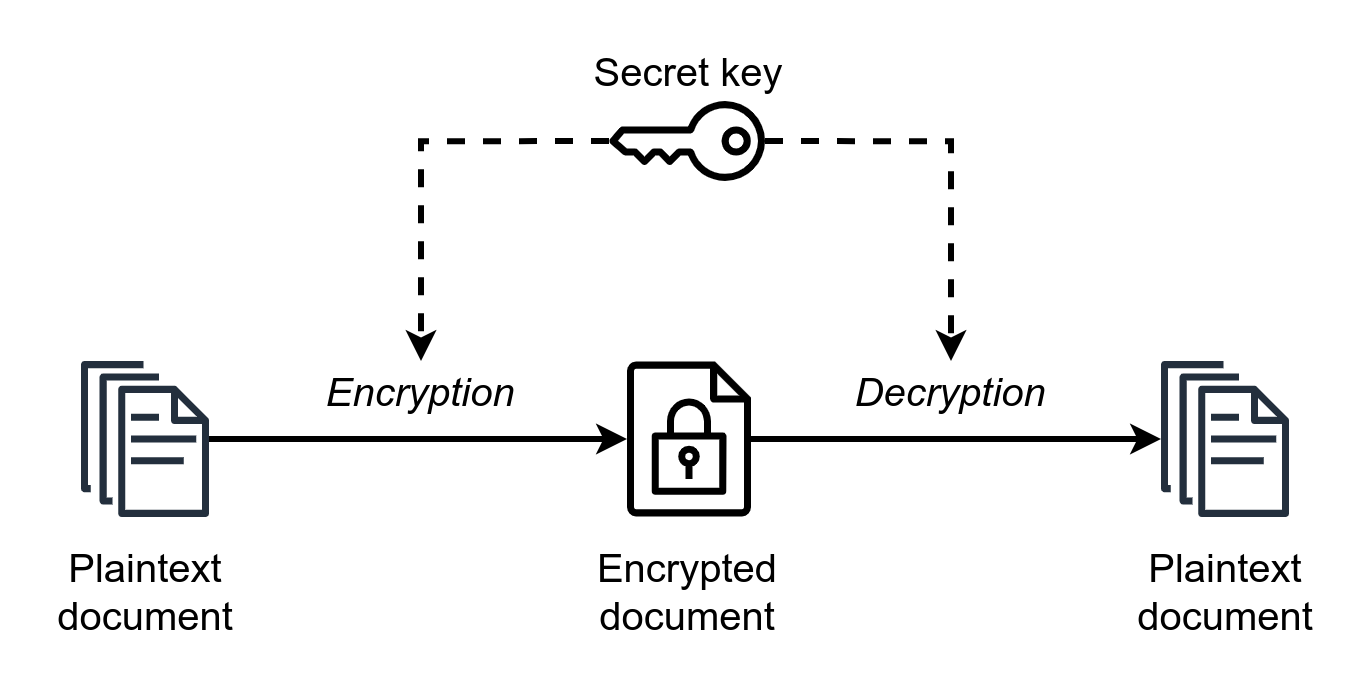
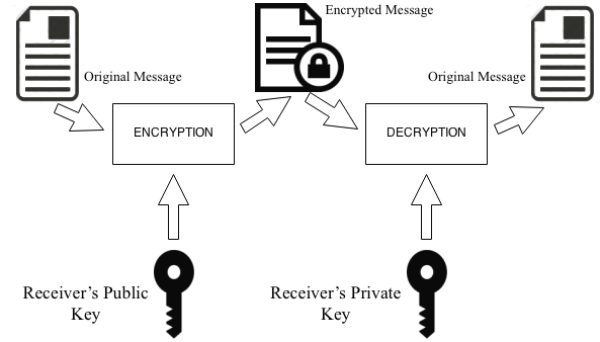
**Symmetric and Asymmetric crypto systems**-

n operating system security, both symmetric and asymmetric cryptographic systems play important roles in ensuring confidentiality, integrity, authentication, and other security aspects. Here's an overview of symmetric and asymmetric crypto systems in operating system security:

Symmetric Cryptography: 

1. Shared Key: Symmetric cryptography uses a shared secret key for both encryption and decryption. The same key is used by both the sender and recipient.
2. Efficiency: Symmetric algorithms, such as AES (Advanced Encryption Standard) or DES (Data Encryption Standard), are computationally efficient and suitable for encrypting large amounts of data.
3. Confidentiality: Symmetric encryption provides strong confidentiality, ensuring that only authorized parties possessing the secret key can decrypt the encrypted data.
4. Key Distribution: The main challenge with symmetric cryptography is securely distributing the shared key to all authorized parties. Key management becomes critical for maintaining confidentiality.
5. Examples of Usage: Symmetric encryption is commonly used for disk encryption, file encryption, network communication encryption (e.g., SSL/TLS), and data protection within an operating system.

Asymmetric Cryptography: 

1. Public and Private Keys: Asymmetric cryptography uses a pair of keys: a public key for encryption and a private key for decryption. The keys are mathematically related but computationally infeasible to derive one from the other.
2. Key Distribution and Authentication: Asymmetric cryptography addresses the key distribution challenge faced by symmetric encryption. The public keys can be freely distributed, while private keys remain securely stored.
3. Digital Signatures: Asymmetric cryptography enables the generation and verification of digital signatures, ensuring data integrity, authenticity, and non-repudiation.
4. Key Exchange: Asymmetric cryptography also allows secure key exchange protocols, such as Diffie-Hellman, to establish shared secret keys between two parties over an insecure channel.
5. Efficiency and Performance: Asymmetric algorithms, such as RSA or ECC (Elliptic Curve Cryptography), are computationally more expensive than symmetric algorithms. Hence, they are typically used for encrypting smaller data blocks, digital signatures, key exchange, and authentication.

Hybrid Approach: To leverage the benefits of both symmetric and asymmetric cryptography, a hybrid approach is often employed in operating system security. This involves using symmetric encryption for bulk data encryption due to its efficiency, and asymmetric encryption for secure key exchange, digital signatures, and authentication.

For example, in an SSL/TLS protocol, the server and client establish a secure connection using asymmetric encryption to exchange a shared secret key. Once the shared key is established, symmetric encryption is used for efficient data transmission.

Overall, symmetric and asymmetric cryptography complement each other, providing a robust security framework within operating systems. Their combined usage helps ensure confidentiality, integrity, authentication, and other essential security properties.