Data Link Security Transmission Method Based on SM Cryptographic Algorithms

Bobo Pang[1]

[1]North China Electric Power University, School of Control and Computer Engineering, No. 2 Beinong Road, Changping District, Beijing, China
18810787223[at]163.com

Abstract: ***In recent years, major companies have continuously strengthened the construction of data centers, and the security of data link transmission has become an urgent problem to be solved. Considering that SM cryptographic algorithms have begun to show its superiority compared with the international general cryptographic algorithm, this paper combines the advantages of symmetric encryption, asymmetric encryption and digital signature technology in SM cryptographic algorithms, and proposes a data link security transmission method based on the national secret SM2 algorithm, SM3 algorithm and SM4 algorithm. Experiments show that this method has a good effect against passive attacks and active attacks, and can significantly improve the security of data transmission between stations in two-level data.***

Keywords: Information Security, SM Cryptographic Algorithms, secure transmission

1.Introduction

With the development of information and communication technology, data security has become a concern of various industries. Enterprises also frequently encounter challenges in data security. Different from traditional security work, data protection is further blurred in system, business, and organizational boundaries, and the processes of data generation, flow, and processing are more diverse, and face more severe challenges in terms of confidentiality, integrity, and availability. At the same time, the open sharing and frequent flow of data make security prevention more difficult [1].

With the deepening of the construction of enterprise data centers, data transmission tasks between data centers at all levels are becoming more and more frequent. And unprotected network transmission makes malicious attacks very easy, resulting in major breaches of data security. Common attack methods include maliciously tampering with forged device status, operating data, virus attacks, forging and pretending to be identities, and attacking the central database [2]. These will bring serious threats to the normal operation of the data transmission link.

This paper considers the use of domestic cryptographic algorithms to ensure the security and reliability of the data transmission link. Regarding the application of domestic cryptographic algorithms in data security, Ding F et al. proposed a smart grid security communication scheme based on two-way authentication and improved SM2 key exchange protocol [3]. Liu D et al. proposed a security encryption scheme for power IoT terminals based on SM3 algorithm, which improves the security of power grid data transmission [4]. Combining the key exchange technology of the SM2 algorithm and the data encryption and decryption technology of the SM1 algorithm, Li Rui et al. proposed a secure access control method for smart distribution network terminals [5]. Compared with these security schemes, this paper does not use a single algorithm, but integrates the characteristics of multiple national secret algorithms to design a data link security transmission method.

2.Introduction to SM Cryptographic Algorithms

In recent years, with the increasing demand for information security in various industries, the State Cryptography Administration of China has promulgated domestic commercial encryption standards and launched a series of domestic encryption algorithms. The encryption algorithms mainly used in the Internet field include SM2 algorithm [6], SM3 algorithm Algorithm [7], SM4 algorithm [8], corresponding to asymmetric encryption algorithm, cryptographic hash algorithm, symmetric encryption algorithm respectively. Compared with the international popular encryption algorithm, the national encryption algorithm has the advantages of higher security performance, smaller calculation amount, faster processing speed, smaller storage space occupation, lower bandwidth requirements, and easier password management.

2.1 SM2 algorithm

The full name of the SM2 algorithm is the SM2 elliptic curve public key cryptography algorithm, which uses the ECC elliptic curve cryptographic mechanism. However, compared with international standards such as ECDSA and ECDH, it adopts a more secure mechanism in terms of signature and key exchange. The SM2 standard consists of four parts: general rules, digital signature algorithm, public key encryption algorithm, and key exchange protocol. The elliptic curve equation used is $y^2 = x^3 + ax + b$, and the unique coefficients of a and b are determined by specifying a and b. Standard curve [9]. The SM2 standard specifies that the cryptographic hash algorithm used is the SM3 cryptographic hash algorithm. The SM2 algorithm is an asymmetric key algorithm, and it is computationally infeasible to obtain the private key from the known public key. Using public key encryption and private key decryption can complete the public key encryption algorithm; private key encryption and public key decryption can complete the digital signature algorithm.

2.2 SM3 algorithm

The SM3 algorithm is a cryptographic hash algorithm specified by the national secret algorithm. The input is a message m with a length of $l(l < 2^{64})$ bits. After message filling and iterative compression, a hash value is obtained, and the output length of the hash value is 256 bits [10].

