power grid\cite{5}. The data of smart grid are transmitted through the network of smart grid. However, these data have the risk of being illegally stolen or changed without protection such as encryption in the process of data transmission. Applying some effective encryption method, e.g. RSA algorithm, to improve security level of smart power system is very necessary.

To deal with security problem during data transferring, in this paper, we introduce the principle and mathematical basis of RSA algorithm, and then propose an adaptive time RSA algorithm, which is able to applied in intelligent power system of smart, so as to solve the high time complexity caused by
the large prime number. Experiments showed that the time complexity of proposed algorithm was reduced without affecting the security of RSA.

2. Related Work

2.1. Encryption Algorithm

The process of data encryption is tantamount to process the original plaintext files or data according to some algorithm. After processing, these files or data will become an unreadable code, referred to as ciphertext, which can only display the original content after entering the corresponding key. Such an algorithm is called encryption algorithm. It uses encryption algorithm to encrypt data or files to protect data and prevent people from being stolen. The inverse process of algorithm encryption is called decryption, which is the process of converting ciphertext into the original data. Encryption technology can be divided into two major categories, symmetric encryption and asymmetric encryption.

Cryptographic algorithm is a mathematical function for encryption and decryption, and cryptographic algorithm is the basis of cryptographic protocol[6]. The security of a cryptosystem depends only on the security of the key, not on the security of the algorithm. Pure data encryption is distinct from software encryption. For pure data encryption, some people do not wish to see the plaintext of these data, using reliable encryption algorithm, as long as the cracker does not know the password of the encrypted data, these data will not be read. And the software needs to run on the program, so the software for the machine, is clear text, for some master decryption, takes some time, the software can be cracked.

An encryption system $S$ can be described by mathematical symbols $S=\{P, C, K, E, D\}$, where $P$ is plaintext space that denotes all possible plaintext sets, $C$ is ciphertext space that represents all possible ciphertext sets, $K$ is key space that is a variable parameter in encryption algorithm, $E$ is encryption algorithm that consists of some equations, rules or programs, and $D$ is the decryption algorithm that is the inverse operation of $E$. When the key $K$ is given, we can have

$$C = EK(P)$$ (1)

where $P$ is plaintext, $C$ is ciphertext and $E$ is encryption algorithm.

After decrypting the ciphertext $C$, the plaintext $P$ is obtained.

$$EK=D^{-1}K$$ (2)

$$DK=E^{-1}K$$ (3)

where $D^{-1}$ is the inverse operation of $D$ and $E^{-1}$ is the inverse operation of $E$.

We can be seen that the encryption design is ultimately to determine $E, D$ and $K$.

2.2. Symmetric and Asymmetric Encryption Algorithm

Symmetric encryption algorithm, also known as private key encryption algorithm, is an encryption algorithm that has the same key for encryption and decryption[7]. Sometimes it is not called traditional cryptographic algorithm as the encryption key can be derived from the decryption key, and the decryption key can also be deduced from the encryption key. In most symmetric encryption algorithms, the encryption key and the decryption key are the same ones; so this encryption algorithm is also called secret key algorithm or single key algorithm. DES algorithm, 3DES algorithm, TDEA algorithm, Blowfish algorithm, RC5 algorithm and IDEA algorithm are all symmetrical encryption algorithms.

Unlike symmetric encryption algorithm, asymmetric encryption algorithm requires two keys. One is a public key and the other is a private key. The public key and the private key are a pair. If the data is encrypted with the public key, only the corresponding private key can be decrypted; if the data is encrypted with the private key, only the corresponding public key can be decrypted. Because encryption and decryption use two different keys, this algorithm is known as asymmetric encryption algorithm.
2.3. RSA
RSA algorithm is the most influential and commonly used public key encryption algorithm\cite{8}. It is a kind of asymmetric encryption algorithm. It can resist most known cryptographic attacks so far. It has been recommended by ISO as a public key data encryption standard.

In smart grid, some data must be transmitted through the network. If these data are not encrypted, they may be acquired illegally. If RSA algorithm is used to encrypt and then transmit, the security of data will be greatly improved. Therefore, the application of RSA algorithm in smart grid is feasible.

