# LAB 2

Virtual Machine/Cryptoanalysis

PM

100 Points Total

DUE 2/16/2020 11:59:59

## Overview

In this lab, students will learn about Virtual Machines (VMs) and their importance to testing. Testing Cryptool2 to encrypt and decrypt various ciphers.

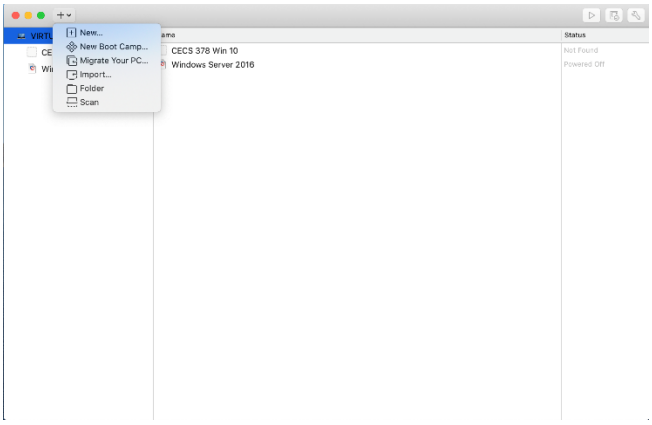
## Assignment & Instructions

Go to https://www.cryptool.org/en/ct2-downloads download and install the **CrypTool 2.1 (Stable Build 8186.5).** It is the most recent and stable build they have available.

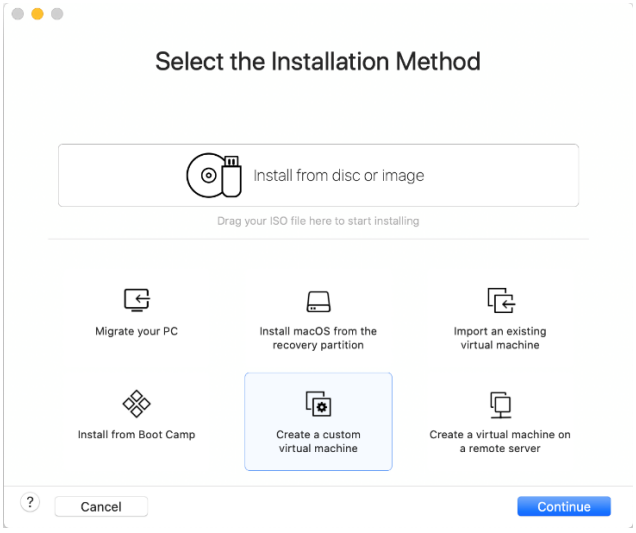
Note: For each question asked, label your answer with the part, followed by the instruction. For example, your response to a question posed in Part 1, instruction 1, should be labeled as **I-1:**

### Part I: Preparation (10pts)

1. Create a Virtual Machine (VM) running Windows 10 (If you don't already have one)
    - The following instructions were done using VMware Fusion
2. Open up VMware fusion. Click on the "+" symbol and select New…