Message filling process. Assuming that the length of the message m is l bits, first add the bit "1" to the end of the message, and then add k "0", k is the smallest non-negative integer satisfying $l + 1 + k \equiv 448 (\bmod 512)$. Then add a 64-bit string, which is a binary representation of length 1. The bit length of the padded message m' is a multiple of 512.

Iterative compression process. Group the padded message m' by 512 bits: $m' = B^{(0)}B^{(1)}\ldots B^{(n-1)}$, where $n = (l + k + 65)/512$.

Iterate over m' as follows:

```
**FOR** $i = 0$ **TO** $n - 1$
$V^{(i+1)} = CF(V^{(i)}, B^{(i)})$
**ENDFOR**
```

where CF is the compression function, including the message expansion process and the state update process, which will not be repeated here; $V^{(0)}$ is the 256-bit initial value IV; $B^{(i)}$ is the padded message grouping; iterative compression The result is $V^{(n)}$.

Finally, the 256-bit hash value $y = ABCDEFGH$ is obtained from $ABCDEFGH \leftarrow \oplus V^{(n)}$.

2.3 SM4 algorithm

The SM4 cipher algorithm is a block symmetric key algorithm. The block length of this algorithm is 128 bits, and the key length is 128 bits. Both the encryption algorithm and the key expansion algorithm adopt a nonlinear iterative structure, and the number of operation rounds is 32 rounds. The algorithm structure of data decryption and data encryption is the same, except that the round key is used in the opposite order, and the decryption round key is the reverse order of the encryption round key [11].

The encryption algorithm consists of 32 iterative operations and 1 reverse order transformation R.

32 iterative operations is shown in equation (2.3-1):

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i), \quad i = 0, 1, \cdots, 31 \qquad (2.3\text{-}1)$$

Reverse order transformation is shown in equation (2.3-2):

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}) \qquad (2.3\text{-}2)$$

The decryption transformation of the SM4 algorithm is the same as the encryption transformation structure, the only difference is the use order of the round key. When decrypting, use the round key sequence $(rk_{31}, rk_{30}, \ldots, rk_0)$.

3.Scheme design and implementation

3.1 General idea

In this paper, a data link security transmission method based on domestic encryption algorithm is proposed. In recent years, the national encryption algorithm has developed rapidly. As a commercial encryption standard in China, it has obvious advantages compared with the internationally popular encryption algorithm. For example, SM2 public key encryption algorithm has higher security performance than other asymmetric public key algorithms such as RSA algorithm. The security of 160 bits SM2 algorithm is equivalent to that of 1024 bits RSA algorithm, while the security of 210 bits SM2 algorithm is comparable to that of 2048 bits algorithm. In terms of speed, the key generation, authentication, key negotiation and encryption of the SM2 algorithm have outstanding advantages over the RSA algorithm due to the relatively shorter key string; the SM2 algorithm requires less storage space, and the password Generally, it is 192~256bit, and the password of RSA algorithm generally needs 1024~4096 bits [12]. Compared with the SHA-256 algorithm, the SM3 algorithm is designed with the addition of message double-word insertion and P substitution in its compression function. The compression function is more complex and can resist cryptanalysis attacks such as differential analysis with strong collision and linear analysis with weak collision [13]. For the SM4 grouped symmetric key algorithm, the key length is 128 bits. If the exhaustive attack method is used to attack, it requires 2^{128} operations, which is much larger than the 2^{56} operations required to crack the DES algorithm. is not going to work [14].

Compared with the SM4 algorithm, the SM2 public key encryption algorithm has the advantages of small storage space occupied by the key and high security, but it also has the defects of complex algorithm, slow encryption and decryption of large blocks of data and low efficiency [15]. This paper combines the advantages of SM4 algorithm with high encryption speed, high encryption security, simple key management and low bandwidth requirements, and comprehensively uses SM2 algorithm and SM4 algorithm to encrypt data. The basic principle is: the sender randomly generates a random key of the SM4 algorithm, encrypts the data with the SM4 algorithm, and then encrypts the key with the SM2 algorithm. In this way, after receiving the ciphertext data and the encrypted key data, the receiver also uses the SM2 algorithm to decrypt the random key, and then uses the random key to perform SM4 decryption on the ciphertext. Since the random key for encrypting data is different each time, the problem of SM4 key management is avoided. In addition, the SM3 hash algorithm and the SM2 digital signature algorithm are used to digest and sign the data, so that the data is tamper-proof and non-repudiation.

