Hybrid AES256-RSA1024/2048 Encryption Methodology on Procedures of ZKTeco products

Hybrid AES256-RSA1024/2048
Encryption Methodology on Procedures of ZKTeco products

This paper explores the Fundamentals RSA1024/2048 / AES256 Encryption and Procedures of encryption methods. In this paper, we review the dominant RSA1024/2048 and AES256 standard.

Table of Contents

Abstract

Network security has become an increasingly crucial topic, as it can be read and maliciously used by everyone who has access to the network. For example, a protocol analyzer can read packets and gain classified information, a hostile party can tamper with packets and cause damage by hindering, reducing, or preventing network communications within your organization.

To ZKTeco security system, Data Encryption is always one of the key elements for safety. We focus on cryptography to secure data transmitted in network. Thus, we are striving to enhance protection against espionages and data thefts.

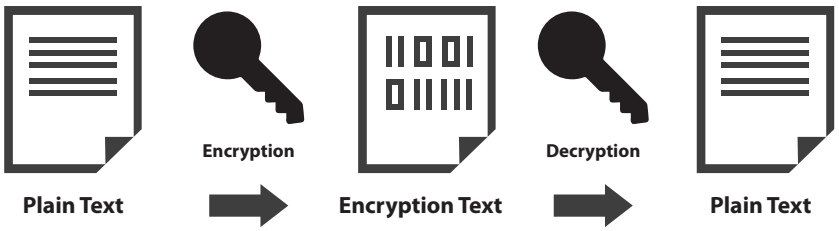
While taking into consideration the advantages of using web services, we must also focus on two crucial aspects, the security of data being exchanged and minimizing the size of data transfer. Therefore, it is crucial to ensure data secrecy, authenticity, and integrity of the data being transferred between the client and the host application.

Fundamentals of Encryption and Decryption

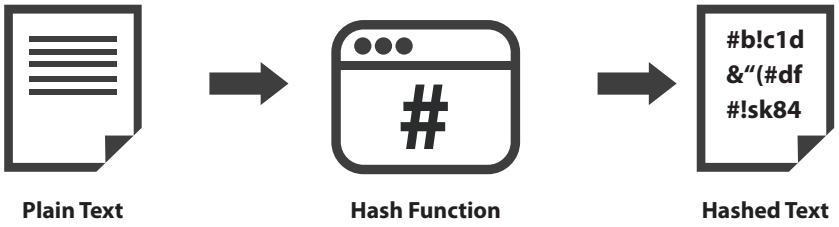
Encryption is a security control primarily for confidentiality protection for data, it is a mathematical transformation used to scramble data requiring protection (plaintext) into a form that unauthorized people or machines are not able to easily read (ciphertext). The ciphertext is displayed in a random format and does not reveal anything about the content of the original data. Once encrypted, no person (or machine) can discern anything about the content of the original data by reading the encrypted form of the data.

Encryption is a reversible transformation. It is useful and readable only when encrypted data (ciphertext) can be reversed back to its original unencrypted form (plaintext). This reveRSA1024/2048l process is referred to as decryption. An encryption process has one corresponding decryption process, which is used to reverse the encrypted data (ciphertext) back to its original content (plaintext).

