

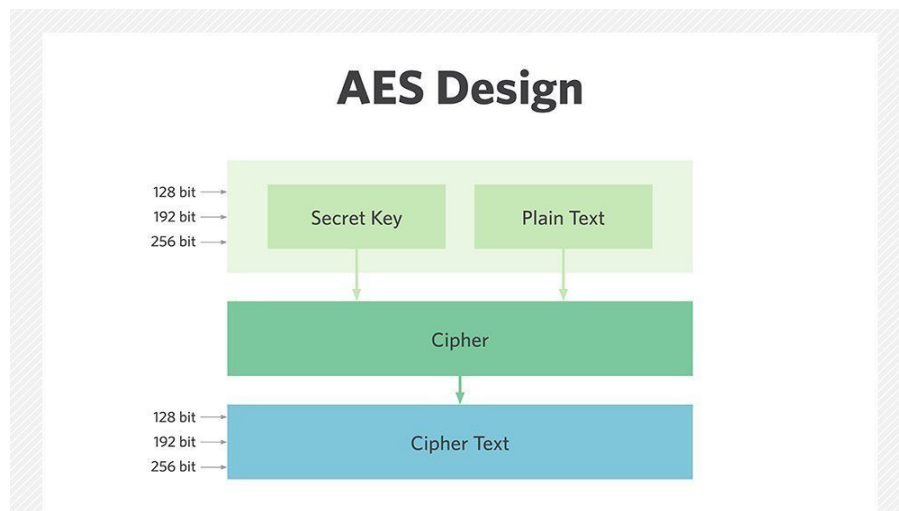
Assignment 1

1. Set up Wireshark for a specific interface. Go to a website which involves sending HTTP requests, it could be a website you set up on your own as well. Send a HTTP request and analyze the packet on wireshark. Analyze the packet.
Include following details : Frame number of the sent request, frame number of the received response, protocol used, source , destination, etc.
2. There is a packet capture file created during some connection. The packet capture file gives you information of the packets transferred and received and their details. Find out a vulnerability in the connection. Here is a link to the pcap file generated :
<https://drive.google.com/file/d/1FWI3lU0o-l-fuC824etKzTm9fDbHEKsQ/view?usp=drivesdk>
Analyze the file using Wireshark. Write down what you find.

To ensure no copying/plagiarism, let's make the submission a bit interesting.
You will have to encrypt your answer using AES algorithm.

What is AES?

It is a symmetric encryption algorithm. Don't worry about how it works or what symmetric encryption is. **We will teach you this in a lot of detail soon.** I'm sure you all know what encryption is. Just know that it is an encryption algorithm which takes text and a key as input and produces an encrypted text as output.

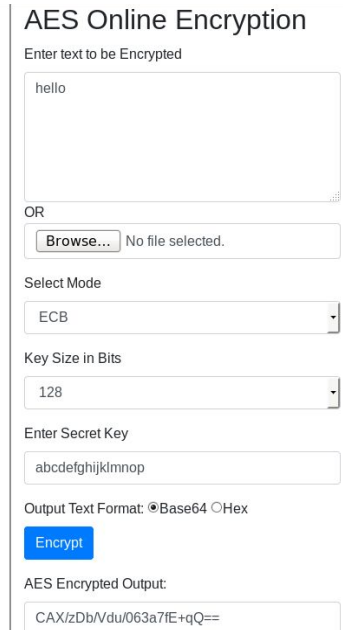


This is a tool you can use to encrypt the file :

<https://www.devglan.com/online-tools/aes-encryption-decryption>

Use a **128** bit key, i.e, 16 characters long key and in **ECB** mode. (Again, I will teach you this soon enough)

For example :



The screenshot shows a web interface titled "AES Online Encryption". It has two input methods: "Enter text to be Encrypted" with a text area containing "hello", and "OR" with a file upload button labeled "Browse..." and the text "No file selected.". Below these are three dropdown menus: "Select Mode" set to "ECB", "Key Size in Bits" set to "128", and "Enter Secret Key" containing the 16-character key "abcdefghijklmnop". There is a radio button for "Base64" (selected) and a radio button for "Hex". A blue "Encrypt" button is present. At the bottom, the "AES Encrypted Output:" is shown as "CAX/zDb/Vdu/063a7fE+qQ==".

Put the AES encrypted output in a text file(your_name.txt) in the folder **Assignment 1**, similar to Assignment 0.

PM the secret key to me.

I will decrypt and check your answers. xP
Please ask doubts as and when you encounter them.
All the best!