3.2 Scheme realization

3.2.1 Encryption and decryption

This paper encrypts confidential data based on the SM2 public key encryption algorithm and SM4 block cipher algorithm in the domestic cryptographic algorithm to ensure the security of the data link between the two levels of data. The flow of the sender encrypted data scheme is shown in Figure 3.2.1-1.

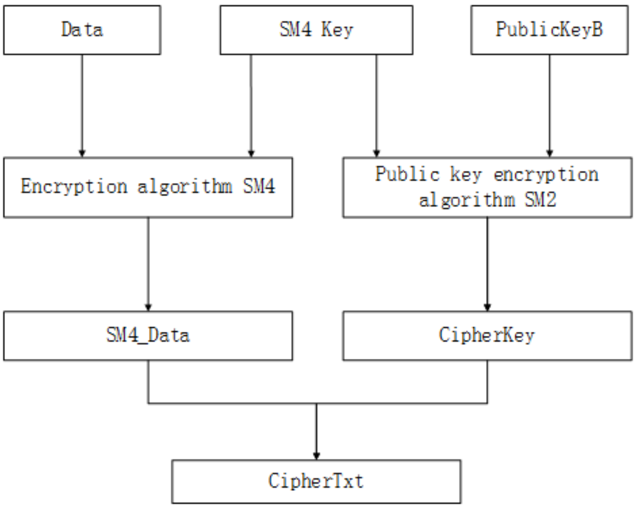


Figure 3.2.1-1: Encryption flowchart

In Figure 3.2.1-1, the Data is the unencrypted data to be transmitted by the sender; the SM4 key is randomly generated by the sender, and only held by the sender at this time; the PublicKeyB is the public key that matches the private key of the SM2 algorithm of the recipient of this data transmission, and can be obtained through the receiver's public key distribution mechanism. When the sender encrypts plaintext data, it first generates the SM4 key, uses Encryption algorithm SM4 and the SM4 key to encrypt the Data, and obtains SM4_Data(the SM4 ciphertext of the Data); then uses the Public key cryptographic algorithm SM2 and the PublicKeyB to encrypt SM4 key, obtain the Cipherkey(SM2 ciphertext of the SM4 key); Finally, the CipherTxt is obtained by linking the obtained two ciphertexts.

After receiving the CipherTxt, the receiver obtains the SM4_Data and the Cipherkey. First, decrypt the Cipherkey of the SM4 key with PrivateKeyB(receiver's SM2 private key) to obtain the SM4 key; then use the SM4 key to decrypt the SM4_Data to obtain the Data. The decryption process of the receiver is shown in Figure 3.2.1-2.

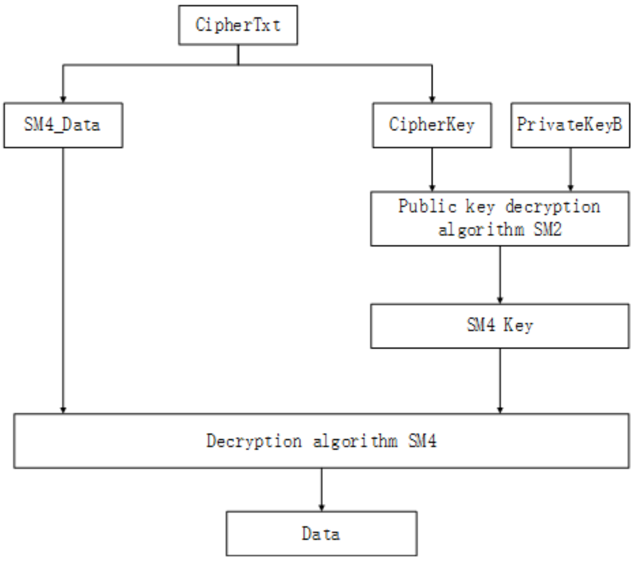


Figure 3.2.1-2: Decryption flowchart

3.2.2 Digital signature and verification

This paper completes the signature authentication scheme based on the SM3 cryptographic hash algorithm and the SM2 digital signature algorithm to ensure the integrity and non-repudiation of the data link. Before transmitting the data, the data sender first uses the SM3 algorithm to obtains the Hash value of the Data, and then uses the Hash value of the Data as input, and uses the PrivateKeyA(sender's SM2 private key) to obtain the Digital signature of the Data through the Digital signature algorithm SM2. The sender's signature process is shown in Figure 3.2.2-1.

