

The lab is on familiarization with the OpenSSL utility and its various options.

1. Encoding a text file's contents in Base64 format
2. Encrypting a file with DES, with no salt used and decrypting the encrypted file
3. Testing encryption by encrypting a file with DES and then attempting to decrypt it using a wrong password
4. Generating an RSA key pair
5. Displaying the key pair and the related information of the generated RSA key pair
6. Generating the public RSA keyfile from the RSA key pair generated before and displaying the contents of the public RSA keyfile
7. Encrypting a sample text file with the public key generated earlier
8. Decrypting the generated ciphertext file using the private key generated
9. Testing encryption and decryption using a symmetric cipher method (AES-256-CBC or any other symmetric cipher)
10. Generating a MD5 hash of the contents of a text file
11. Generating a signed digest with SHA512 method, using the RSA private key generated before for the signature and verifying the integrity of the file using the signed digest and the public key
12. Generating a new certificate signing request with the RSA key pair generated earlier
13. View the contents of the certificate signing request
14. Automatically signing a certificate request and create the a self signed certificate
15. View the content of certificate