2.4. Mutual Prime Relation
If there are two positive integers, these two positive integers have no other common factors except 1. We call these two positive integers reciprocal.

A prime number has no other factors except 1 and itself. Mutual prime relations seem to have some relationship with prime numbers, but there is no absolute relationship. The two prime numbers must be mutually prime relations. However, the two numbers that are mutually prime relations are not necessarily two prime numbers. Then, we can draw some rules about the reciprocal prime relations.

Rule 1: If one number is prime and the other one is not a multiple of the former, then the two numbers are mutually prime relations.

Rule 2: If there are two numbers, the larger one is prime, then the two numbers constitute reciprocal prime relations.

Rule 3: 1 and any natural number form reciprocal prime relations.

Rule 4: \( p \) and \( p-1 \) form reciprocal prime relations when \( p \) is an integer larger than 1.

Rule 5: \( p \) and \( p-1 \) form reciprocal prime relations

Rule 6: If \( p \) is an odd number greater than 1, then \( p \) and \( p-2 \) form a reciprocal relationship.

2.5. Euler Theorem and Function
If two positive integers \( a \) and \( n \) are mutually prime, then the Euler function of \( n \) can make the following equation hold

\[
\alpha(n) \equiv 1(\text{mod } n)
\]

that is, the remainder of \((n)\) of a divides by \( n \) is 1, or that is to say, 1 of a can be divided by \( n \). Euler theorem can greatly simplify some operations, which are more obvious in RSA algorithm.

For any given positive integer \( n \), in a positive integer less than or equal to \( n \), the method of solving the number of reciprocal prime relations with \( n \) is called Euler function\cite{9}.

In the first case, if \( n=1 \), then \( \phi(n)=1 \), because 1 and any number (including itself) constitute a reciprocal relationship.

In the first case, if \( n \) is a prime number, then \( \phi(n)=n-1 \), because prime number and every natural number less than it constitutes a primary reciprocal relationship.

In the third case, if \( n \) is a power of a prime number, that is, \( n=p^k \) where \( p \) is a prime, and \( K \) is an integer greater than or equal to 1, then \( \phi(p^k)=p^{k-1} \). It is because only when a number does not contain a prime number \( p \), it can be a mutual prime with \( n \). There are \( n=p^k \) number of prime number \( p \), and the number \( p^k \) minus this number is the number that is mutually prime with \( n \). The above equations can be reduced to the following equation.

\[
\phi(p^k) = pk-k-1 = pk(1-1/p)
\]

where if \( k \) equals 1, it becomes the second case.

In the fourth case, if \( n \) can be decomposed into the product of two mutually prime integers, i.e. \( n=p_1p_2 \), there will be \( \phi(n)=\phi(p_1)\phi(p_2) \), i.e. the product of Euler functions of products equals the product of Euler functions of each factor.

In the fifth case, because any positive integer greater than 1 can be written as the product of a series of prime numbers, i.e. \( n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r} \). According to the conclusion of the fourth possibility, we can get \( \phi(n) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) \). According to the conclusion of the third case, we can get
Through the above five cases, we obtain the general equation of Euler function.

2.6. Modular Anti-Element

If two positive integers $a$ and $n$ are mutually prime, then an integer $b$ can be found so that $ab-1$ can be divisible by $n$, or the remainder of $ab$ divided by $n$ is 1.

$$ab \equiv 1 \pmod{n}$$  \hspace{1cm} (6)

where $b$ is called the modular inverse element of $a$.

Euler theorem can be used to prove simply that modular anti-elements must exist. We know that the equation of Euler theorem is $a^{\varphi(n)} \equiv 1 \pmod{n}$. Then the equation can be transformed into

$$a^{\varphi(n)-1} \equiv 1 \pmod{n}$$  \hspace{1cm} (7)

where $a^{\varphi(n)-1}$ is the modular and inverse element of $a$, and it can be obtained that the modular and inverse elements must exist.