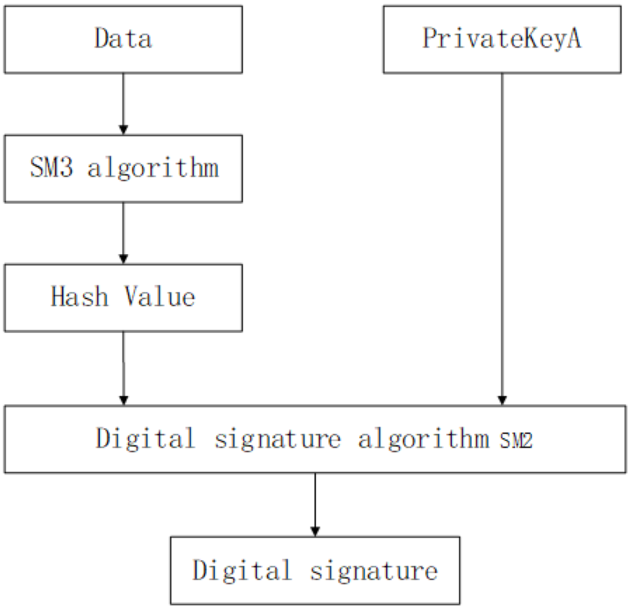


Figure 3.2.2-1: Digital signature flowchart

The receiver receives the encrypted data and Digital signature sent by the sender, and needs to verify the Digital signature to ensure that the data comes from the correct sender and has not been tampered with. The signature can be verified through the following process: first, after the Data is obtained by the decryption algorithm, it is used as the input of the SM3 algorithm, and the Hash Value2 of the Data can be obtained; Match the SM2 public key, decrypt the digital signature, and get Hash Value1. Compare the two hash values, if they are consistent, it means that the signature verification is passed and the received message is correct. The verification signature process is shown in Figure 3.2.2-2.

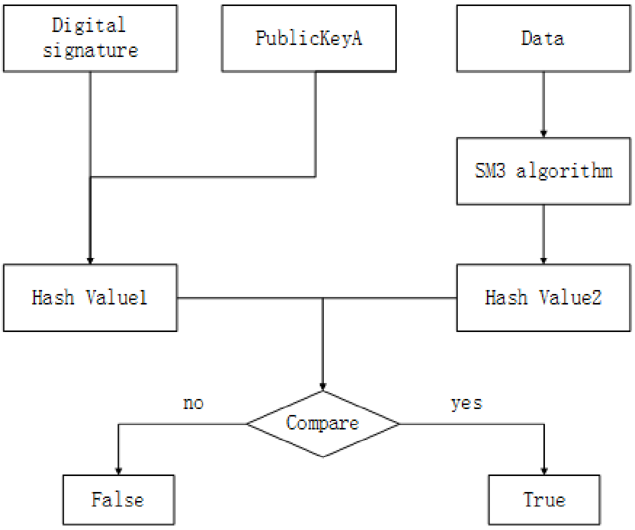


Figure 3.2.1-2: Verification flowchart

3.2.3 Process of sending data

Suppose the SM2 public key of sender A is PublicKeyA, and the SM2 private key is PrivateKeyA. The SM2 public key of receiver B is PublicKeyB, and the SM2 private key is PrivateKeyB. Both parties can obtain the other party's SM2 public key through the other party's public key distribution mechanism. The Key is the session key randomly generated by the sender for SM4 encryption. The process of sending Data from sender A to receiver B is shown in Figure 3.2.3-1.