Encryption and Decryption

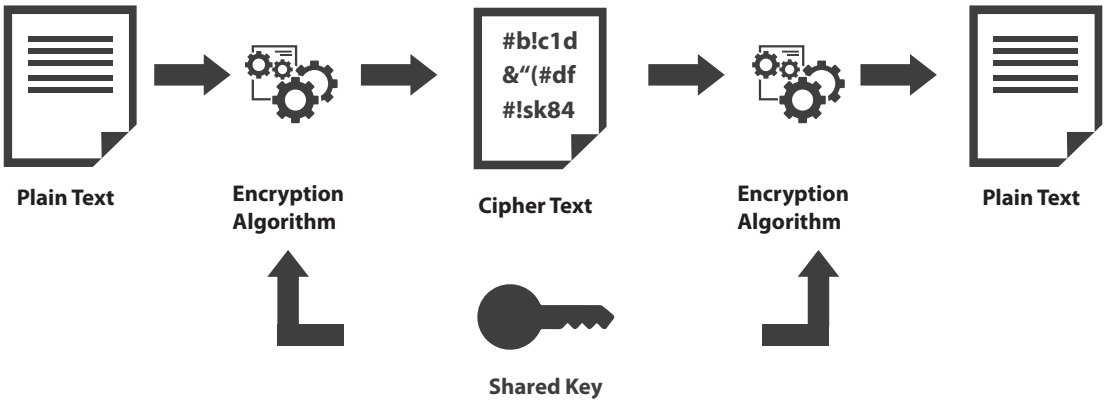


Hashing Algorithm



Symmetric Encryption

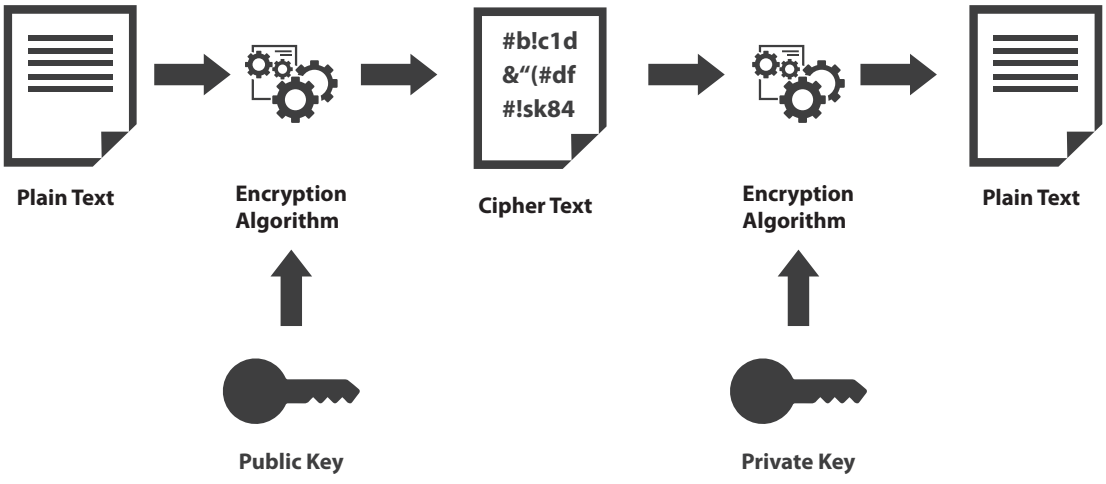
Symmetric encryption requires a shared secret to encrypt and decrypt. Each device encrypts the data before sending information across the network, and this same key is used to both encrypt and decrypt the data. Examples of symmetric key encryption are Data Encryption Standard (DES), triple DES (3DES), and Advanced Encryption Standard (AES256).



Asymmetric Encryption

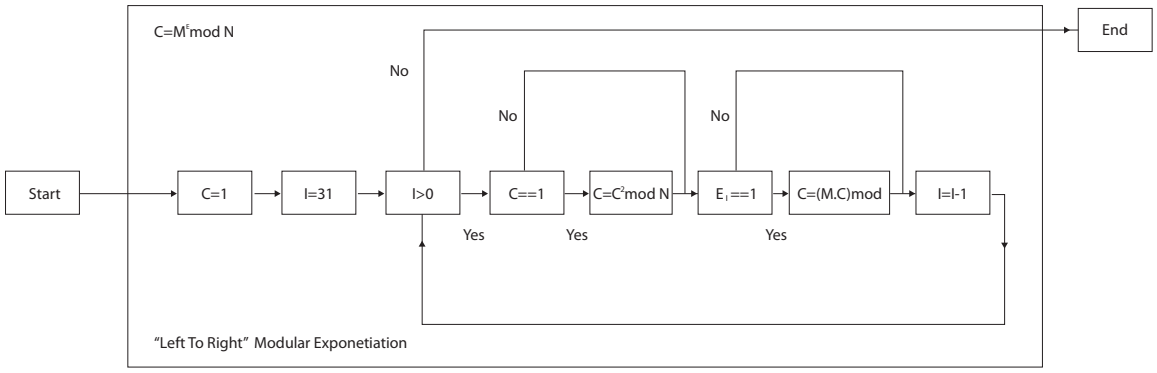
Devices that use asymmetric encryption use different keys for encryption than they do for decryption. These keys are called private and public key.

Private keys encrypt a hash from the message to create a digital signature that is then verified (via decryption) using the public key; Public keys encrypt a symmetric key for secure distribution to the receiving host, who then decrypts that symmetric key using their exclusively held private key. It is not possible to encrypt and decrypt using the same key. This is a variant of public key encryption that uses a combination of both a public and private key. An example of an asymmetric encryption is Rivest, Shamir and Adleman (RSA).



