OpenSSL Quick Reference Guide

Installation & Setup

```bash
# Check if OpenSSL is installed
type openssl

# Install OpenSSL (if needed)
sudo apt-get install openssl

# Get help
openssl
man openssl
```

Basic File Encryption

Create Test File

```bash
echo "This is confidential information." > plaintext.txt
cat plaintext.txt
```

Encrypt File (AES-256)

```bash
openssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.txt -k password123
```

Decrypt File

```bash
openssl enc -d -aes-256-cbc -in encrypted.txt -out decrypted.txt -k password123
cat decrypted.txt
```

List Files

```bash
ls
# Shows: plaintext.txt, encrypted.txt, decrypted.txt
```

Command Breakdown

openssl enc -aes-256-cbc -salt -in file -out encrypted -k password

- `openssl enc` = calls OpenSSL encoding tool
- `-aes-256-cbc` = AES encryption with 256-bit key in CBC mode
- `-salt` = adds randomness for better security
- `-in file` = input file to encrypt
- `-out encrypted` = output file for encrypted data
- `-k password` = password for encryption

openssl enc -d -aes-256-cbc -in encrypted -out decrypted -k password

- `-d` = decrypt mode
- `-aes-256-cbc` = same encryption algorithm for decryption
- `-in encrypted` = encrypted file to decrypt
- `-out decrypted` = output file for decrypted content

Common Issues & Solutions

Incorrect password:

- Error: `bad decrypt`
- Solution: Double-check password spelling

File not found:

- Check file paths and filenames
- Use `ls` to verify files exist

Permission issues:

- Run with `sudo` if needed
- Check file permissions