Overview

In this lab, students will learn about the importance of Cryptanalysis and how the implementation of mix characters can be a make it or break it in security. Students will also be 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.

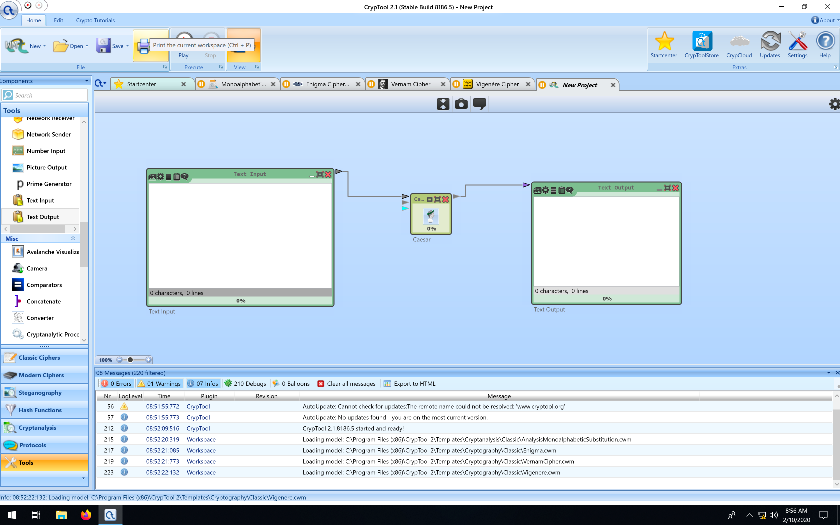
Note: For each question asked, label your answer with the part, followed by the instruction. For example, your response to a question posed in Part 1, instruction 1, should be labeled as **I-1:**

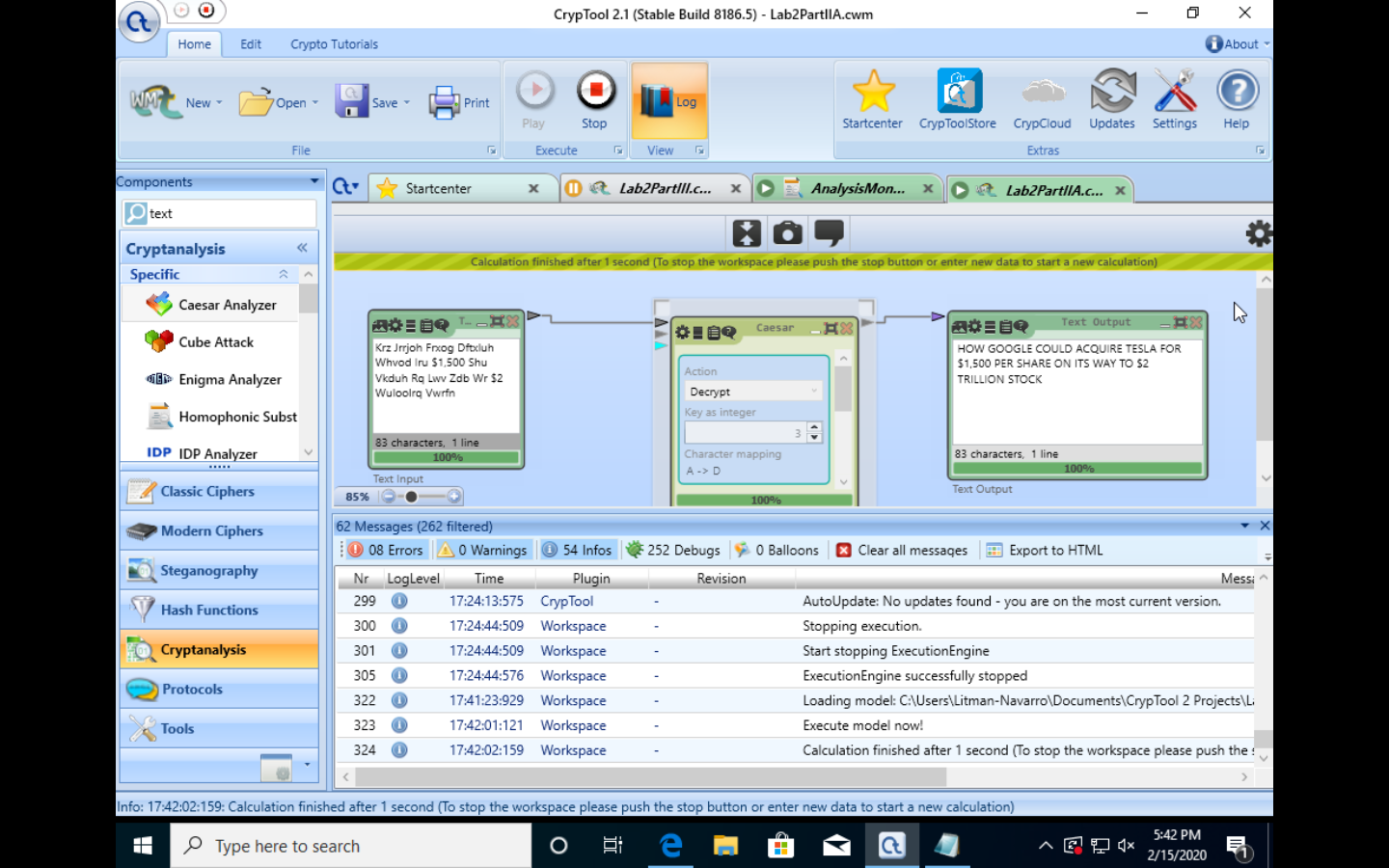
## Part II-A: Caesar’s Cipher (20 pts)