RSA (Rivest-Shamir-Adlenan)

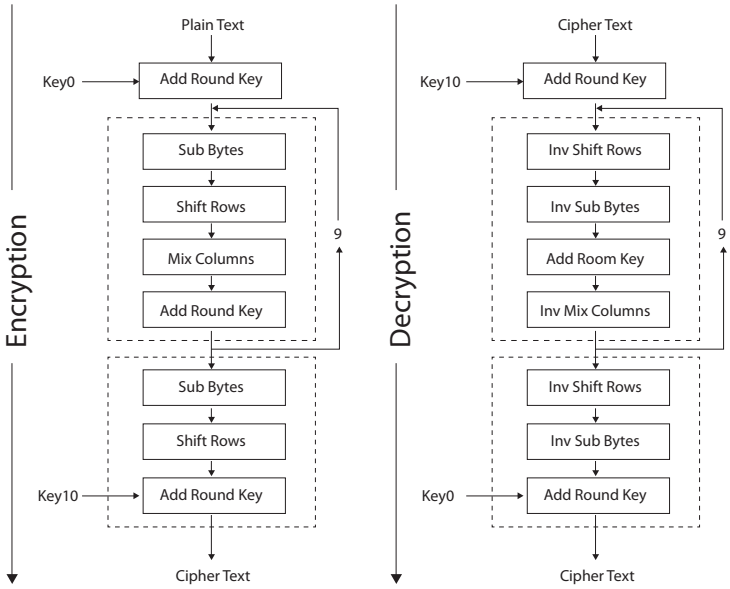
RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely applied for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). The reliability of RSA is based on the difficulty of prime factorization towards large integers. The more difficult the factorization is, the great security RSA offers. Until now there is no feasible formula which is able to attack RSA. As long as the key has enough length, it is hard to decrypt information encrypted with RSA.



AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. The algorithm is described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. AES became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard.



Implementation

From the above comparison, we know that RSA requires greater consumption of hardware processing power and time with its higher security of encryption and decryption, which is not suitable for large-scale data encryption and decryption, thus completely applying RSA public-key cryptosystem for data transfer does not meet the actual application needs. AES, although consumes comparatively low hardware processing power and is relatively quicker, is attached with concerns regarding the security management of AES keys in network communication, which is the key point to guarantee the security of AES encryption. ZKTeco integrates both systems' advantages and realizes its pioneering hybrid data encryption solution, it applies AES symmetric key encryption to encrypt transmitted raw data, and simultaneously applies RSA asymmetric key cryptosystem to encrypt and transfer AES keys to maximize the security of encryption process.

ZKTeco Encryption Procedures

I) First, AES256 and RSA1024/2048 keys are randomly generated by ZKTeco Private Key Algorithm

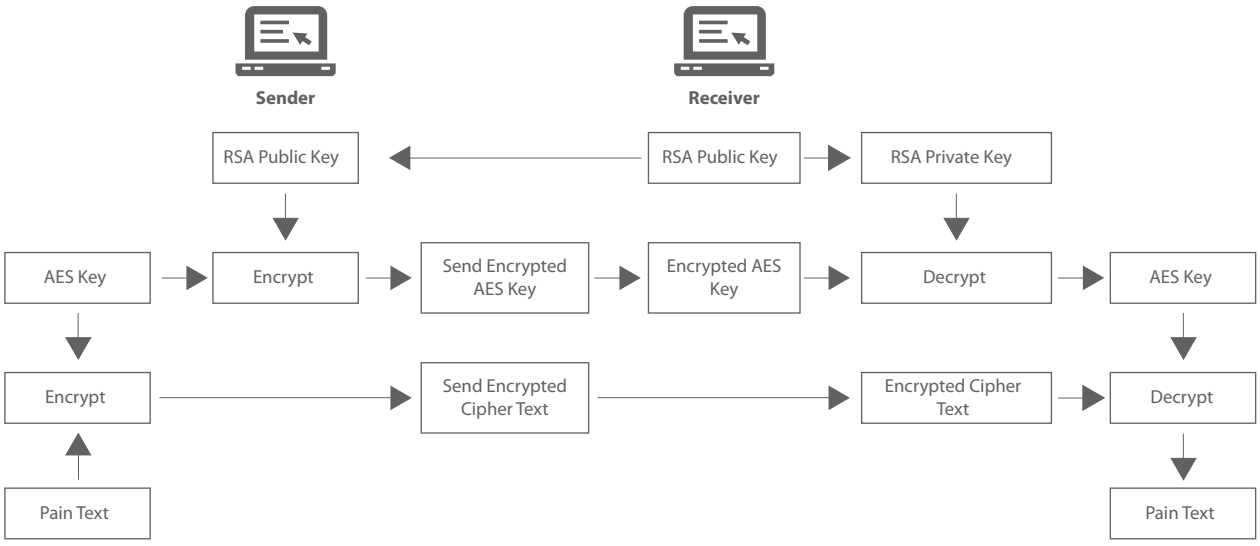
II) AES256 private key encrypts raw data