3. Click on "Create a custom virtual machine" and click "Continue"



# LAB 2

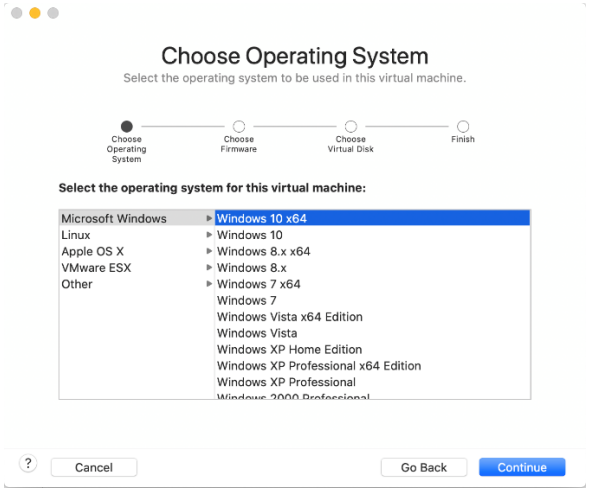
## Virtual Machine/Cryptoanalysis

PM

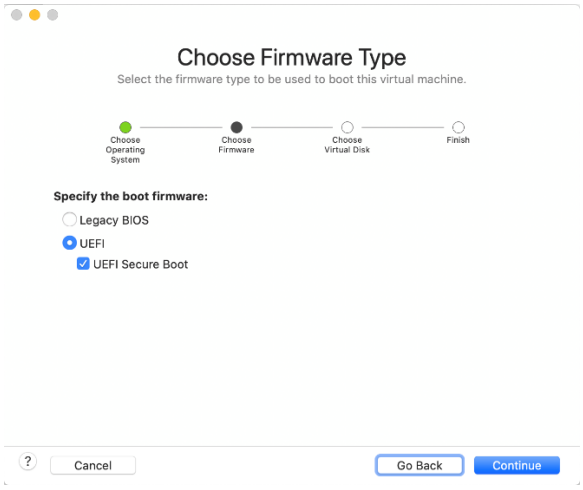
100 Points Total

DUE 2/16/2020 11:59:59

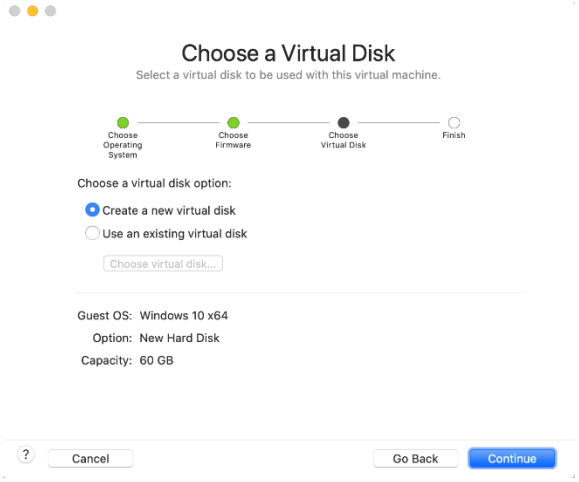
4. Under “Choose Operating System.” Select Windows 10 x64, click continue




5. Under “Choose Firmware Type.” Make sure you select “UEFI & UEFI Secure Boot” then click continue




6. Under “Choose a Virtual Disk” Select “Create a new virtual disk” and click “Continue”



# LAB 2

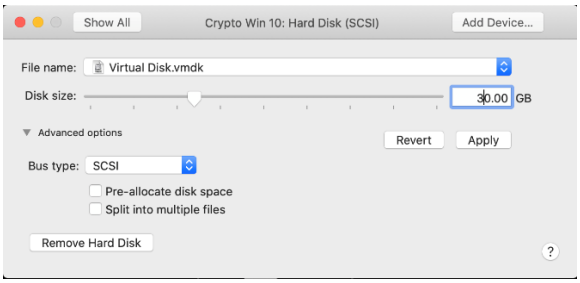
## Virtual Machine/Cryptoanalysis

PM

100 Points Total

DUE 2/16/2020 11:59:59

7. When setting up your virtual Hard Disk, make sure it is set to 30GB and “Split into multiple files” is not checked. Also depending on how much memory your computer currently has; you should consider giving your virtual machine at least 8GB.




8. The following step is depending on your current laptop hardware. Depending on how much memory your computer currently has; you should consider giving your virtual machine at least 8GB.


