**CS 177**

**Homework 1**

**Task 1:**

1. A hacker guesses Sandra’s CSIL password:
   1. Violation of confidentiality: the hacker (an unauthorized individual) is trying to get into confidential (private) information of Sandra (an authorized individual) that has been purposefully made unavailable to the hacker.
   2. Violation of data integrity: the hacker (an unauthorized individual), if guessed correctly, can now have access to Sandra’s files and changed them in a malicious way.
   3. Violation of source integrity: the hacker, if guessed correctly, can use Sandra’s CSIL account under Sandra’s identification; thus destroying the trustworthiness of the source.
   4. Violation of availability: If the hacker changes Sandra’s CSIL password after successfully guessed her password, he can prevent Sandra (an authorized individual) from accessing it.
2. A thief steals Alice’s passport:
   1. Violation of confidentiality: Passport contains a lot of sensitive information that should not be accessible by an unauthorized individual. However, the thief could access this information in this case.
   2. Violation of source integrity: the thief can now use Alice’s identity via her passport to do illegal activities, thus ruining the source integrity (trustworthiness)
   3. Violation of availability: Alice (an authorized individual) now does not have access to her passport.
3. The FBI wiretaps the cell phone of a suspect in a criminal investigation:
   1. Violation of confidentiality: The FBI (unauthorized group to the phone call conversation) can now have access to any secret information that the suspect passes around on his/her phone during a conversation.
4. A virus encrypts the victim’s hard drive with a secret key, and a criminal asks for a ransom to decrypt it.:
   1. Violation of availability: The victim (an authorized individual) can no longer access his system.
5. Charlie finds an efficient method to break AES:
   1. Violation of confidentiality: By being able to break the AES, Charlie (an unauthorized individual) can now has access to sensitive and private information not meant for him to see in the first place.
6. Rhonda registers the domain name “StefanoTessaro.com” and refuses to let Stefano Tessaro buy or use the domain name.:
   1. Violation of data source: Because Rhonda is not Stefano Tessaro; thus any action from the side StefanoTessaro.com is inherently misleading and untrustworthy.
7. Jonah obtains Peter’s credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number:
   1. Violation of confidentiality: Credit card number are not meant to be accessible for unauthorized source (Jonah in this case); thus by being able to obtain it, Jonah has violated confidentiality.
   2. Violation of source integrity: Jonah now can use Peter’s credit card number to make order from the account; thus the source of the data transaction is untrustworthy.
   3. Violation of data integrity: By being able to cancel Peter’s credit card, Jonah has violated the data integrity in an unauthorized way (He’s not authorized to do such a thing on Peter’s data).
   4. Violation of availability: By replacing the Peter’s credit card with a new card, Peter (an authorized person) now no longer has access to his credit card, online payments, or banking information.
8. Lucas obtains Francines’s fingerprints.:
   1. Violation of source integrity: Lucas can now use Francines’s fingerprints to do malicious thing under Francines’s disguise, thus ruining the trustworthiness of the source (Francines’s fingerprints)

**Task 2:**

1. The APSB16-29 for Adobe Flash Player does contain vulnerabilities affecting Adobe Flash Player. The versions being affected are Adobe Flash Player Desktop Runtime version 22.0.0.211 and earlier on Windows and Macintosh platforms, Adobe Flash Player Extended Support Release version 18.0.0.366 and earlier on Windows and Macintosh platforms, Adobe Flash Player for Google Chrome version 22.0.0.211 and earlier on Windows, Macintosh, Linux and ChromeOS platforms, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 version 22.0.0.211 and earlier on Windows 10 and 8.1 platforms, and Adobe Flash Player for Linux version 11.2.202.632 and earlier on Linux platform.
2. The window of vulnerability for these vulnerabilities has been closed.
3. I chose vulnerability with CVE-2016-4271. Its CVSS v3 scores for this vulnerability is 7.5
4. This vulnerability exploited the information leak/disclosure weakness (CWE-200)

**Task 3a:**

Since there are only 26 ways of turning the plaintext into ciphertext. I just brute force all 26 possible ways of deciphering the ciphertext and read through each result to look for the correct one.

1. Input:

BUQHD VHEC OUIJUHTQO, BYLU VEH JETQO, XEFU VEH JECEHHEM. JXU YCFEHJQDJ

JXYDW YI DEJ JE IJEF GKUIJYEDYDW.

1. My Python Code: Submitted online
2. Output: Please look at REFERENCE #1 in the back.
   1. The plaintext has been highlighted in the reference. Here, I will only show the answer: LEARN FROM YESTERDAY, LIVE FOR TODAY, HOPE FOR TOMORROW. THE IMPORTANT THING IS NOT TO STOP QUESTIONING.

**Task 3b:**

First, I create a FourLetterWordFrequencyCounter, a ThreeLetterWordFrequencyCounter, and a CharacterFrequencyCounter Python scripts. Each script will count the frequency of each 4 letter word/3 letter word/character respectively in the ciphertext and order them in descending order.

1. The Code: Submitted online
2. The Output: For the full output of each script, please check the back REFERENCE #2. Here, I will only include the most important result of the counters.

