Lab - Creating Codes

Objectives

In this lab, you will create and encrypt messages using online tools.

Part 1: Search for an online encoding and decoding tool.

Part 2: Encrypt a message and email it to your lab partner.

Part 3: Decrypt the ciphertext.

Background / Scenario

Secret codes have been used for thousands of years. Ancient Greeks and Spartans used a scytale (rhymes with Italy) to encode messages. Romans used a Caesar cipher to encrypt messages. A few hundred years ago, the French used the Vigenère cipher to encode messages. Today, there are many ways that messages can be encoded.

There are several encryption algorithms that can be used to encrypt and decrypt messages. Virtual Private Networks (VPNs) are commonly used to automate the encryption and decryption process.

In this lab, you and a lab partner will use an online tool to encrypt and decrypt messages.

Required Resources

- PC with internet access

Instructions

Part 1: Search for an online encoding and decoding tool.

There are many different types of encryption algorithms used in modern networks. One of the most secure is the Advanced Encryption Standard (AES) symmetric encryption algorithm. We will be using this algorithm in our demonstration.

a. In a Web browser, search for **encrypt decrypt AES online**. Several different tools will be listed in the search results.

b. Explore the different links provided and choose a tool. In our example, we used the tool available from:

http://aesencryption.net/

Part 2: Encrypt a message and email it to your lab partner.

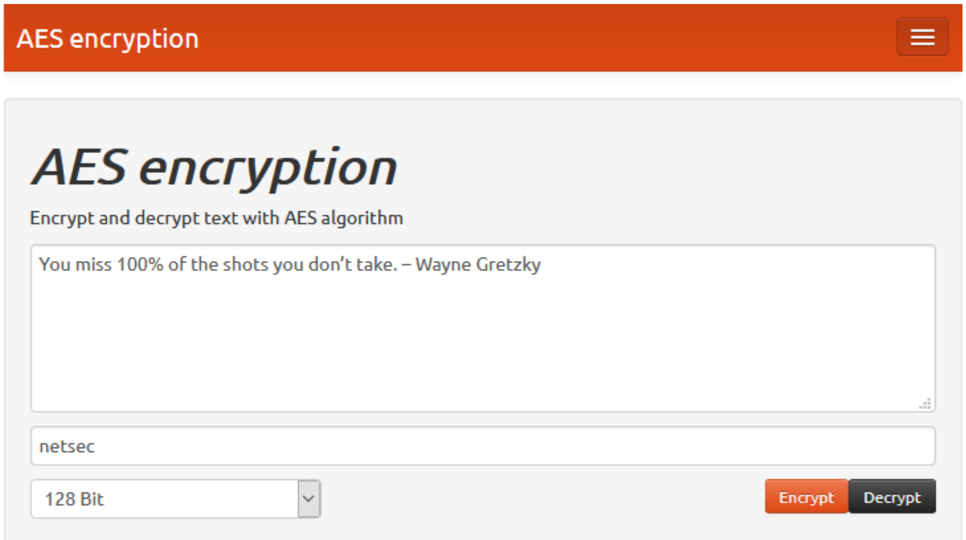
In this step, each lab partner will encrypt a message and send the encrypted text to the other lab partner.

Note: Unencrypted messages are referred to as plaintext, while encrypted messages are referred to as ciphertext.

a. Enter a plaintext message of your choice in the text box. The message can be very short or it can be lengthy. Be sure that your lab partner does not see the plaintext message.

A secret key (i.e., password) is usually required to encrypt a message. The secret key is used along with the encryption algorithm to encrypt the message. Only someone with knowledge of the secret key would be able to decrypt the message.

b. Enter a secret key. Some tools may ask you to confirm the password. In our example, we used **netsec** as the secret key.



AES encryption

AES encryption

Encrypt and decrypt text with AES algorithm

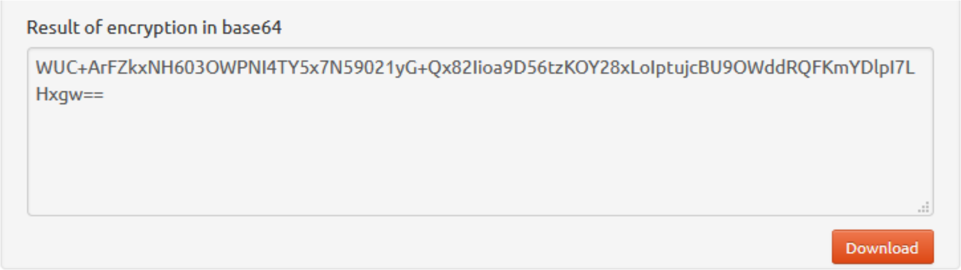
You miss 100% of the shots you don’t take. – Wayne Gretzky

netsec

128 Bit

c. Next click on **Encrypt**.

In the Result of encryption in base64 window, random text is displayed. This is then encrypted message.



Result of encryption in base64

```
WUC+ArFZkxNH603OWPNI4TY5x7N59021yG+Qx82Iioa9D56tzKOY28xLoIptujcBU9OWddRQFKmYDlpI7L
Hxgw==
```

d. Copy or Download the resulting message.

e. Email the encrypted message to your lab partner.

Part 3: Decrypt the ciphertext.

AES is a symmetric encryption algorithm This means that the two parties exchanging encrypted messages must share the secret key in advance.

a. Open the email from your lab partner.

b. Copy the ciphertext and paste it in the text box.

c. Enter the pre-shared secret key.

d. Click **Decrypt** and the original cleartext message should be displayed.

What happens if you use a wrong secret key?