OpenSSL Encryption!

By: Isaac Chang

OpenSSL

- Software library that provides secure communication methods and encryption options
- Includes the two encryption methods we talked about last time!

Go to repl.it and do the following steps:

- Create a Debian Linux repl.it environment
- Follow the instructions on the readme page
- Once you finish, you should have a Debian Linux environment ready!

Download sudo, nano and OpenSSL

Sudo allows you to execute system commands like maintaining privileges and downloading libraries

Download OpenSSL, which is the library we will be using

Commands:

apt-get install sudo -y

sudo apt-get update

sudo apt-get install openssl

sudo apt-get -y install nano

Create a text file with a message using nano

We did this two lessons ago!

Create encryption key!

Use the web to see if you can figure out how to create a 128 byte symmetric encryption key!

openssl rand -out keyfile.bin 32

Run AES encryption command to encrypt created txt file

openssl enc -aes-256-cbc -salt -in hello.txt -out encryptedfile.txt -kfile key.bin

Command breakdown:

Openssl - first word typically signifies what library you are running

enc - similar to a setting/mode in openssl

-aes-256-cbc - the encryption method

-salt - declares that you want to add extra values to make the encryption harder to break

- in - a command flag that is followed by the file you want to encrypt

-out - a command flag that is followed by the name of the file after encryption

-kfile - a command flag that means openssl is taking a file as the encryption key

Note: each library has their own unique flags, make sure you know what you are doing!

See what happens when you try to read the encrypted file!

Hint: cat

Decrypt!

openssl enc -d -aes-256-cbc -salt -in encryptedfile.txt -out decryptedfile.txt -kfile key.bin

Just add a -d flag after the enc word! -d means decrypt

Also, switch the input and output!

How does this work with multiple people?

- Send your encryption key to trusted members
- Encrypt the messages you want to send, and send encrypted messages to them!
- They can then decrypt it with the encryption key you gave them

Obviously, this is insecure because anyone with the key and encrypt and decrypt. That’s where RSA comes in…