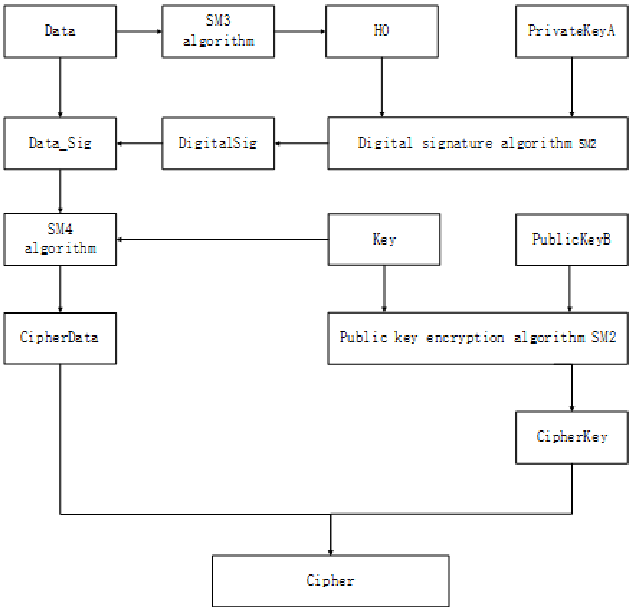
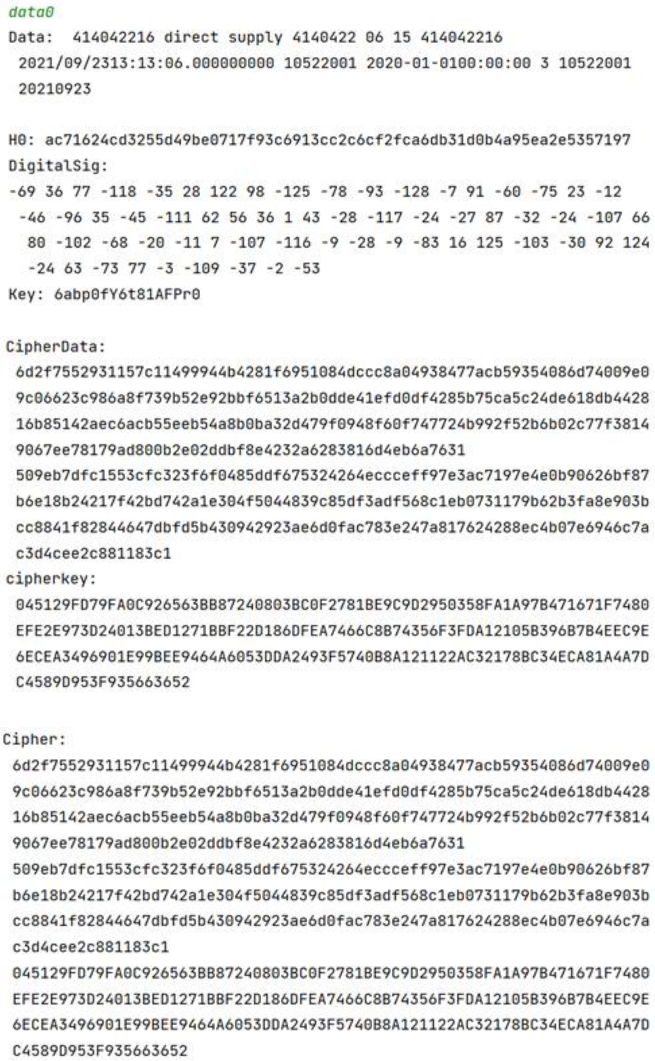


Figure 3.2.3-1: Flowchart of sending data

The process of sending data by sender A is shown in Figure 3.2.3-2. Where the data0 is the file name from which plaintext data is read. The DigitalSig (digital signature) is a byte array type, which needs to be converted to a string type during encryption. Finally get the Cipher to be sent.



```
data0
Data:  414042216 direct supply 4140422 06 15 414042216
 2021/09/2313:13:06.000000000 10522001 2020-01-0100:00:00 3 10522001
 20210923

H0: ac71624cd3255d49be0717f93c6913cc2c6cf2fca6db31d0b4a95ea2e5357197
DigitalSig:
-69 36 77 -118 -35 28 122 98 -125 -78 -93 -128 -7 91 -60 -75 23 -12
 -46 -96 35 -45 -111 62 56 36 1 43 -28 -117 -24 -27 87 -32 -24 -107 66
  80 -102 -68 -20 -11 7 -107 -116 -9 -28 -9 -83 16 125 -103 -30 92 124
  -24 63 -73 77 -3 -109 -37 -2 -53
Key: 6abp0fY6t81AFPr0

CipherData:
 6d2f7552931157c11499944b4281f6951084dccc8a04938477acb59354086d74009e0
 9c06623c986a8f739b52e92bbf6513a2b0dde41efd0df4285b75ca5c24de618db4428
 16b85142aec6acb55eeb54a8b0ba32d479f0948f60f747724b992f52b6b02c77f3814
 9067ee78179ad800b2e02ddbf8e4232a6283816d4eb6a7631
 509eb7dfc1553cfc323f6f0485ddf675324264eccceff97e3ac7197e4e0b90626bf87
 b6e18b24217f42bd742a1e304f5044839c85df3adf568c1eb0731179b62b3fa8e903b
 cc8841f82844647dbfd5b430942923ae6d0fac783e247a817624288ec4b07e6946c7a
 c3d4cee2c881183c1
cipherkey:
 045129FD79FA0C926563BB87240803BC0F2781BE9C9D2950358FA1A97B471671F7480
 EFE2E973D24013BED1271BBF22D186DFEA7466C8B74356F3FDA12105B396B7B4EEC9E
 6ECEA3496901E99BEE9464A6053DDA2493F5740B8A121122AC32178BC34ECA81A4A7D
 C4589D953F935663652


Cipher:
 6d2f7552931157c11499944b4281f6951084dccc8a04938477acb59354086d74009e0
 9c06623c986a8f739b52e92bbf6513a2b0dde41efd0df4285b75ca5c24de618db4428
 16b85142aec6acb55eeb54a8b0ba32d479f0948f60f747724b992f52b6b02c77f3814
 9067ee78179ad800b2e02ddbf8e4232a6283816d4eb6a7631
 509eb7dfc1553cfc323f6f0485ddf675324264eccceff97e3ac7197e4e0b90626bf87
 b6e18b24217f42bd742a1e304f5044839c85df3adf568c1eb0731179b62b3fa8e903b
 cc8841f82844647dbfd5b430942923ae6d0fac783e247a817624288ec4b07e6946c7a
 c3d4cee2c881183c1
 045129FD79FA0C926563BB87240803BC0F2781BE9C9D2950358FA1A97B471671F7480
 EFE2E973D24013BED1271BBF22D186DFEA7466C8B74356F3FDA12105B396B7B4EEC9E
 6ECEA3496901E99BEE9464A6053DDA2493F5740B8A121122AC32178BC34ECA81A4A7D
 C4589D953F935663652
```