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?
   1. Plaintext: “How Google Could Acquire Tesla For $1,500 Per Share On Its Way to $2 Trillion Stock”
6. Provide a screenshot of this task and workspace.





### Part II-B: Caesar’s Cipher (20 pts)

Assume we are given a Key 🡪 K=13 as an encryption key in Caesar’s cipher.

1. What is the result of the following double encryption (Ci):
   1. Assuming an encryption key of k=13, taking an arbitrary string such as “EARTH” and encrypting with the Caesar’s Cipher using key k=13 would yield the string “RNEGU”. A second round of encryption would yield again the string “EARTH”.
2. Ci = E (K, E (K, Mi)), where Mi is an arbitrary plaintext element? Explain your answer.
   1. The result of the following double encryption C will be each letter upshifted by K elements in the alphabet, using modular arithmetic to circle back to the beginning of the alphabet when an element is shifted past the letter Z. An abstraction that might best be used to visualize this is perhaps a circle with 26 evenly spaced markings around it’s circumference and one mark outside the circle to indicate the current position, as is seen on some combination locks. Taking again as our encryption key k=13, we can begin by encrypting then first letter from our arbitrary message M, which in this we case we can set to M = “ant” for convenience and clarity, making our equation C = E(k=13, E(k=13, M=”ant”)). Rotating ‘a’ by 13 letters yields ‘n’, ‘n’ yields ‘a’, and ‘t’ yields the letter ‘g’, making our equation C = E(k=13, M=”nag”). Upon inspection we can see that a key of 13 simply switches each letter to the one halfway across the alphabet. Performing the second part of the calculation goes as follows: C = E(k=13, M=”nag”) = “ant”. Clearly by the nature of Caesar’s Cipher, a double encryption with a key of 13 brings us full circle around the alphabet to the original plaintext message, in effect decrypting it.
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)?
   1. When using an encryption key of k=2, it should require 13 consecutive encryptions to effectively decrypt the message, as seen in the earlier question when the encryption key k=13 was used.

