Information Encryption and Data Storage Security

Hang Wu*

School of software, Tianjin Polytechnic University, Tianjin, China

*Corresponding author: 2111320315@tiangong.edu.cn

Abstract. Nowadays, people increasingly rely on communication software to communicate. Users can use communication software for daily life information communication and involve work, transactions, or some private content. Moreover, time or money can be lost if that information is leaked. Therefore, ensuring communication security becomes a critical issue. Communication security generally involves two aspects: information transmission and data storage. Attackers do more than attack the transmitted information. It can also steal data that is already stored. This paper first introduces the encryption algorithm of information transmission. And then, this paper introduces secure data storage methods for information encryption.Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms are mature encryption algorithms currently used. Using RSA to encrypt the AES key in information transmission can make the information more secure and reliable. In addition, adding RSA algorithm-supported digital signature verification technology can ensure the authenticity and integrity of messages. Data storage is just as necessary as information encryption. Data needs to be stored in a database. Besides, this paper introduces how the security mechanism of the MySQL database controls user access to the database.

Keywords: Encryption, AES, RSA, MD5, Digital Signature, MySQL.

1. Introduction

Communication has been around since the dawn of man. At that time, people mainly relied on body language to communicate with each other. Information can be received and conveyed between people through the eyes, ears, and mouth. Realize the communication between people. This form of communication has been inherited from primitive societies, later, with the progress of human society. People can communicate over long distances with the help of material media, such as letters. The message that people are going to convey is written on things. The delivery of goods by the person to the person to whom the information is to be received. This kind of communication costs people. Moreover, it takes a long time.

Moreover, information is time-sensitive. Such communication may need clarification. Modern long-distance communication technology has been produced due to the ongoing advancement of research and technology. The telegraph and telephone made communication fast. People no longer need to send things to get the word out. This saves the workforce and time. Now people can use mobile phones or computers to communicate quickly.

Since ancient times, the problem of communication security has always existed. However, the way to solve this problem is changing with the progress of technology.

The earliest encryption of communications used private networks. That is physically isolating other people. However, the objective conditions are different following the emergence of the Internet and the decrease in private networks. The strategy for privacy goes from "do not let you see it" to "if you see it, you do not understand it." This is done by first encrypting the message into a ciphertext and then decrypting it into a message when it arrives at the receiver.

Now communication software commonly used encryption technologies are AES (Advanced Encryption Standard) and RSA (). While the technologies referred to above have been proven effective, Santhosh Kumar B J believes that the encryption strength is still lacking, so Santhosh Kumar B J adopted a more reliable dual encryption technology [1]. RSA is an asymmetric encryption algorithm that encrypts the information using a public key and then sends the information, one must possess the private key, and both are irreversible. The public and private keys are generated simultaneously and correspond to each other. For example, A has the public key, while B has the

public and private keys. A encrypts the data with the public key and sends the ciphertext to B, which can decrypt it using the private and public keys [2]. AES belongs to symmetric encryption, where A uses a password to encrypt the data with AES, and B uses the same password to decrypt the ciphertext [3].

When using a single encryption algorithm, such as only using AES, a significant issue is that, as a symmetric algorithm, it requires the encryption and decryption parties to use the same key. This creates a critical key management problem - how to distribute essential keys to authorized recipients distributed worldwide without risking significant key leakage due to oversight during transmission? The answer is to combine AES and RSA encryption algorithms. The AES key is transmitted using RSA, and after the client and server obtain the AES key, they can transmit the actual content. This approach utilizes the flexibility of RSA, which can modify the AES key at any time, and utilizes the efficiency of AES, which can efficiently transmit data.

After encrypting the information, the RSA-supported digital signature is used to render certain the security of the message transmission process through MD5 (Message-Digest Algorithm 5). Most digital signatures are based on the RSA algorithm. The advantage of this is that it is relatively easy to implement, convenient to use, has muscular encryption strength, and is difficult to crack [4].

Encryption of information can also be applied to data storage. Encrypt the data and then store it to protect the data security. However, this is expensive. Therefore, users can set database access permissions to protect data security. This not only costs less but also protects the security of the data. The following describes the MySQL database permissions.

The main function of the MySQL (Structured query language) permissions system is to verify that a user connected to a MySQL server host is legitimate and to give the user permission to select, insert, update, and delete records on a database table. When connecting to a MySQL server, the host decides the user's identity to which the user is connected and the specified user name. MySQL access control consists of two steps: First, the server checks to see if a connection is allowed, and if a connection is allowed, the server checks each request from the user to see if it has enough permissions to implement it.

In Section 2, two kinds of information encryption algorithms and digital signatures are introduced in detail, and their advantages are analyzed. Section 3 introduces the security mechanism of the database. Both of these components are extremely important in the overall security of communications.

2. The Encryption Algorithm Used for Communication

RSA encryption, AES encryption, and digital signature are the most popular methods. This paper mainly studies these three encryption methods: RSA, AES, and MD5. The AES encryption encrypts the chats and files to ensure security during transmission. Moreover, RSA encryption is a digital signature and encrypt method in the key exchange. The MD5 encrypt method to use as a digital signature in the chat transmission.

