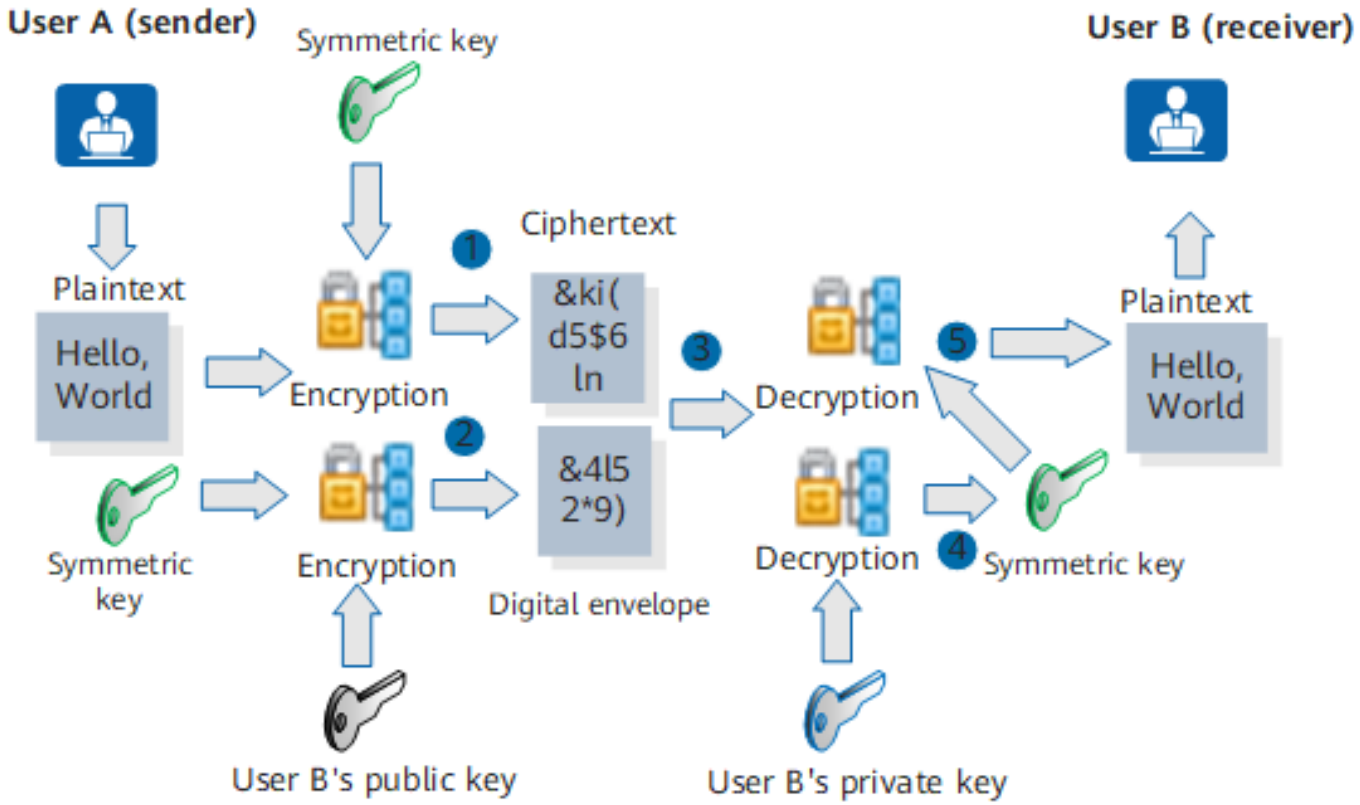
Digital Envelope
Including Keyed Hash MAC

by Ryan Baertlein

What to Expect…

- What is a digital envelope
- Project 1 implementation
  - KeyGen.java
  - Sender.java
  - Receiver.java

What is a Digital Envelope



Source: https://support.huawei.com/enterprise/en/doc/EDOC1100066169/3c50cadf/basic-concepts-of-pki

What is a Digital Envelope (cont.)

- Public key cryptography prevents security risks when distributing a symmetric key
- In asymmetric key pairs, the public key encrypts data and the private key decrypts data
- The sender/receiver *do not* exchange keys
- The sender uses the receiver’s public key to encrypt data
- The receiver uses its private key to decrypt data
- The receiver's private key is not shared to keep the data secure

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100066169/3c50cadf/basic-concepts-of-pki

Implementation: KeyGen.java

- Input: 16-character string for symmetric key generation
- Create a pair of RSA public and private keys for receiver Y, Ky+ and Ky–
- Generate a **`byte[]`** symmetric key using user input
- Save keys to file

Implementation: Sender.java

- Input: plaintext, symmetric key, and receiver Y's public key
- Concatenate (Kxy || M || Kxy),
- Calculate the hash: SHA256 (Kxy || M || Kxy), then print the hash
- Encrypt plaintext, M, using the symmetric key: AES-En Kxy (M)
- Encrypt the symmetric key with the public key: RSA-En Ky+ (Kxy)

Implementation: Receiver.java

- Input: cyphertext, hash text, encrypted symmetric key, and receiver Y's private key
- Use RSA Decryption to get the symmetric key, then print the key
- Use AES Decryption to get plaintext, M, then print and save the plaintext
- Compare the sender's hash text with the receiver's calculated hash text
    - Compare sender's SHA256 hash with the locally calculated SHA256 hash
    - Print the local hash value
    - Report hashing error if any

Its Purpose

- Digital envelopes protect the confidentiality of a message between a sender and receiver
  - The sender must use their own private key to decrypt the symmetric key
  - The symmetric key can then decrypt the message
- Improves key distribution, security, as well as overall efficiency
- The disadvantage of digital envelopes is without the use of a digital signature, the receiver cannot verify the sender’s identity