Aim: Implementation of Symmetric and Asymmetric Key Cryptographic Algorithm using Kali Linux

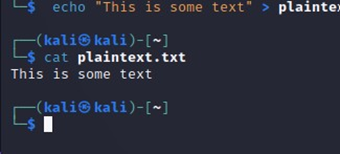
Software Required: -

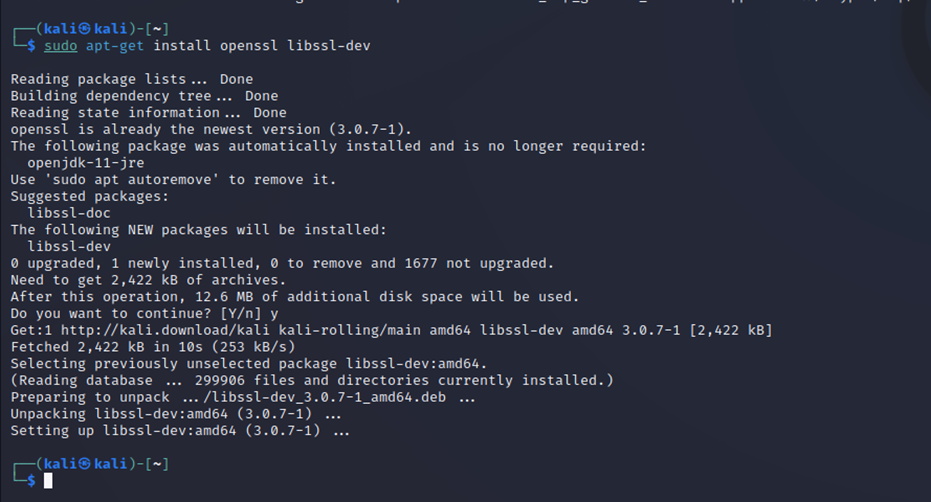
Kali Linux, Metaspoitable

Procedure and Outputs: -

Implementation of Symmetric Key Cryptographic Algorithm using Kali Linux: -

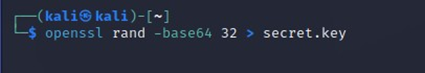






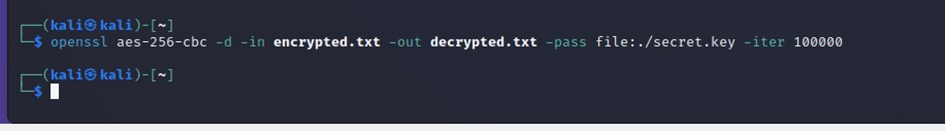
Generate a secret key:

• In this step, we will generate a secret key that will be used for both encryption and decryption. We will use OpenSSL to generate a random key with the AES-256 cipher:



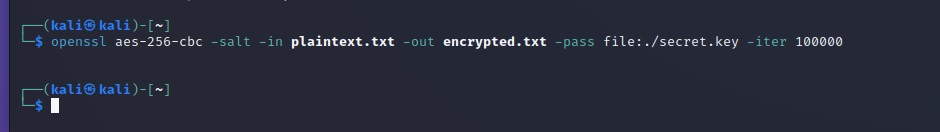
Encrypt a file:

• In this step, we will use the secret key to encrypt a file using AES algorithm:



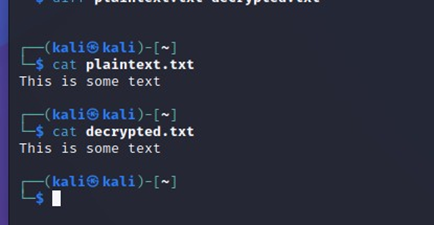
Decrypt a file:

• In this step, we will use the same secret key to decrypt the encrypted file:



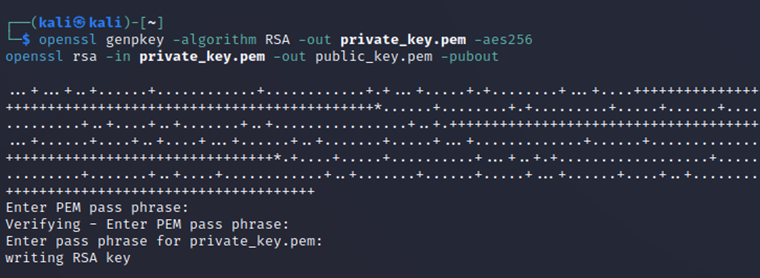
Verify the decrypted file:

• In this step, we will verify that the decrypted file is identical to the original plaintext file:

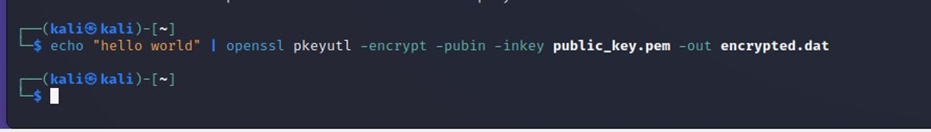


Implementation of Asymmetric Key Cryptographic Algorithm using Kali Linux:

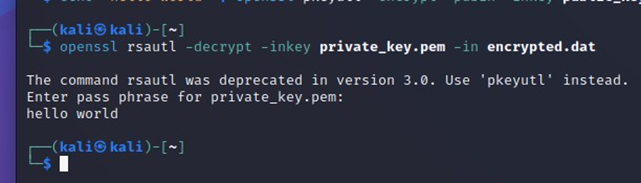
Step 1: Generate Key Pairs We need to generate a public/private key pair first. To generate an RSA key pair with 2048 bits, use the following command:



Step 2: Encryption Now that we have the key pairs, let's use the public key to encrypt a message. In this example, we will encrypt a message "hello world" and store the encrypted message in a file called "encrypted.dat".



Step 3: Decryption To decrypt the encrypted message, we need to use the private key. The following command will decrypt the message and print it to the console:



The above command will use the private key to decrypt the message and print it to the console.

Result: -

Successfully all commands were executed.