9. Under CD/DVD (SATA), make sure “Connect CD/DVD Drive” is checked and you have mounted your Windows 10 Educational. Version .ISO


10. Boot your Windows VM. Your screen should look something like this.

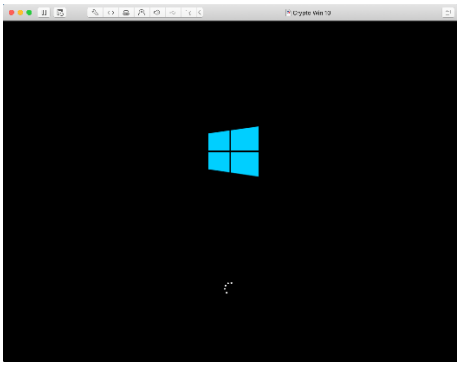
# LAB 2

## Virtual Machine/Cryptoanalysis

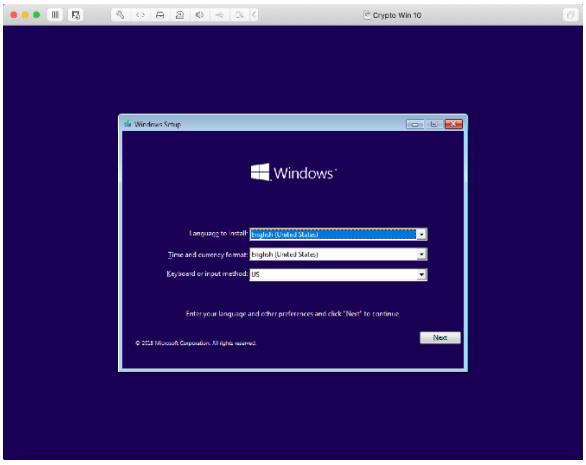
PM

100 Points Total

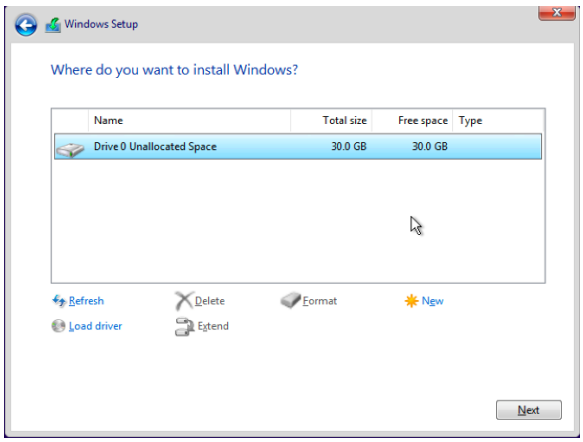
DUE 2/16/2020 11:59:59



11. On the next screen you would be asked to enter your License Key. Enter your License Key and continue.
12. On the following screen leverage defaults and click “Next”




13. On the next screen, click “Install Now.” Then Select “Custom Installation” and you should see a screen like this. Click “Next”