3. Algorithmic Implementation

3.1. Adaptive Generation of Large Prime Numbers

The generation of two relatively large primes is the basis of RSA algorithm, but the generation of primes is also an important factor affecting the time complexity of RSA algorithm. If the two selected primes are very large, the time complexity of RSA algorithm will be very high. Otherwise, if the two selected primes are very small, the algorithm will be relatively unsafe. To solve the problem, we propose an adaptive time RSA algorithm to solve this problem.

Our algorithm balances the time complexity and security with the goal of reducing the time complexity without affecting the security. We get two better prime numbers and save them. In the first encryption, the time complexity may be higher, because it needs to be obtained many times, but when we get two better prime numbers, the time complexity can be greatly reduced in the future encryption work. The algorithm of selecting prime number is based on the time range that users can bear. Because the initial value we set is relatively high, it needs to be adaptively reduced to the time range that users can bear.

3.2. Generate Asymmetric Key

The first step to generate a key is to select two different large prime numbers, $p$ and $q$. We generate prime adaptively as the approach described above, and then calculate the product $n$ of $p \cdot q$ as well as $\varphi(n)=(p-1)(q-1)$. The procedure is shown as Figure 1.

![Figure 1. The process of public key and private key generation](image.png)

Choose two different large prime numbers $P$ and $Q$

Calculate the product $n = P \cdot Q$ and $\varphi(n)=(p-1)(q-1)$

Choose a random integer $e$ greater than 1 and less than $\varphi(n)$, so that $\gcd(e, \varphi(n))=1$

Calculate $d$ so that $d^e=1 \mod \varphi(n)$

$P, Q$ are destroyed, $\{e, n\}$ is public key, $\{d, n\}$ is private key

Generally speaking, it is easy to get the result by multiplying two relatively large prime numbers, but it is particularly difficult to factorize a particularly large number. Therefore, one part of the key generated by RSA is the product of two relatively large prime numbers. After obtaining $n$ and $\varphi(n)$, a random integer $e$ larger than 1 but smaller than $\varphi(n)$ is selected so that $\gcd(e, n)=1$, and the gcd function is the largest common divisor of two numbers\textsuperscript{[10]}, and the maximum common divisor of two numbers is 1, then the two numbers are mutually prime.
After that, \( d \) is calculated to make \( d \cdot e = 1 \pmod{\phi(n)} \). Finally, \( p \) and \( q \) that are used to generate \( n \) are destroyed, and \( \{e, n\} \) is used as the public key, which is used for encryption, and \( \{d, n\} \) is used as the private key which key is held in the hands of individuals to decrypt the encrypted data. Consequently, the key pair is \( \{e, d, n\} \).

### 3.3. Encryption and Decryption

With the above mathematical foundation, we can easily get the encryption algorithm and the corresponding decryption algorithm. As shown in Figure 2, plaintext is transformed into ciphertext after being processed by public key \( A \), and then transmitted. The other party can decrypt the corresponding cipher text only by using private key \( A \) corresponding to public key \( A \). The decrypted plaintext is identical with the plaintext before encryption, and the whole process of encryption and decryption is completed.

![Encryption and decryption process](image)

**Figure 2.** Encryption and decryption process

### 3.4. Encryption Algorithms

The encryption algorithm\(^{(1)}\) needs the public key \( \{e, n\} \) obtained above. We use the letter \( C \) to represent the ciphertext, the letter \( M \) to represent the information needed to be encrypted, and the encryption equation to encrypt \( C = M^e \pmod{n} \), from which we know that encryption is the \( e \)th power of plaintext \( M \), and then divide it by \( n \). The remainder is the ciphertext as long as we use the encryption equation to encrypt. The process of getting \( E \) and \( n \) from above shows that these two numbers are not obtained casually, but through mathematical concepts and strict mathematical calculation. We propose an adaptive RSA encryption algorithm for generating primes, as algorithm 1.