Figure 3.2.3-2: Process of sending data

3.2.4 Process of receiving data

Figure 3.2.4-1 shows the system flow after receiver B receives the Cipher.

The processing process after the receiver receives the encrypted data is shown in Figure 3.2.4-2. In terms of implementation, the signature verification result can be directly obtained by the hash value H2 and the DigitalSig experience signature function. If the verification is passed, the plaintext data Data is successfully received.

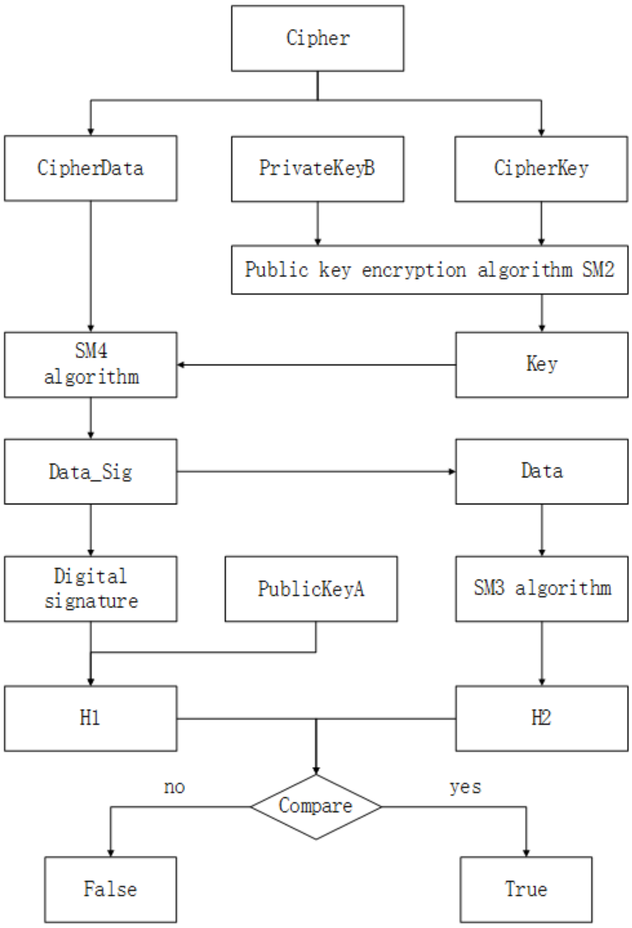
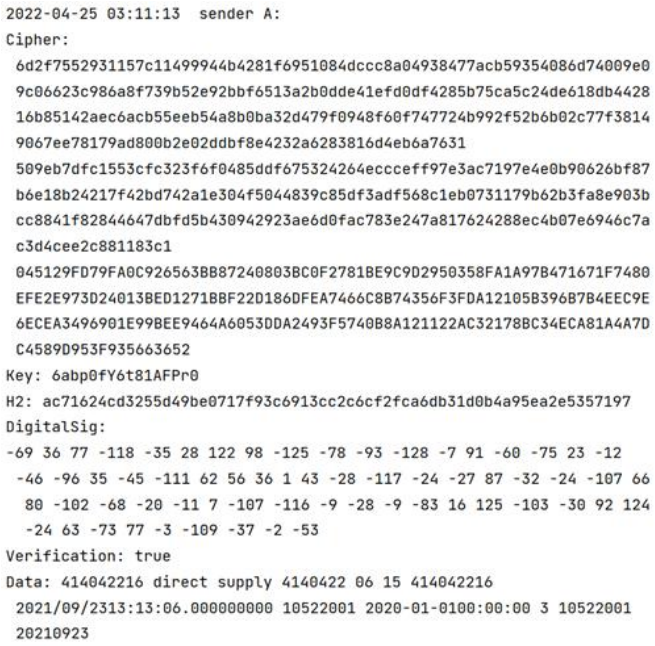


