Cyber Security Lab

RSA in Real Life (OpenSSL on Linux)

You can explore RSA key generation and encryption using OpenSSL commands:

```
# Generate private key
openssl genrsa -out private.pem 2048


# Extract public key
openssl rsa -in private.pem -pubout -out public.pem


# Encrypt file using public key
echo "SAEED" > message.txt

openssl rsautl -encrypt -inkey public.pem -pubin -in message.txt
-out encrypted.bin


# Decrypt file using private key
openssl rsautl -decrypt -inkey private.pem -in encrypted.bin -
out decrypted.txt

cat decrypted.txt
```

File Verification by RSA Signature Demonstration

RSA can also be used for authentication and integrity.

```
# Generate hash of a message
echo "Important data" > data.txt
openssl dgst -sha256 -sign private.pem -out signature.bin
data.txt

# Verify the signature
openssl dgst -sha256 -verify public.pem -signature signature.bin
data.txt
```

RSA demo using Python (no libraries, just math):

```
# RSA example in Python

# Step 1: Select primes
p = 17
q = 11
n = p * q
phi = (p - 1) * (q - 1)

# Step 2: Choose e and compute d
e = 7
d = 103  # since 7 * 103 = 721 ≡ 1 mod 160

# Step 3: Encrypt and Decrypt
msg = 88  # Message as integer
cipher = pow(msg, e, n)
print("Encrypted:", cipher)

decrypted = pow(cipher, d, n)
print("Decrypted:", decrypted)
```