III) Transmitting terminal encrypts AES256 keys with RSA1024/2048 public key, and contains them in the content delivered to the transmitting terminal

IV) In RSA1024/2048 mechanism, only receiving terminals which own private keys are able to decrypt and obtain AES256 private keys, and are thus able to decrypt received data utilizing AES256 keys

V) Receiving terminal processes related raw data

VI) All AES256 and RSA1024/2048 private keys are generated by ZKTeco own key algorithm, thus enabling maximized optimization of the entire encryption and decryption procedures

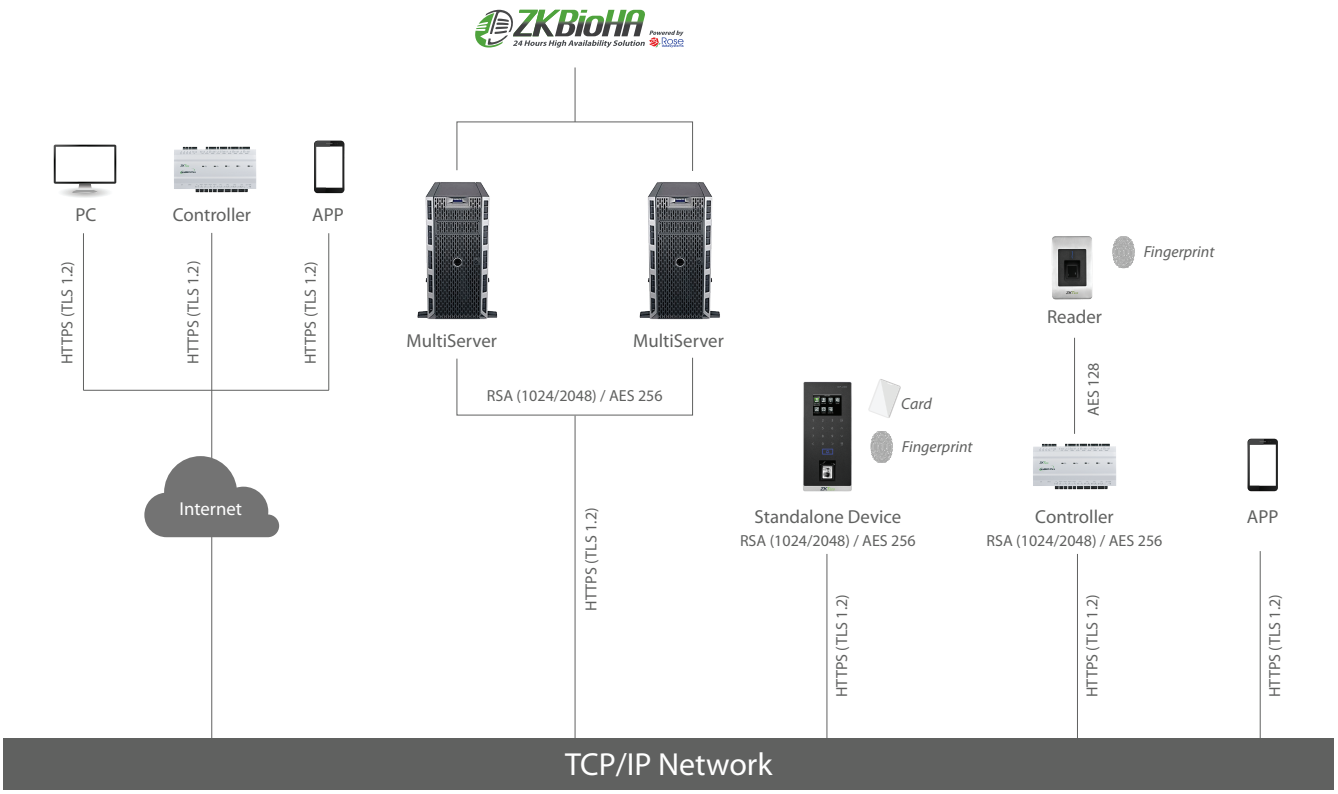


Communications Encryption

To ensure privacy and confidentiality of information, ZKTeco Applications also support the use of the following encryption technologies for communications:

ZKTeco Applications can be configured to run completely under HTTPS. Our applications support TLS encryption for client connections.

For data security over local area network (LAN) and wide area network (WAN), ZKTeco Applications support the use of Transport Layer Security (TLS) capabilities to secure transmission of data between Web browsers and the ZKTeco applications server. In addition, TLS also supports secure authentication between the ZKTeco application servers and controller devices.



Communications Encryption in the ZKTeco Basic Application Environment

*The actual condition may differ according to product model and network environment.

ZKTeco Inc.
E-mail: sales@zkteco.com
www.zkteco.com