Figure 3.2.4-1: Flowchart of receiving data



```
2022-04-25 03:11:13  sender A:
Cipher:
 6d2f7552931157c11499944b4281f6951084dccc8a04938477acb59354086d74009e0
 9c06623c986a8f739b52e92bbf6513a2b0dde41efd0df4285b75ca5c24de618db4428
 16b85142aec6acb55eeb54a8b0ba32d479f0948f60f747724b992f52b6b02c77f3814
 9067ee78179ad800b2e02ddbf8e4232a6283816d4eb6a7631
 509eb7dfc1553cfc323f6f0485ddf675324264eccceff97e3ac7197e4e0b90626bf87
 b6e18b24217f42bd742a1e304f5044839c85df3adf568c1eb0731179b62b3fa8e903b
 cc8841f82844647dbfd5b430942923ae6d0fac783e247a817624288ec4b07e6946c7a
 c3d4cee2c881183c1
 045129FD79FA0C926563BB87240803BC0F2781BE9C9D2950358FA1A97B471671F7480
 EFE2E973D24013BED1271BBF22D186DFEA7466C8B74356F3FDA12105B396B7B4EEC9E
 6ECEA3496901E99BEE9464A6053DDA2493F5740B8A121122AC32178BC34ECA81A4A7D
 C4589D953F935663652
Key: 6abp0fY6t81AFPr0
H2: ac71624cd3255d49be0717f93c6913cc2c6cf2fca6db31d0b4a95ea2e5357197
DigitalSig:
-69 36 77 -118 -35 28 122 98 -125 -78 -93 -128 -7 91 -60 -75 23 -12
 -46 -96 35 -45 -111 62 56 36 1 43 -28 -117 -24 -27 87 -32 -24 -107 66
  80 -102 -68 -20 -11 7 -107 -116 -9 -28 -9 -83 16 125 -103 -30 92 124
  -24 63 -73 77 -3 -109 -37 -2 -53
Verification: true
Data: 414042216 direct supply 4140422 06 15 414042216
 2021/09/2313:13:06.000000000 10522001 2020-01-0100:00:00 3 10522001
 20210923
```

Figure 3.2.4-2: Process of receiving data

3.3 Security Analysis

This article uses packet capture software Wireshark and scripting language to imitate and attack the data transmission link, but cannot crack the ciphertext. The security analysis is as follows.

1) Two-way authentication is implemented. When the sender transmits data, it not only needs to use its own SM2 private key to digitally sign the hash value obtained by the SM3 algorithm, but also needs to use the receiver's SM2 public key to encrypt the SM4 key; the receiver needs to apply the encrypted data after receiving the encrypted data. The sender's SM2 public key is used to verify the signature, and its own SM2 private key is used to decrypt the SM4 key. If the signature verification fails, it indicates that the data comes from an illegal user; if the illegal user obtains the encrypted data, the ciphertext cannot be cracked to obtain the SM4 key, and the plaintext data cannot be obtained. That is, this process can not only prevent the sender from sending data to illegal users, but also prevent the receiver from receiving messages from illegal users.

2) Data confidentiality is achieved. This paper proposes a hybrid encryption scheme to encrypt data, that is, the national secret SM4 algorithm is used to encrypt the plaintext data, and the SM2 algorithm is used to encrypt the SM4 key. Combining the advantages of fast encryption speed of SM4 algorithm and high encryption security of SM2 algorithm, simple key management and low bandwidth requirements, it protects data from passive attacks, so that the confidentiality of data is greatly guaranteed, and SM4 is also avoided. Problems with key management.