# LAB 2

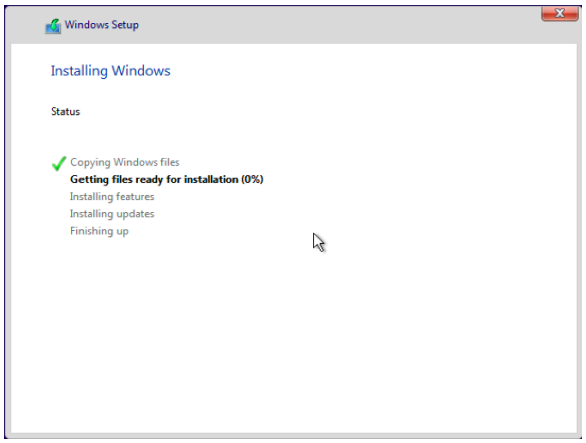
Virtual Machine/Cryptoanalysis

PM

100 Points Total

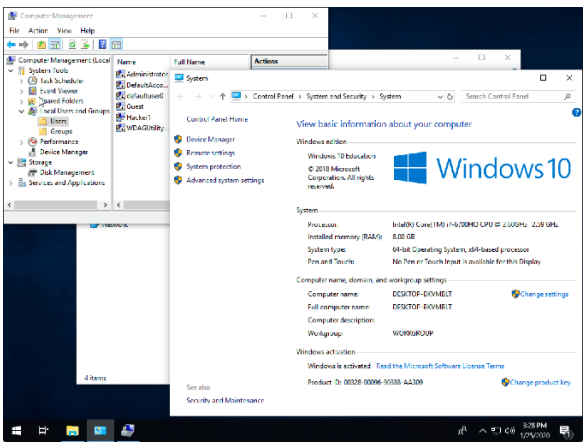
DUE 2/16/2020 11:59:59

14. Windows should start installing and you should see something like this.




15. Once Windows is done installing the files. You will need to go through the Basic setup.
    - Select a region → United States, click Next
    - Select keyboard layout → US, lick Next
    - Select a second keyboard → Optional, click Skip

16. Under the Account screen **make sure you do not sign in with any Microsoft account**, and instead you select at the bottom left of the screen "Domain join instead"
17. Type in your Last Name and click Next. Then type in a password and click Next. You will be asked to confirm your password.
18. Create your security questions, click Next
19. Optional, you can either Decline or Accept Cortana as your personal assistant
20. Optional Privacy Settings, click Accept
21. Once everything is done. You should be able to log in to Windows, please open the following boxes and take a screenshot. It should look like the following, make sure you paste it in your lab under Part I.



# LAB 2

Virtual Machine/Cryptoanalysis

PM

100 Points Total

DUE 2/16/2020 11:59:59

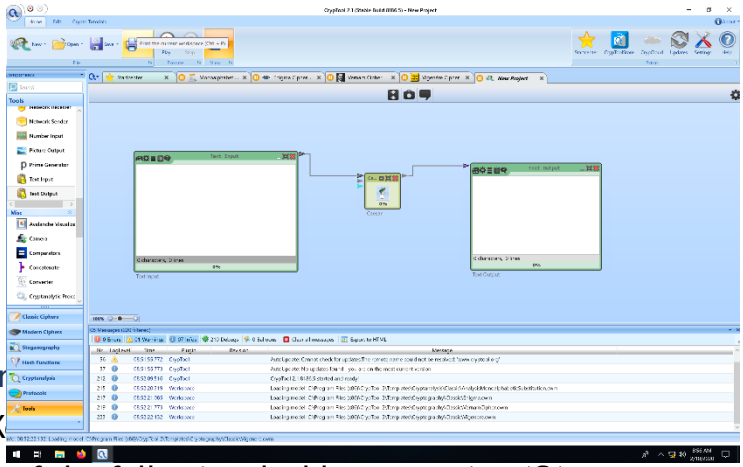
22. Now go online and install Firefox Web browser
23. Change your computer name to reflect your First Name Last Name
24. Take  a screenshot of this task and included it here

## Part II-A: Caesar's Cipher (20 pts)

Given the following Cesar's cipher, find out the plaintext which corresponds to the following ciphertext. To solve this problem, you will need to use CrypTool2 which you should have downloaded and installed in Part I.

Krz Jrrjoh Frxog Dftxluh Whvod Iru $1,500 Shu Vkduh Rq Lwv Zdb Wr $2 Wuloolrq Vwrfn

1. Open Cryptool2 → Click New → Select Workspace
2. On the left hand side, under Classic Ciphers → Select Caesar and drag it into your workspace
3. Now select tools on the left hand side and drag a Text Input/Output box
4. Connect them all to decrypt the given ciphertext, click the Play button
5. What is the plaintext?
6. Provide a screenshot of this task and workspace.



## Part II-B: Caesar's Cipher

Assume we are given a K

1. What is the result of the following double encryption ($C_i$):

# LAB 2

Virtual Machine/Cryptoanalysis

DUE 2/16/2020 11:59:59 PM

100 Points Total

2. $C_i = E(K, E(K, M_i))$, where $M_i$ is an arbitrary plaintext element? Explain your answer.
3. How many encryption times will it take with key → K=2 before we start observing the same effects as in the previous example with (K=13)?

## Part III: Caesar's Cipher Frequency Analysis (25 pts)

In this portion of the lab you will compare the before and after histograms encryption. Describe and explain your observations of the two.

