### **File Encryption Techniques**

### **1. Advanced Encryption Standard Crypt**

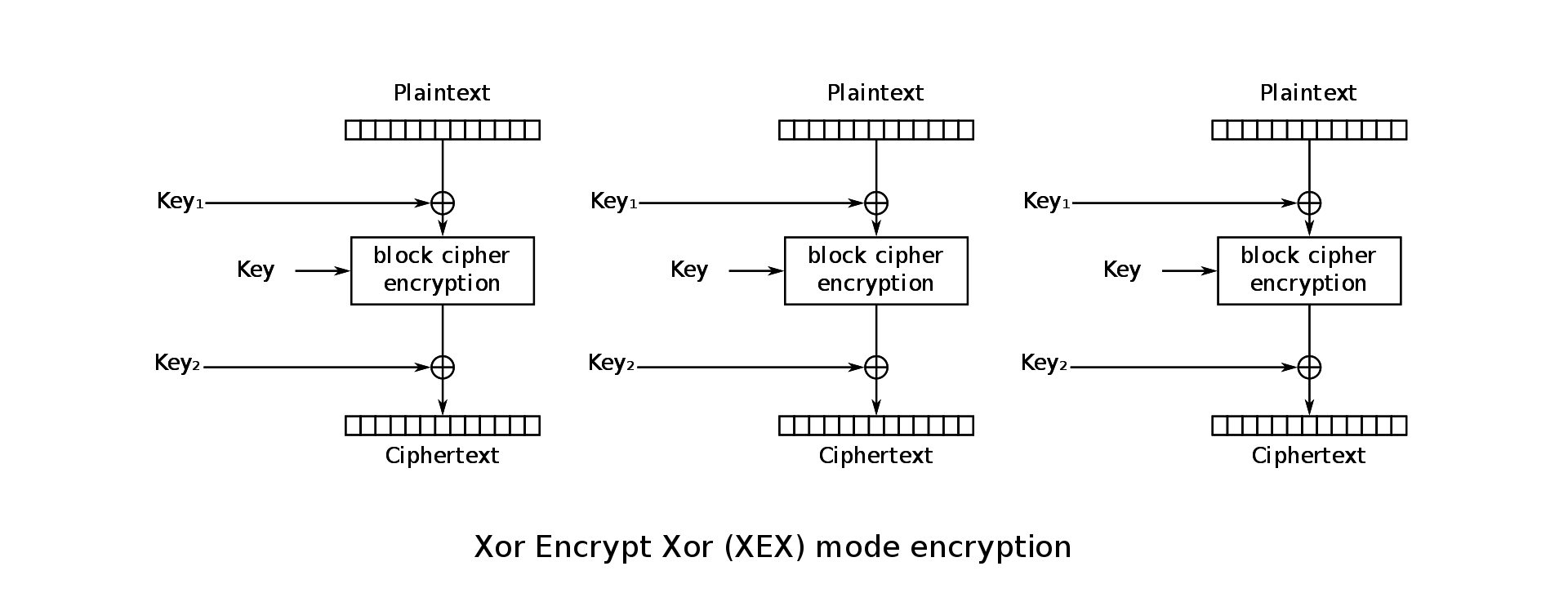
AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files. Using a powerful 256-bit encryption algorithm, AES Crypt can safely secure most sensitive files. perfect solution for those who wish to backup information and store that data at a bank, in a cloud-based storage service, and any place where sensitive files might be accessible by someone else.

### **2. Rivest-Shamir-Adleman (RSA)**

Rivest-Shamir-Adleman is an asymmetric encryption algorithm that is based on the [factorization](https://searchsecurity.techtarget.com/definition/RSA) of the product of two large prime numbers. Only someone with the knowledge of these numbers will be able to decode the message successfully. RSA is often used when transmitting data between two separate endpoints (e.g., web connections), but works slowly when large volumes of data need to be encrypted.

**3. DES-X**

The reason for the introduction of the DES-X was an attempt to increase the security of the original DES algorithm. The proposed solution with DEX-X was to use two more 64-bit keys which would be applied to make it harder for an attacker to guess the key of the DES algorithm. Basically, the first additional key is XORed to the plain text which is then encrypted with DES. The second additional key is XORed to the resulting cipher.



### **4. Triple DES (Data Encryption Standard)**

Triple DES is a symmetric encryption and an advanced form of the DES method that encrypts blocks of data using a 56-bit key. Triple DES applies the DES cipher algorithm three times to each data block. Triple DES is commonly used to encrypt ATM PINs and UNIX passwords.

### **5. Twofish**

Twofish is a license-free encryption method that ciphers data blocks of 128 bits. It’s considered the successor to the 64-bit Blowfish encryption method and more versatile than its specialized successor, Threefish. Twofish always encrypts data in 16 rounds regardless of the key size. Though it works slower than AES, the Twofish encryption method continues to be [used by some file and folder encryption software solutions](https://www.schneier.com/academic/twofish/products/).

**6. Open SSL Tool**

[OpenSSL](https://www.openssl.org/) is an amazing tool that does a variety of tasks, including encrypting files.

### **Step 1: Generate key pairs**

Before you can encrypt files, you need to generate a pair of keys. You will also need a passphrase, which you must use whenever you use OpenSSL, so make sure to remember it.

### **Step 2: Extract the public keys**

Remember, the public key is the one you can freely share with others, whereas you must keep your private key secret. So, Alice must extract her public key and save it to a file using the following command:

### **Step 3: Exchange public keys**

These public keys are not much use until they exchange them with each other. Several methods are available for sharing public keys, including copying the keys to each other's workstations using the scp command.

### **Step 4: Exchange encrypted messages with a public key**

To encrypt this secret message, one needs to use the openssls -encrypt command, providing three inputs to the tool:

1. The name of the file that contains the secret message
2. public key (file)
3. The name of a file where the encrypted message will be stored

After encryption, the original file is still viewable, whereas the newly created encrypted file looks gibberish on the screen. You can be assured that the secret message has been encrypted:

### **Step 5: Decrypt the file using a private key**

using the -decrypt command-line argument providing the following information to the utility:

1. The encrypted file (which he got from sender)
2. own private key
3. A file name to save the decrypted output to via redirection