For FourLetterWordFrequencyCounter:

Counter({'PQSP': 13, 'PJOE': 9, 'QTIT': 8, 'PQTI': 6, 'SPTG': 6, 'JCSP': 6, 'GTGJ': 6, 'CSPT': 6, 'GJCS': 6, 'TGJC': 6, … })

For ThreeLetterWordFrequencyCounter:

Counter({'PQT': 23, 'PQS': 15, 'QSP': 15, 'QTI': 13, 'TGJ': 12, …})

For CharacterFrequencyCounter:

Counter({'T': 165, 'P': 126, 'S': 102, 'O': 93, 'Q': 80, 'I': 79, 'E': 77, 'J': 68, 'G': 58, 'A': 44, 'Z': 42, 'C': 31, 'H': 28, 'X': 28, 'B': 27, 'U': 24, 'W': 21, 'K': 15, 'D': 14, 'F': 13, 'L': 10, 'M': 3, 'R': 1})

From the result shown above, here are a few conclusions that I can make. ‘T’ is the most popular character in our ciphertext: ‘E’ is the most popular character in English language; ‘P’ is the second most popular character in ciphertext: ‘E’ is the second most popular character in English. ‘S’ is the third most popular character in ciphertext: ‘A’ is the third most popular character in English. Moreover, we see that ‘PQT’ is the most popular 3-letter word in the ciphertext; and ‘THE’ is the most popular 3-letter word in the English language. Additionally, we see that, ‘PQSP’ is the most popular 4-letter word in the ciphertext; and “THAT” is the most popular 4-letter word in English. Thus, we can safely assume that the following mapping must from ciphertext to plantext must be correct: ‘P’ => ‘T’; ‘T’=>’E’; ‘Q’=>’H’; ‘S’=>’A’. That was our first conclusion.

Next up, we check out ‘PJOE’. With the current mapping, we can turn ‘QTIT into ‘HE\_E’ and ‘PQTI' int ‘THE\_’. These two clues and the fact that the most popular 5-letter English word is ‘THERE’ give me a strong conviction that I must be ‘R’. Thus, ‘I’ => ‘R’. This is our second conclusion.

At this point, I decided to based ‘O’ being the fourth most popular in our ciphertext and also the fourth most popular word in the English language. I will map ‘O’=>’O’. This is my third conclusion.

Interestingly, when this mapping happens, our deciphered text becomes: (upper case is deciphered, lower case is ciphered)

bOwRacOREAegaEuEelEARaAhOOwRbATHERadROwhHTbORTHOeTHjacOeTjeEeTAeExeATjOecOecEjuEgjezjdERTlAeggEgjcATEgTOTHEkROkOajTjOeTHATAzzfEeAREcREATEgErwAzeOxxEAREEehAhEgjeAhREATcjujzxARTEaTjehxHETHERTHATeATjOeORAeleATjOeaOcOecEjuEgAegaOgEgjcATEgcAezOehEegwRExEAREfETOeAhREATdATTzEbjEzgObTHATxARxEHAuEcOfETOgEgjcATEAkORTjOeObTHATbjEzgAaAbjeAzREaTjehkzAcEbORTHOaExHOHEREhAuETHEjRzjuEaTHATTHATeATjOefjhHTzjuEjTjaAzTOhETHERbjTTjehAegkROkERTHATxEaHOwzggOTHjadwTjeAzARhERaEeaExEcAeeOTgEgjcATExEcAeeOTcOeaEcRATExEcAeeOTHAzzOxTHjahROwegTHEdRAuEfEezjujehAeggEAgxHOaTRwhhzEgHEREHAuEcOeaEcRATEgjTbARAdOuEOwRkOORkOxERTOAggORgETRAcTTHExORzgxjzzzjTTzEeOTEeORzOehREfEfdERxHATxEaAlHEREdwTjTcAeeEuERbORhETxHATTHElgjgHEREjTjabORwaTHEzjujehRATHERTOdEgEgjcATEgHERETOTHEwebjejaHEgxORmxHjcHTHElxHObOwhHTHEREHAuETHwabARaOeOdzlAguAecEgjTjaRATHERbORwaTOdEHEREgEgjcATEgTOTHEhREATTAamREfAjejehdEbOREwaTHATbROfTHEaEHOeOREggEAgxETAmEjecREAaEggEuOTjOeTOTHATcAwaEbORxHjcHTHElhAuETHEzAaTbwzzfEAawREObgEuOTjOeTHATxEHEREHjhHzlREaOzuETHATTHEaEgEAgaHAzzeOTHAuEgjEgjeuAjeTHATTHjaeATjOewegERhOgaHAzzHAuEAeExdjRTHObbREEgOfAegTHAThOuERefEeTObTHEkEOkzEdlTHEkEOkzEbORTHEkEOkzEaHAzzeOTkERjaHbROfTHEEARTH