## 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.**

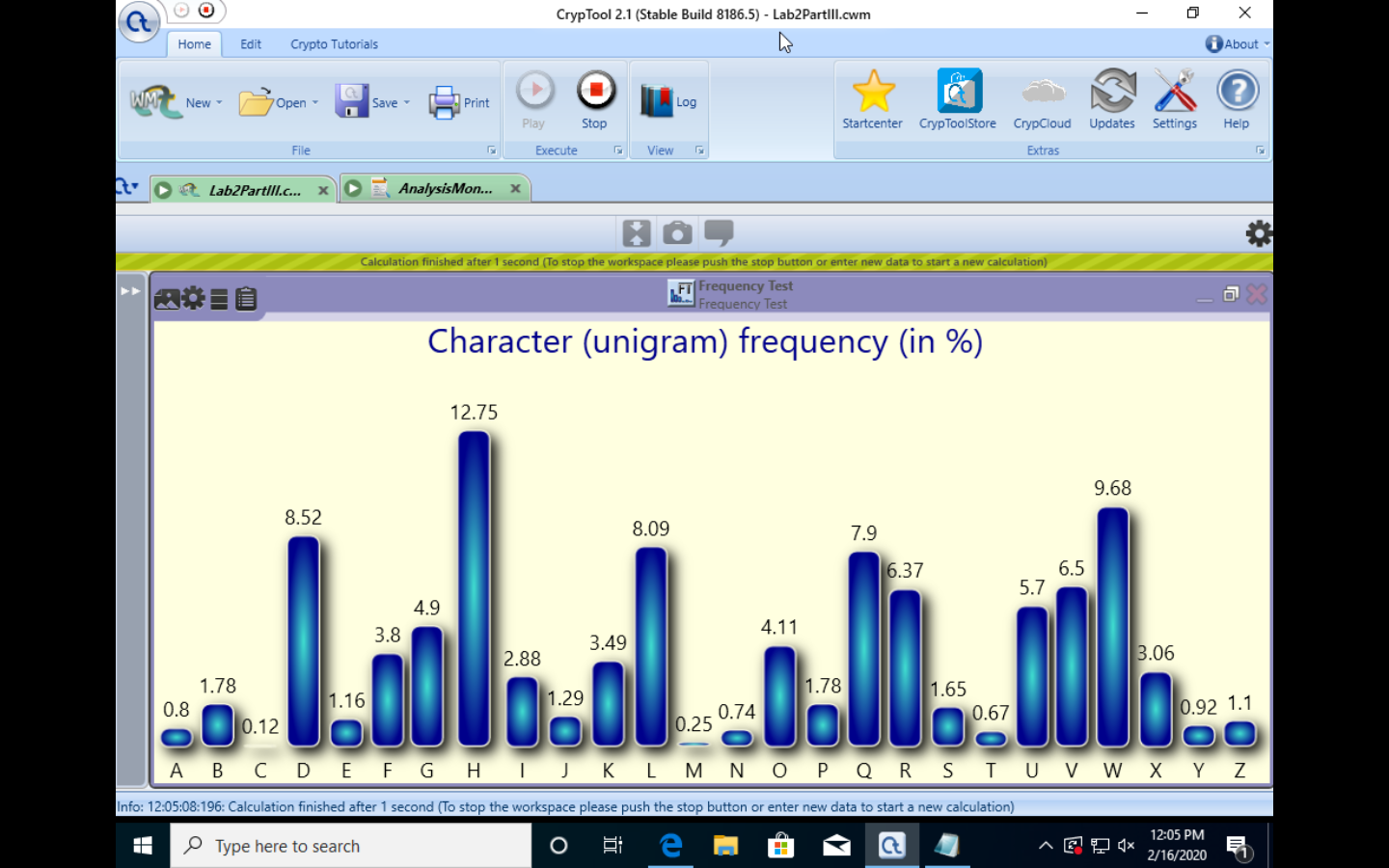
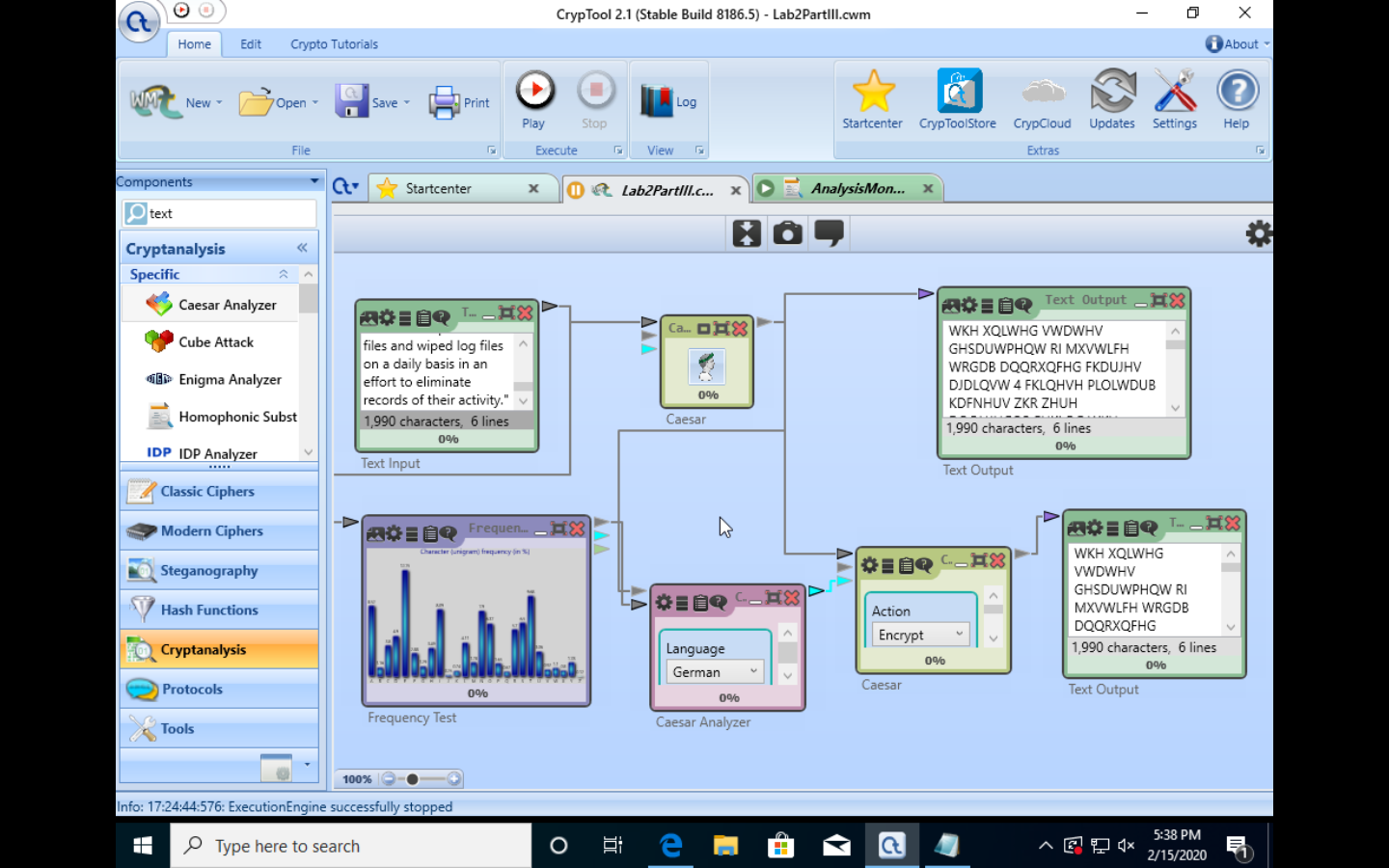
**"Once they accessed files of interest, the conspirators then stored the stolen information in temporary output files, compressed and divided the files, and ultimately were able to download and exfiltrate the data from Equifax's network to computers outside the United States. In total, the attackers 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."**