2.1. Digital signature

Digital signatures, simply a string of ones and zeros generated by a digital signature algorithm, are used to verify and authenticate electronic documents [5]. Signing a document or a message through a digital signature usually needs three steps. The first step is to generate and verify the key and a secret key. The second step is to input the secret key and the original message M and generate the output \sigma. The third step is to verify, taking input M, secret key, and \sigma. If it can verify (M, sign (M, SK), VK) =1, it means the message or the document can be trusted.

2.2. RSA, AES and MD5

RSA. The public key issued by an RSA user is generated from two valid prime numbers and an extra value. The primes will be kept secret during this process. Moreover, verify the message with

the public key. However, if the signed message is direct, the attacker might compute the third message without the private key just by multiplying them. So, before signing the message, the message needs to be encrypted through the hash function. Then nobody can tamper with the message.

AES is a symmetric-key algorithm, meaning the same key is used for encrypting and decrypting the data. About three key lengths are supported in AES encryption 128,192,256-bit lengths [6]. Figure 3 shows the AES encryption flowchart.

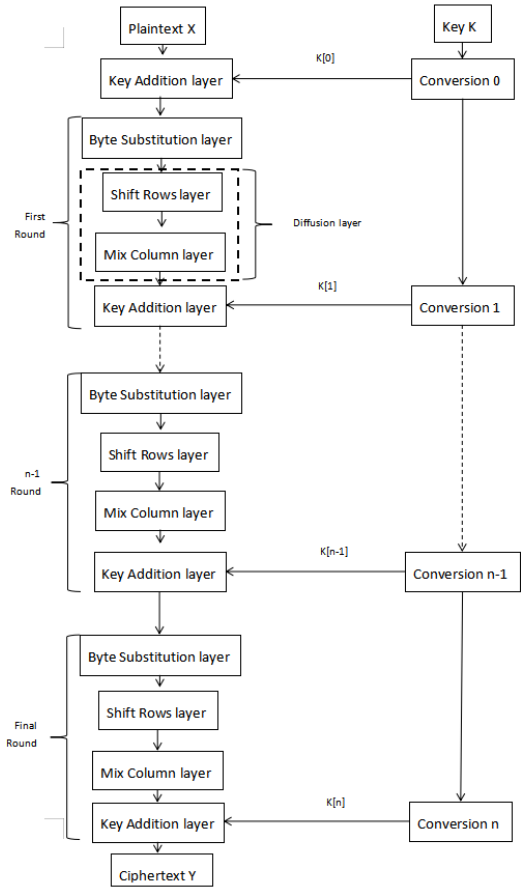

Fig. 1 AES encryption flowchart

MD5. With this algorithm, a variable-length message is like 128-fixed-length output. The input message is divided into 512-bit blocks; the message is filled in so that its length will be divided by 512 [7]. The sender encrypts the information by the public key and sends it to the receiver. The recipient needs to decrypt the message with a specific private key to get the message's content.

2.3. Advantage analysis

Compared to asymmetric encryption, the most significant benefit of AES encryption is its high computational efficiency. In the asymmetric-key algorithm, the computer must do many complexes computes. For example, in the RSA algorithm, many large numbers need to multiply or mod, but the computer needs to compute bit operation in the symmetric-key algorithm. It is much more efficient for a computer to compute it than in an asymmetric-key algorithm. So, it will boost the effect of the chatting app. Another benefit of AES is that it can use for chat and document encryption, and it has relative safety at the same time. Up to now, only 64-bit AES can be attacked.

RSA is an asymmetric-key algorithm. Since the public and private keys are different, and the private key cannot be deduced from the public key, the responsible department may send the user the encryption key table, like a telephone book. Another benefit of RSA encryption is that it can use as a digital signature to ensure the sent content does not tamper with the attacker. This function will be helpful when used in AES private key exchanges.

MD5 can be used to verify that information has not been tampered with. Attackers may steal user information, or they may alter the content of information to mislead us. MD5 also prevents people from seeing the plaintext directly.

3. Security Mechanism of the Database

The emergence of the Internet has changed people's lives. People nowadays have access to a great deal of information through the Internet. Using the Internet to communicate also generates many data. This data needs to be stored. Moreover, users need to keep that data and information safe. In consequence, the server must be high availability and highly scalability. Such a server can be used with MySQL Cluster technology [8].

3.1. Connect confirm

A MySQL server determines whether to accept or reject a connection request from a user based on the User's identity. The Host, user name, and a user password can verify the User's identity.

Authentication uses the range fields of the user table. Only the hostname and user name match those in the User, and the password is accurate will the server accept the connection. The hostname or IP can be either a Host value. In Host, fields can use '%' or baseline value. In User, fields can not use '%' or baseline value.

An anonymous user's record in the User database matches a connection but has no user name. If the server permits anonymous login, the blank user name will move on to the following authentication stage.

A connection request can match multiple records in the user table. If there are many matches, after reading the user table at launch, the server sorts the issue to address it. When a user tries to connect, the records in the user table are browsed in sorted order, and the first matching record is used.

