

## 21.0.3 Lab - Creating Codes



This lab has been updated for use on NETLAB+.  
[www.netdevgroup.com](http://www.netdevgroup.com)

### Objectives

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.

In this lab, you will create and encrypt messages.

**Part 1: Encrypt a message.**

**Part 2: Decrypt the ciphertext.**

### Background / Scenario

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 will use a tool to encrypt and decrypt messages.

### Instructions

#### Part 1: Encrypt a message.

In this step, you will encrypt a message.

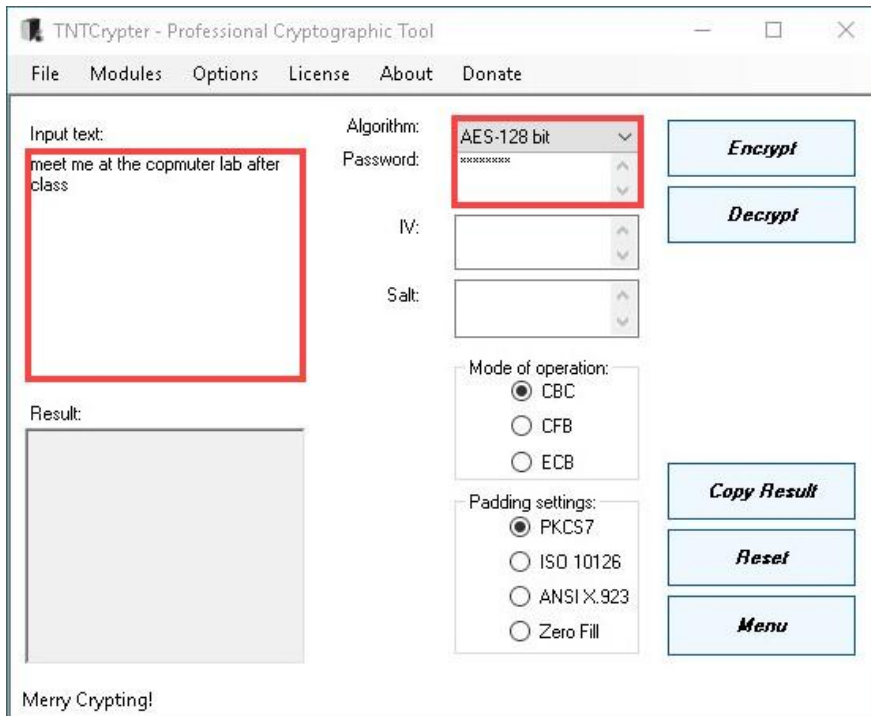
**Note:** Unencrypted messages are referred to as plaintext, while encrypted messages are referred to as ciphertext.

- Access the **WinClient** machine. Unlock the machine by clicking on the drop-down arrow for that specific machine's tab and select **Send CTRL+ALT+DEL**.
- Login as the **CyberOpsUser** using **cyberops** as the password.
- Navigate to the **Toolbox** folder and double-click **tntcrypter\_2.0.0.0** to launch the application.
- In the application window, click on the **Encrypt or Decrypt** button within the *Text* panel.
- Enter a plaintext message of your choice in the text box. The message can be very short or it can be lengthy. For this example, "**meet me at the computer lab after class**" message was used.

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.

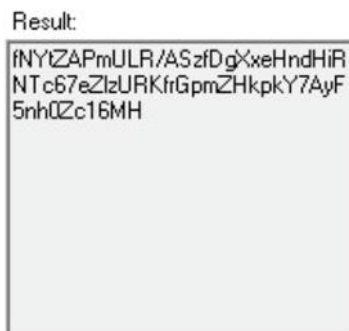
### 21.0.3 Lab - Creating Codes

- f. Enter a secret key. Some tools may ask you to confirm the password. In our example, we used the cyberops secret key. Make sure to select **AES-128 bit** as the algorithm.



- g. Next click on **Encrypt**.

In the *Result* pane, random text is displayed. This is then encrypted message.



- h. Click **Copy Result**.
- i. Open **Notepad**, paste the encrypted message, and then proceed to save the text file in **C:\Users\CyberOpsUser\Documents** as encrypted.txt as the filename.
- j. Log out from the *CyberOpsUser*.

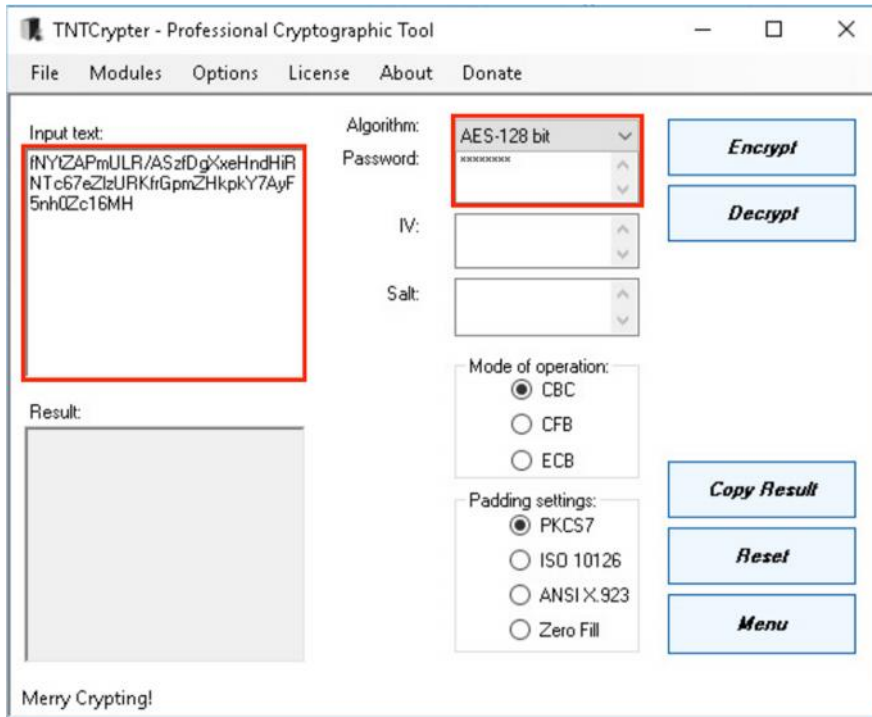
### Part 2: Decrypt the ciphertext.

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

- a. Log back into **WinClient** as the Administrator using cyberops as the password.
- b. Navigate to the **Toolbox** folder and double-click **tntcrypter\_2.0.0.0** to launch the application.

### 21.0.3 Lab - Creating Codes

- Change focus back to the **File Explorer** window, navigate to **C:\User\CyberOpsUser\Documents**, and open the **encrypted.txt** file.
- Copy the encrypted message.
- Change focus to the **TNTCrypter** application and click **Encrypt or Decrypt**.
- Paste the encrypted message into the **Input text** field, choose **AES-128 bit** as the *Algorithm*, and type cyberops into the *Password* field.



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



What happens if you use a wrong secret key?

---

---

---

---