A screenshot of a computer

Description automatically generated

1. Provide a screenshot for this task which includes the histogram for the plaintext and for the encrypted text.



1. Explain your observations (Note: One sentence is not enough)
   1. Both the encrypted and plaintext behave exactly as we would expect English language messages to. That is to say that the relative frequencies of letters in the plaintext tend toward those vowels (namely ‘e’, which accounts for 12.75% of letters) that normally we might look for when in attempting to decrypt a Caesar’s cipher encrypted text. Consequently, after encrypting our plaintext and examining our histogram we can easily tell our key by finding the letter with the highest number of occurrences, ‘H’, and counting how many shifts it takes to get from ‘E’ to ‘H’. Clearly this number of shifts, 3, is our encryption key.

## 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.**

**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.**

1. Use the pre-built templates. Templates 🡪 Cryptoanalysis 🡪 Classical
2. Leave all of the settings as default.
3. Provide the plaintext
   1. Plaintext: THERE ARE OVER A HUNDRED POTENTIAL WAYS HACKERS CAN RUIN YOUR LIFE BY HAVING ACCESS TO YOUR WIFI NETWORK THATS ALSO CONNECTED TO YOUR COMPUTERSZ SMARTPHONESZ AND OTHER SMART DEVICESJ WHETHER ITS ABOUT EXPLOITING OPERATING SYSTEM AND SOFTWARE VULNERABILITIES OR MANIPULATING NETWORK TRAFFICZ EVERY ATTACK RELIES ON THE REACHABILITY BETWEEN AN ATTACKER AND THE TARGETED DEVICESJ IN RECENT YEARSZ WE HAVE SEEN HOW HUNDREDS OF WIDELY USED SMARTBUTINSECURE DEVICES MADE IT EASIER FOR REMOTE ATTACKERS TO SNEAK INTO CONNECTED NETWORKS WITHOUT BREAKING WIFI PASSWORDSJIN THE LATEST RESEARCH SHARED WITH THE HACKER NEWSZ CHECK POINT EXPERTS TODAY REVEALED A NEW HIGHSEVERITY VULNERABILITY AFFECTING PHILIPS HUE SMART LIGHT BULBS THAT CAN BE EXPLOITED OVERTHEAIR FROM OVER METERS AWAY TO GAIN ENTRY INTO A TARGETED WIFI NETWORKJ THE UNDERLYING HIGHSEVERITY VULNERABILITYZ TRACKED AS CVEZ RESIDES IN THE WAY PHILIPS IMPLEMENTED THE IGBEE COMMUNICATION PROTOCOL IN ITS SMART LIGHT BULBZ LEADING TO A HEAPBASED BUFFER OVERFLOW ISSUEJIGBEE IS A WIDELY USED WIRELESS TECHNOLOGY DESIGNED TO LET EACH DEVICE COMMUNICATE WITH ANY OTHER DEVICE ON THE NETWORKJ THE PROTOCOL HAS BEEN BUILT INTO TENS OF MILLIONS OF DEVICES WORLDWIDEZ INCLUDING AMAON ECHOZ SAMSUNG SMARTTHINGSZ BELKIN EMO AND MOREJ THROUGH THIS EXPLOITATIONZ A THREAT ACTOR CAN INFILTRATE A HOME OR OFFICES COMPUTER NETWORK OVERTHEAIRZ SPREADING RANSOMWARE OR SPYWAREZ BY USING NOTHING BUT A LAPTOP AND AN ANTENNA FROM OVER METERSZ THE CHECK POINT RESEARCHERS TOLD THE HACKER NEWSJ CHECK POINT ALSO CONFIRMED THAT THE BUFFER OVERFLOW HAPPENS ON A COMPONENT CALLED THE BRIDGE THAT ACCEPTS REMOTE COMMANDS SENT TO THE BULB OVER IGBEE PROTOCOL FROM OTHER DEVICES LIKE A MOBILE APP OR ALEXA HOME ASSISTANTJ
   2. Note: Clearly program struggled to comprehend characters like commas, periods, and dashes. If I had more free time this week to debug this, I would have attempted to, but a one-to-one correlation between punctuation marks and letters is clearly evident. For clarity I did not edit the plaintext from produced by the program, if I had though, the translation scheme would be that ‘J’ correlates to periods and ‘Z’ correlates to commas.
4. Provide the key
   1. Key: azertyuio.qsdfgh klmwxcvb,
   2. Note: I could not figure out how to manually edit the key, but I believe removing the ‘.’, ‘,’, and ‘ ‘ from the key would have fixed the errors in decryption.
5. Provide a screenshot of this task.