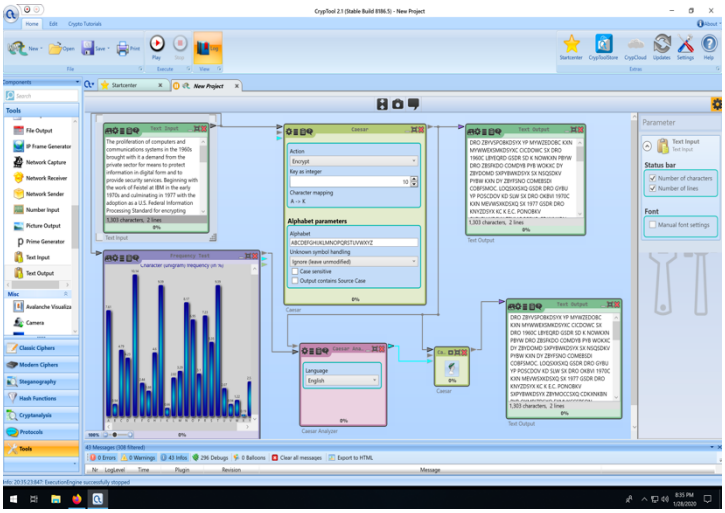
1. Create a new Workspace
2. On the left hand side, under Classic Ciphers → Select Caesar and drag it into your workspace
3. On the left hand side, under Cryptanalysis → Select Frequency Test and drag it into your workspace
4. Still under Cryptanalysis → Select Caesar Analyzer and drag it into your workspace
5. Now select tools on the left hand side and drag a Text Input/Output box as needed
6. Connect them all to encrypt/decrypt the given ciphertext, click the Play button
7. Use the following Text for this task:

**The United States Department of Justice today announced charges against 4 Chinese military hackers who were allegedly behind the Equifax data breach that exposed the personal and financial data of nearly 150 million Americans. In a joint press conference held today with the Attorney General William Barr and FBI Deputy Director David Bowdich, the DoJ officials labeled the state-sponsored hacking campaign as the largest hacking case ever uncovered of this type. The four accused, Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei, have also been indicted for their involvement in hacking and stealing trade secrets, intellectual property and confidential information from several other U.S. businesses in recent years.**

**"They used this access to conduct reconnaissance of Equifax's online dispute portal and to obtain login credentials that could be used to further navigate Equifax's network. The defendants spent several weeks running queries to identify Equifax's database structure and searching for sensitive, personally identifiable information within Equifax's system," the DoJ said.**
**"Once they accessed files of interest, the conspirators then stored the stolen information in temporary output files, compressed and divided the files, and ultimately were able to download and exfiltrate the data from Equifax's network to computers**

**outside the United States. In total, the attackers ran approximately 9,000 queries on Equifax's system, obtaining names, birth dates, and social security numbers for nearly half of all American citizens."**

**"The defendants took steps to evade detection throughout the intrusion, as alleged in the indictment. They routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, used encrypted communication channels within Equifax's network to blend in with normal network activity, and deleted compressed files and wiped log files on a daily basis in an effort to eliminate records of their activity."**



8. Provide a screenshot for this task which includes the histogram for the plaintext and for the encrypted text.
9. Explain your observations (Note: One sentence is not enough)

## Part IV: Monoalphabetic Substitution Cipher (25 pts)

Monoalphabethic cipher is similar to Caesar's cipher, in which the letters of the plaintext are replaced by a different letter of the alphabet. The difference is that the encryption key can be any permutation of the plaintext elements, which increases from 26 (Ceasar's Cipher) to 26!... However, this cipher is still vulnerable to the "relative frequency attacks"