**Algorithm 1:** Adaptive RSA Encryption Algorithm for Generating Primes

| Input: | Plaintext \( M \) |
|---|---|
| **Output:** | ciphertext \( C \) |
| 1. **While**(true): | |
| 2. Choose two different large prime \( P \) and \( Q \) | |
| 3. Calculate the time difference between \( P \) and \( Q \) | |
| 4. **If** (time difference < limit time) | |
| 5. **Break** | |
| 6. **End While** | |
| 7. Calculate \( n = Q \times P \) | |
| 8. Calculate \( \phi(n) = (p-1)(q-1) \) | |
| 9. Choose a random integer \( e \) | |
| 10. Let \( e \) greater than 1 and less than \( \phi(n) \) and \( \gcd(e, \phi(n)) = 1 \) | |
| 11. Calculate \( d \) so that \( d \cdot e = 1 \pmod{\phi(n)} \) | |
| 12. \( \{e, n\} \) is public key \( \{d, n\} \) is private key | |
| 13. use the equation \( C = M^e \pmod{n} \) to encrypt the plaintext \( M \) | |
| 14. **Return** \( C \) | |
3.5. Decryption Algorithm

The encryption algorithm needs the public key \{e, n\}. The decryption algorithm needs the private key \{d, n\} obtained above. Similarly, C and M are used to represent the ciphertext and plaintext respectively.

The decryption process can use the decryption equation \(M = C^d \mod n\), which can be obtained by dividing the number of ciphertext C by N after the d power, and the remainder is plaintext M. Knowing D and N can decrypt plaintext. The process of encryption and decryption is the same, but one is using public key encryption, the other is using private key decryption \([12]\). Therefore, we need to keep the private key well, otherwise we cannot access and decrypt the information. The adaptive RSA decryption algorithm for generating primes is showed as algorithm 2.

| Algorithm 2: Adaptive RSA Decryption Algorithm for Generating Primes |
|-------------------------------------------------------------|
| **Input**: ciphertext C                                      |
| **Output**: Plaintext M                                     |
| 1. get private key \{d, n\} by Algorithm 1                   |
| 2. use the equation \(M = C^d \mod n\) to decrypt the ciphertext C |
| 3. Return M                                                  |

3.6. Digital Signature

Digital signature is to add a digital signature after the data to be transmitted. The digital signature is to verify whether the received information has been tampered with, so as to ensure the security of the data to be transmitted.

In the process of data transmission, we don't know if our message has been intercepted and tampered with during transmission. Then we add a signature to the plaintext we transmit, encrypt it with public key and put it in the end of the data, transmit it to the other party, and decrypt the signature with the sender's public key. Then decrypt the signature with the private key in hand \([13]\). If the two results are known, then we can know that the public key held by the sender is correct, and the message has not been tampered with in the propagation path.

4. Application in Smart Grid

Smart grid is the intellectualization of power grid \([14]\). It is based on integrated, high-speed two-way communication network. Data transmission through the network is likely to be lost, and the data in the power grid are very important. The data in some household meters can be easily acquired in the process of transmission. Therefore, it is necessary to encrypt these data. In the process of transmission, even if intercepted, the encrypted ciphertext will be obtained. Thus, the intercepted data is useless. Therefore, in smart grid, where data transmission is used, we use RSA algorithm to encrypt the data at one end of the information, and decrypt the encrypted data at the other end. In this case, the security of data transmission is greatly improved.

We simulate the experiment of encrypting the power data, and then decrypt the encrypted data. All the power data used in our simulation experiment are analog data. During the experiment, we can clearly see the results of encrypting the data and using decryption method to get the results of decrypted plaintext. The experimental results are shown in Figures 3, Figure 4 and Figure 5.
Figure 3. For each parameter (because the parameter is too long, only part of it is shown)

Figure 4. Simulates encrypted data

Figure 5. Encrypted ciphertext and decrypted plaintext

As shown in Figure 3, the number of $p$ and $q$ is very large. In the process of generation, the time-consuming complexity is relatively large. Because the generation of $p$ and $q$ is relatively large, the other parameters, including public and private keys, are very large. Therefore, after encryption, the generated ciphertext is very large, and the generated ciphertext and plaintext are far from each other. Even if intercepted, important information cannot be obtained. Finally, we get the plaintext which we simulate by decryption method. As can be seen from Figure 5, the experimental results are very successful.

