



openHPI – Internet Security Encryption Methods

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Working Principle of Symmetric 1-Key Encryption Methods

Let us start with a description of how the symmetric **1-key encryption methods** (symmetric cryptography) work ...

- Encryption and decryption of a message is done with the same key - "**secret key**"
 - both sender and receiver need this key
 - the problem: secure key exchange

- Formal mathematical description:

$$f_{\text{decrypt}}(\text{key}, f_{\text{encrypt}}(\text{key}, \text{plaintext})) = \text{plaintext}$$

1-Key Encryption Methods

Some Encryption principles:

- Diffusion
 - each piece of the plaintext should influence as many places as possible in the encrypted cipher text, so that minor changes in the plaintext will lead to many changes in the cipher text
- Confusion:
 - The connection between cipher text and the key should be as complex as possible to make interference more difficult

Common procedures use a **round-based approach**

- To increase complexity, the encryption is applied with different (parts of the) key on repeatedly "rearranged" text

DES – Data Encryption Standard

- First official encryption standard of US government from 1976
- As it has merely a key length of 56 bits it should no longer be used, since the resulting possible number (2^{56}) of different keys is not high enough to withstand brute force
- Triple-DES runs the DES algorithm three times, thus attaining a higher security level

AES – Advanced Encryption Standard

- It is the method that won the cryptography competition in 2000
- Since then it is deemed as the encryption standard and DES successor
- Has various key lengths: 128, 192, 256 bits

Before communication can be protected by means of 1-key encryption, communication partners must agree on a common secret key ...

- The key cannot be sent unencrypted over the open Internet, otherwise, attackers can eavesdrop the key during transport over the Internet and later decrypt the encrypted content
- Key exchange is a basic problem of 1-key encryption
 - one possible solution is to use the “Diffie-Hellman” key exchange method
- This problem does not occur when the communication is protected by means of **2-key** encryption methods

Now let's consider **2-key encryption methods**:

- Main idea: The use of a pair of keys for encryption and decryption purposes:
 - **Private key:**
 - must be kept secret from every other subscriber
 - **Public key:**
 - is made available to all other subscribers
- Message encrypted with a public key can only be decrypted with the associated private key
- Message encrypted with a private key can only be decrypted with the associated public key

Important Requirement:

- The private key **cannot be calculated** from the associated public key

2-Key Procedure Methods – Encryption and Decryption (1/2)

Requirement:

- Each user has a key pair consisting of
 - a secret private key K_{private}
 - a public key K_{public}
- The public key must be
 - freely accessible for everyone and
 - safely dedicated to its owner

Encryption of a message with a user's **public** key allows only that user to decrypt the message with their private key

$$f_{\text{decrypt}}(K_{\text{private}}, f_{\text{encrypt}}(K_{\text{public}}, \text{plaintext})) = \text{plaintext}$$

Confidentiality of the message can thus be ensured

2-Key Procedure Methods – Encryption and Decryption (2/2)

Encryption of a message with a user's private key allows anyone else to verify that the message originates from the sender, namely only when a message can be decrypted with their public key

$$f_{\text{decrypt}}(\mathbf{K}_{\text{public}}, f_{\text{encrypt}}(\mathbf{K}_{\text{private}}, \text{plaintext})) = \text{plaintext}$$

Liability and message **integrity** can thus be ensured

Precondition: Both procedures work only if:

- public keys are not compromised; and
- private keys are kept secret

RSA

- Developed by **R**ivest, **S**hamir and **A**dleman
- Most web servers use the RSA method to secure connections
- RSA supports different key lengths; nowadays, keys should be at least **2048 bits** long
- The security of RSA is based on the mathematical problem of prime factorization of large numbers, which is very difficult to solve
 - more on that will be explained in an excursion

Hybrid Encryption

Hybrid encryption methods combine advantages of 1-key and 2-key encryption methods for compensating their disadvantages

Why is a combination useful?

- 1-key encryptions are very efficient, but require a safe exchange of the secret key
- 2-key encryption does not require a secure key exchange, but is very complex to calculate and therefore not suitable for large amounts of data

Hybrid methods combine efficiency of 1-key encryption methods with the initial security of 2-key encryption methods

Hybrid Encryption – Working Principle

Communication partners agree on

- 1-key method **X** and
- 2-key method **Y**

- 1) Generation of a random secret session key **S** for later application of the 1-key encryption **X**
- 2) By means of the 2-key encryption method **Y**, the session key **S** is encrypted with the public key of the receiver and sent to him/her
- 3) The receiver decrypts the received session key **S** with his private key
- 4) Actual communication can now be secured using the 1-key method **X** with the securely exchanged session key **S**

Hybrid encryption is used in many places on the Internet to secure communication:

- Network protocol suite **IPsec**
 - Security of Internet data packets on the transport layer
- **TLS/SSL** – Transport Layer Security / Secure Sockets Layer
 - protection of Internet connections, e.g.,
for web applications (online banking)
- Encryption of emails:
 - **PGP** – Pretty Good Privacy
 - **GPG** – GNU Privacy Guard