3.2. Request confirm

After authentication, a connection is established with the server. For each request on this connection, the server checks that the user has permission to execute it. These permissions can be any of from the table. Complex queries can make understanding MySQL rules for deciding how to fetch data challenging [9].

For administrative requests, the server retrieves the user's access record. When the request is allowed, consent to access. However, when the request is disgruntled, access is denied.

When the database receives a request, the server will start working. It will review the record to determine the requesting authority. Access is available only when the request is granted. Suppose the permissions in the user table need to be increased. The server will check the db first. The user might also check the host later. The two are combined to determine permissions. The specific process is as follows: 1) The server will search the db for matching records. The host is also checked to confirm permissions. The records can be accessed if a match is checked. 2) If records can be matched in db. Moreover, it is also in the host. Then the user's permissions are determined based on the record. 3) If the Host field of the matched db table record is empty. So the user will drill down to see if there is a record in the host, and if there is one, look at some of the permissions that match. No record, no access.

In addition. If the user finds that the permissions in one table are insufficient, the user can combine the tables. For example, if two permissions are applied at the same time, the records of one table can be shared with the other table. So the user can combine them. The host can also specify that a host cannot use the database, which can be recorded in the host.

By manipulating table records in the MySQL database, users can be given specific permissions to control the user connection and access to the database. The user table is particularly important among the permission tables because it holds the user's password, and its permissions are global.

4. Discussion

Network security is becoming increasingly important owing to the expanding role of distributed computation, databases, and telecommunications applications such as electronic mail [10]. In network security, information encryption, and information storage are particularly important. However, there are some questions about these two parts.

As far as AES is concerned, it has many advantages, and there is no ability to break the full version of AES. However, science and technology are constantly evolving. The computing power of computers is also increasing rapidly. In the future, the encryption algorithms used today may be broken. So the encryption algorithm cannot be used permanently. It is constantly updated with the progress of science and technology.

More than one encryption algorithm was mentioned in the introduction of this paper. Using more than one encryption algorithm to encrypt information may need to be more secure. A single encryption algorithm can not achieve encryption and verification simultaneously. So when encrypting information, several encryption algorithms are usually used to ensure information security. This way, the advantages of different encryption algorithms can be fully used to improve information security. Symmetric encryption and asymmetric encryption have their advantages. At the same time, information security is very high using these two encryption algorithms and digital signature verification.

There needs to be more than encryption to secure communications. Various software or hardware problems, such as virus invasion or hardware damage, are encountered daily. These security vulnerabilities cannot be remedied by encryption or permission Settings. Therefore, communication security must also strengthen response measures in all aspects to ensure information security.

5. Conclusion

People are communicating more and more via the Internet. Network communication brings people convenience and saves time. However, many security risks in the network will threaten communication security. Encryption and permissions were born. This will improve communication security. This paper focuses on two essential parts of communication: information encryption and secure storage. In the process of information transmission and storage will be frequently attacked. Attackers will tamper with and steal information. The damage can be massive if some confidential documents are lost, or trade information is tampered with by competitors. To avoid these losses, people encrypt information. Set access permissions for stored information. Internet communication has become an indispensable part of daily life. Since there are many security risks, people should pay attention to them and actively solve these problems from the root.

The network has no security, and critical information may be leaked anytime. This paper introduce some prevalent encryption algorithms and some permission Settings. However, these technologies should be improved, and the encryption algorithm should be upgraded continuously. With that, better and more secure methods to protect information security will be developed in the future.

References

[1] BJ, S. K., Nair, A., & VK, R. R. (2017, April). Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images. In 2017 international conference on communication and signal processing (ICCSP) (pp. 1057-1060). IEEE.

[2] Karakra, A., & Alsadeh, A. (2016, July). A-RSA: Augmented RSA. In 2016 SAI Computing Conference (SAI) (pp. 1016-1023). IEEE.

[3] Nadjia, A., & Mohamed, A. (2015, March). Aes ip for hybrid cryptosystem rsa-aes. In 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15) (pp. 1-6). IEEE.

[4] Yang, T., Zhang, Y., Xiao, S., & Zhao, Y. (2021). Digital signature based on ISRSAC. China Communications, 18(1), 161-168.

[5] N. Bodapati, N. Pooja, E. A. Varshini and R. N. S. Jyothi, "Observations on the Theory of Digital Signatures and Cryptographic Hash Functions," 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2022, pp. 1-5, doi: 10.1109/ICSSIT53264.2022.9716495.

[6] A. Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 333-338, doi: 10.1109/SMART50582.2020.9336800.

[7] M. B. Kılıç, "Encryption Methods and Comparison of Popular Chat Applications", Advances in Artificial Intelligence Research, vol. 1, no. 2, pp. 52-59, Sep. 2021

[8] Prabowo A , Satoto K I , Somantri M . Perancangan MySQL Cluster Untuk Mengatasi Kegagalan Sistem Basis Data Pada Sisi Server[J]. tk electrical engineering electronics nuclear engineering, 2011.

[9] MD Giacomo. MySQL: lessons learned on a digital library[J]. IEEE Software, 2005, 22(3):10-13.

[10] SharmaRavi. Data communication and security[J]. ACM Sigsac Review, 1986.