The parameters of the algorithm are $p$, $q$, $n$, $\phi(n)$, $e$, and $d$, where $d$ is the decisive factor to generate the private key. If $d$ leaks and the private key is cracked, then the data is no longer safe. If $d$ does not leak, then the data is relatively safe. In the case of knowing $n$ and $e$, we need to go through several steps to derive $d$. According to the equation $d*e=1 \mod \phi(n)$, we know that only knowing $e$ and $\phi(n)$
can we calculate $d$. As $e$ is already known, we need to get $\phi(n)=(p-1)(q-1)$. According to the equation of $\phi(n)$, we know that we must get $p$ and $q$ if we want to get $\phi(n)$. The product of $p$ and $q$ is $n$, so it is extremely difficult to deduce $p$ and $q$. In the experiment, we can see that the values of $p$ and $q$ are large and their product is even larger. Since it is very difficult to factorize such a large number, RSA algorithm is reliable without leaking $d$.

5. Conclusion

Nowadays, with the development of social network, data have the risk of being stolen or changed illegally through the Internet. Therefore, in the process of data communication, encryption of some important data is indispensable\textsuperscript{(15)}. It is also very important to encrypt important data in smart grid. RSA algorithm can play a decisive role in solving the problem area. The superiority of RSA algorithm has been proved over time, and it has a very good performance in various fields. The application of RSA in smart grid will gradually become more and more important with time.

To overcome the shortcoming of ineffectiveness of conventional RSA algorithm directly in smart grid, we put forward an adaptive RSA algorithm that create primes adaptively according to the time limit of the encryption algorithm without losing the effect of RSA algorithm.

6. References

[1] He D, Zeadally S, Kumar N, et al. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 2052-2064.
[2] Ma L, Jin W. Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography[J]. Optics Communications, 2018, 407:51-56.
[3] Wu C, Zhou F, Zhu Z, et al. Analysis framework of RSA algorithms in elastic optical rings[J]. Journal of Lightwave Technology, 2019, 37(4): 1113-1122.
[4] Krishna A V N, Narayana A H, Vani K M. Fully homomorphic encryption with matrix based digital signature standard[J]. Journal of Discrete Mathematical Sciences & Cryptography, 2017, 20(2):439-444.
[5] Amin S M, Wollenberg B F. Toward a smart grid: power delivery for the 21st century[J]. IEEE Power and Energy Magazine, 2005, 3(5):34-41.
[6] Jacobson M J, Scheidler R, Stein A. Cryptographic protocols on real hyperelliptic curves[J]. Advances in Mathematics of Communications, 2017, 1(2):197-221.
[7] Chen V M, Hogg P J. Encryption and decryption of tissue factor[J]. Journal of Thrombosis and Haemostasis, 2013, 11(s1):277-284.
[8] Wang J F, Wang S, Liu Y H. Chinese characters knapsack public key encryption algorithm research[J]. Applied Mechanics and Materials, 2012, 198-199:1518-1522.
[9] Bayad A. Modular properties of elliptic Bernoulli and Euler functions[J]. Advanced Studies in Contemporary Mathematics, 2010, 3(3):389-401.
[10] Pasten H, Wang T Y. GCD bounds for analytic functions[J]. International Mathematics Research Notices, 2017, 2017(1): 47-95.
[11] Shepherd S J. The Tiny Encryption Algorithm[J]. Cryptologia, 2007, 31(3):233-245.
[12] Brakerski Z, Segev G. Function-private functional encryption in the private-key setting[J]. Journal of Cryptology, 2015:1-24.
[13] Siregar H, Junaeti E, Hayatmo T. Implementation of digital signature using AES and RSA algorithms as a security in disposition system of letter[J]. IOP Conference Series: Materials Science and Engineering, 2017, 180(1):1-10.
[14] Gong Y, Cai Y, Guo Y, et al. A privacy-preserving scheme for incentive-based demand response in the smart grid[J]. IEEE Transactions on Smart Grid, 2016, 7(3): 1304-1313.
[15] Quang Do-Vinh, Tran-Nhut-Khia Hoan, Koo I. Energy-efficient data encryption scheme for cognitive radio networks[J]. IEEE Sensors Journal, 2018, 18(5):2050-2059.