1. Decrypt the following message which was encrypted using a monoalphabetic substitution

**MITKT AKT GXTK A IWFRKTR HGMTFMOAS CABL IAEQTKL EAF KWOF BGWK SOYT ZB IAXOFU AEETLL MG BGWK COYO FTMCGKQ MIAM'L ASLG EGFFTEMTR MG BGWK EGDHWMTKL, LDAKMHIGFTL, AFR GMITK LDAKM RTXOETL.**
**CITMITK OM'L AZGWM TVHSGOMOFU GHTKAMOFU LBLMTD AFR LGYMCAKT XWSFTKAZOSOMOTL GK DAFOHWSAMOFU FTMCGKQ MKAYYOE, TXTKB AMMAEQ KTSOTL GF MIT KTAEIAZOSOMB ZTMCTTF AF AMMAEQTK AFR MIT MAKUTMTR RTXOETL.**
**OF KTETFM BTAKL, CT IAXT LTTF IGC IWFRKTRL GY CORTSB WLTR LDAKM-ZWM-OFLTEWKT RTXOETL DART OM TALOTK YGK KTDGMT AMMAEQTKL MG LFTAQ OFMG EGFFTEMTR FTMCGKQL COMIGWM ZKTAQOFU COYO HALLCGKRL.**
**OF MIT SAMTLM KTLTAKEI LIAKTR COMI MIT IAEQTK FTCL, EITEQ HGOFM TVHTKML MGRAB KTXTASTR A FTC IOUI-LTXTKOMB XWSFTKAZOSOMB AYYTEMOFU HIOSOHL IWT LDAKM SOUIM ZWSZL MIAM EAF ZT TVHSGOMTR GXTK-MIT-AOK YKGD GXTK 100 DTMTKL ACAB MG UAOF TFMKB OFMG A MAKUTMTR COYO FTMCGKQ.**
**MIT WFRTKSBOFU IOUI-LTXTKOMB XWSFTKAZOSOMB, MKAEQTR AL EXT-2020-6007, KTLORTL OF MIT CAB HIOSOHL ODHSTDTFMTR MIT NOUZTT EGDDWFOEAMOGF HKGMGEGS OF OML LDAKM SOUIM ZWSZ, STAROFU MG A ITAH-ZALTR ZWYYTK GXTKYSGC OLLWT.**

# LAB 2

## Virtual Machine/Cryptoanalysis

DUE 2/16/2020 11:59:59 PM

100 Points Total

**NOUZTT OL A CORTSB WLTR COKTSTLL MTEIFGSGUB RTLOUFTR MG STM TAEI RTXOET EGDDWFOEAMT COMI AFB GMITK RTXOET GF MIT FTMCGKQ. MIT HKGMGEGS IAL ZTTF ZWOSM OFMG MTFL GY DOSSOGFL GY RTXOETL CGKSRCORT, OFESWROFU ADANGF TEIG, LADLWFU LDAKMMIOFUL, ZTSQOF TDG AFR DGKT.**

**"MIKGWUI MIOL TVHSGOMAMOGF, A MIKTAM AEMGK EAF OFYOSMKAMT A IGDT GK GYYOET'L EGDHWMTK FTMCGKQ GXTK-MIT-AOK, LHKTAROFU KAFLGDCAKT GK LHBCAKT, ZB WLOFU FGMIOFU ZWM A SAHMGH AFR AF AFMTFFA YKGD GXTK 100 DTMTKL," MIT EITEQ HGOFM KTLTAKEITKL MGSR MIT IAEQTK FTCL.**

**EITEQ HGOFM ASLG EGFYOKDTR MIAM MIT ZWYYTK GXTKYSGC IAHHTFL GF A EGDHGFTFM EASSTR MIT "ZKORUT" MIAM AEETHML KTDGMT EGDDAFRL LTFM MG MIT ZWSZ GXTK NOUZTT HKGMGEGS YKGD GMITK RTXOETL SOQT A DGZOST AHH GK ASTVA IGDT ALLOLMAFM.**

2. Use the pre-built templates. Templates → Cryptoanalysis → Classical
3. Leave all of the settings as default.
4. Provide the plaintext
5. Provide the key
6. Provide a screenshot of this task.