3) Data integrity is guaranteed. Every time you receive data, you need to compare the hash value obtained by the signature verification with the hash value of the plaintext data, so as to complete the data integrity check, fight against active attacks (counterfeiting, replay, data tampering, business rejection), and ensure The received data is exactly the same as the sent data without being copied, inserted, tampered with, rearranged or replayed. The hash algorithm used in this paper is the national secret SM3 algorithm. Compared with other algorithms at home and abroad, the SM3 cryptographic hash algorithm has high security, small software and hardware implementation area, and high algorithm implementation efficiency [10].

4) Data non-repudiation is guaranteed. Data link security requires not only the protection of data communication parties against attacks by third parties, but also protection of one of the communication parties against deception or forgery by the other party. The scheme in this paper uses digital signature technology to ensure the non-repudiation of data. The receiver uses the sender's SM2 public key to verify the digital signature to confirm that the data comes from the correct sender. Since the SM2 private key is only held by the sender, the other party cannot deny it.

4.Conclusion

This paper comprehensively analyzes the security requirements of data link transmission between enterprise data centers. Based on the superiority of domestic encryption algorithms, the functions and characteristics of SM2 public key encryption algorithm and digital signature algorithm, SM3 cryptographic hash algorithm, and SM4 block cipher algorithm are comprehensively analyzed. A hybrid encryption and identity authentication scheme is designed for secure transmission of enterprise data links. Through simulation experiments, the feasibility, correctness and high security of the method are verified. Security analysis shows that this scheme can comprehensively improve the security performance of the data transmission link, so that the confidentiality, integrity and non-repudiation of data can be effectively guaranteed.

References

[1] "Difficulties in Security Guarantee of State Grid Big Data Center" [J]. Popular Utilization of Electricity, 2020:35(09):51.
[2] Dai Xichang. "The Security Research Of Smart Distribution Grid's Data Transmission" [D]. East China Jiaotong University, 2015.
[3] Ding F, Long Y, Wu P. Study on secret sharing for sm2 digital signature and its application [C]//2018 14th International Conference on Computational Intelligence and Security (CIS). IEEE, 2018: 205-209.
[4] Liu D, Wang R, Zhang H, et al. Research on Terminal Security Technology of Ubiquitous Power Internet of Things Based on PUF and SM3 [C]//2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2019: 910-915.
[5] Li Rui. "Research and implementation of secure access technology for intelligent distribution network terminals" [D]. North China Electric Power University, 2019.DOI:10.27140/d.cnki.ghbbu.2019.001066.
[6] Public key cryptography algorithm SM2 based on elliptic curves: GM/T 0003-2012 [S]. Beijing: Chinese Encryption Administration, 2012-03-21.
[7] GM/T 0004-2012, SM3 Cryptographic Hash Algorithm [S].
[8] GM/T 0002-2012, SM4 Block Cipher Algorithm [S].
[9] Xi Yuhang, Huang Yiping, Su Jiande, Wang Shupei. "Design And Implementation Of Instant Messaging Encryption Software System Based On National Secret Algorithm" [J]. Computer Applications and Software, 2020, 37(06): 303-308+327.
[10] Wang Xiaoyun, Yu Hongbo. "SM3 Cryptographic Hash Algorithm" [J]. Journal of Information Security Research, 2016, 2(11):983-994.
[11] Lu Shuwang, Su Bozhan, Wang Peng, et al. "Overview on SM4 Algorithm" [J]. Journal of Information Security Research, 2016, 2(11):995-1007.
[12] Luo Zhao, Xie Jihua, Gu Wei, et al. "SM2-Cryptosystem Based Information Security Supporting Platform in Power Grid" [C]. Automation of Electric Power Systems. 2014, 38(06):68-74.
[13] Shen Yanzhao. Analysis of SM3 Cryptographic Hash Algorithm [D]. Shanghai: Donghua University, 2013.
[14] Wu Xiao, Guo Peiyuan, He Duoduo. "Implementation of reconfigurable of DES and SM4 encryption algorithm" [J]. Application Research of Computers, 2014, 31(03):853-856.
[15] Wu Juan. "Research and Implementation of Hybrid Cipher Algorithm Based on SM4 and SM2" [J]. Software Guide, 2013, 12(08):127-130.

Author Profile

Bobo Pang, Born in June 1997 in Dangshan, Anhui Province, he is a master's student in the school of control and computer engineering of North China Electric Power University. The main research direction is information security.