Georgia Gwinnett College
School of Science and Technology
ITEC 3300: Information Security
OpenSSL Commands Cheat Sheet

Generate a random secret key

openssl rand ***numbytes*** **>** ***filename***

- The function **rand** implements a cryptographically strong pseudorandom generator.
- The parameter ***numbytes*** following **rand** is the number of pseudorandom *bytes* to output. For example, if you want to generate a random 256 bit key for AES, you would use 32 for ***numbytes*** (because 32 bytes = 256 bits).
- The "**>**" sign redirects the output of a command to a file.
- The parameter ***filename*** is the name of the file to store the output.

Encrypt a file using 256-bit AES with the CBC mode

openssl aes-256-cbc -pbkdf2 -e -in ***plain_file*** **-out** ***cipher_file*** **-pass file:***key_file*

- The cipher **aes-256-cbc** specifies that the **AES** block cipher with a **256-bit key**, in the **CBC** mode of operation, is used.
- The option **-pbkdf2** specifies that **pbkdf2**, a commonly used password-based key derivation function, is used to derive a one-time key and an initialization vector (IV) from a password or a master key.
- The option **-e** specifies that *encryption* is to be performed.
- The option **-in** ***plain_file*** specifies that ***plain_file*** is the name of the input file that contains the plaintext to encrypt.
- The option **-out** ***cipher_file*** specifies that ***cipher_file*** is the name of the output file to write the ciphertext.
- The option **-pass** specifies the source of the key.
- The argument **file:***key_file* specifies that ***key_file*** is the name of the file that contains the *master* key to derive one-time keys from.

openssl aes-256-cbc -pbkdf2 -e -in *plain_file* -out *cipher_file* -pass pass:*password*

- The cipher **aes-256-cbc** specifies that the **AES** block cipher with a **256-bit key**, in the **CBC** mode of operation, is used.
- The option **-pbkdf2** specifies that **pbkdf2**, a commonly used password-based key derivation function, is used to derive a one-time key and an initialization vector (IV) from a password or a master key.
- The option **-e** specifies that *encryption* is to be performed.
- The option **-in *plain_file*** specifies that ***plain_file*** is the name of the input file that contains the plaintext to encrypt.
- The option **-out *cipher_file*** specifies that ***cipher_file*** is the name of the output file to write the ciphertext.
- The option **-pass** specifies the source of the password.
- The argument **pass:*password*** specifies that the parameter ***password*** following **pass:** in the command, is the actual password to derive one-time keys from.

Decrypt a file using 256-bit AES with the CBC mode

openssl aes-256-cbc -pbkdf2 -d -in *cipher_file* -out *plain_file* -pass file:*key_file*

- The cipher **aes-256-cbc** specifies that the AES block cipher with a 256-bit key, in the CBC mode of operation, is used.
- The option **-pbkdf2** specifies that **pbkdf2**, a commonly used password-based key derivation function, is used to derive a one-time key and an initialization vector (IV) from a password or a master key.
- The option **-d** specifies that *decryption* is to be performed.
- The option **-in *cipher_file*** specifies that ***cipher_file*** is the name of the input file that contains the ciphertext to decrypt.
- The option **-out *plain_file*** specifies that ***plain_file*** is the name of the output file to write the plaintext.
- The option **-pass** specifies the source of the key.
- The argument **file:*key_file*** specifies that ***key_file*** is the name of the file that contains the *master* key, which should be the same master key used for encryption.

openssl aes-256-cbc -pbkdf2 -d -in *cipher_file* -out *plain_file* -pass pass:*password*

- The cipher **aes-256-cbc** specifies that the AES block cipher with a 256-bit key, in the CBC mode of operation, is used.

- The option **-pbkdf2** specifies that **pbkdf2**, a commonly used password-based key derivation function, is used to derive a one-time key and an initialization vector (IV) from a password or a master key.

- The option **-d** specifies that *decryption* is to be performed.

- The option **-in *cipher_file*** specifies that ***cipher_file*** is the name of the input file that contains the ciphertext to decrypt.

- The option **-out *plain_file*** specifies that ***plain_file*** is the name of the output file to write the plaintext.

- The option **-pass** specifies the source of the key.

- The argument **pass:*password*** specifies that the parameter ***password*** following **pass:** in the command, is the actual password, which should be the same password used for encryption.

(To be continued)