Noticed the highlighted word, I recognized that word as “TOGETHER”. So ‘H’=>’G’. This is our fourth conclusion. This results in our ciphered text becoming:

bOwRacOREAegaEuEelEARaAGOOwRbATHERadROwGHTbORTHOeTHjacOeTjeEeTAeExeATjOecOecEjuEgjezjdERTlAeggEgjcATEgTOTHEkROkOajTjOeTHATAzzfEeAREcREATEgErwAzeOxxEAREEeGAGEgjeAGREATcjujzxARTEaTjeGxHETHERTHATeATjOeORAeleATjOeaOcOecEjuEgAegaOgEgjcATEgcAezOeGEegwRExEAREfETOeAGREATdATTzEbjEzgObTHATxARxEHAuEcOfETOgEgjcATEAkORTjOeObTHATbjEzgAaAbjeAzREaTjeGkzAcEbORTHOaExHOHEREGAuETHEjRzjuEaTHATTHATeATjOefjGHTzjuEjTjaAzTOGETHERbjTTjeGAegkROkERTHATxEaHOwzggOTHjadwTjeAzARGERaEeaExEcAeeOTgEgjcATExEcAeeOTcOeaEcRATExEcAeeOTHAzzOxTHjaGROwegTHEdRAuEfEezjujeGAeggEAgxHOaTRwGGzEgHEREHAuEcOeaEcRATEgjTbARAdOuEOwRkOORkOxERTOAggORgETRAcTTHExORzgxjzzzjTTzEeOTEeORzOeGREfEfdERxHATxEaAlHEREdwTjTcAeeEuERbORGETxHATTHElgjgHEREjTjabORwaTHEzjujeGRATHERTOdEgEgjcATEgHERETOTHEwebjejaHEgxORmxHjcHTHElxHObOwGHTHEREHAuETHwabARaOeOdzlAguAecEgjTjaRATHERbORwaTOdEHEREgEgjcATEgTOTHEGREATTAamREfAjejeGdEbOREwaTHATbROfTHEaEHOeOREggEAgxETAmEjecREAaEggEuOTjOeTOTHATcAwaEbORxHjcHTHElGAuETHEzAaTbwzzfEAawREObgEuOTjOeTHATxEHEREHjGHzlREaOzuETHATTHEaEgEAgaHAzzeOTHAuEgjEgjeuAjeTHATTHjaeATjOewegERGOgaHAzzHAuEAeExdjRTHObbREEgOfAegTHATGOuERefEeTObTHEkEOkzEdlTHEkEOkzEbORTHEkEOkzEaHAzzeOTkERjaHbROfTHEEARTH

Here, I noticed that the only letter that ‘W’ can be is ‘U’ so we would have ‘ROUGHT’, which usually included in the past form. Thus, ‘W’ => ‘U’. That’s my fifth conclusion. This results in:

bOURacOREAegaEuEelEARaAGOOURbATHERadROUGHTbORTHOeTHjacOeTjeEeTAeExeATjOecOecEjuEgjezjdERTlAeggEgjcATEgTOTHEkROkOajTjOeTHATAzzfEeAREcREATEgErUAzeOxxEAREEeGAGEgjeAGREATcjujzxARTEaTjeGxHETHERTHATeATjOeORAeleATjOeaOcOecEjuEgAegaOgEgjcATEgcAezOeGEegURExEAREfETOeAGREATdATTzEbjEzgObTHATxARxEHAuEcOfETOgEgjcATEAkORTjOeObTHATbjEzgAaAbjeAzREaTjeGkzAcEbORTHOaExHOHEREGAuETHEjRzjuEaTHATTHATeATjOefjGHTzjuEjTjaAzTOGETHERbjTTjeGAegkROkERTHATxEaHOUzggOTHjadUTjeAzARGERaEeaExEcAeeOTgEgjcATExEcAeeOTcOeaEcRATExEcAeeOTHAzzOxTHjaGROUegTHEdRAuEfEezjujeGAeggEAgxHOaTRUGGzEgHEREHAuEcOeaEcRATEgjTbARAdOuEOURkOORkOxERTOAggORgETRAcTTHExORzgxjzzzjTTzEeOTEeORzOeGREfEfdERxHATxEaAlHEREdUTjTcAeeEuERbORGETxHATTHElgjgHEREjTjabORUaTHEzjujeGRATHERTOdEgEgjcATEgHERETOTHEUebjejaHEgxORmxHjcHTHElxHObOUGHTHEREHAuETHUabARaOeOdzlAguAecEgjTjaRATHERbORUaTOdEHEREgEgjcATEgTOTHEGREATTAamREfAjejeGdEbOREUaTHATbROfTHEaEHOeOREggEAgxETAmEjecREAaEggEuOTjOeTOTHATcAUaEbORxHjcHTHElGAuETHEzAaTbUzzfEAaUREObgEuOTjOeTHATxEHEREHjGHzlREaOzuETHATTHEaEgEAgaHAzzeOTHAuEgjEgjeuAjeTHATTHjaeATjOeUegERGOgaHAzzHAuEAeExdjRTHObbREEgOfAegTHATGOuERefEeTObTHEkEOkzEdlTHEkEOkzEbORTHEkEOkzEaHAzzeOTkERjaHbROfTHEEARTH

This is the word “FORGET”. Thus, “B” => “F”. This is my sixth conclusion. This results in:

FOURacOREAegaEuEelEARaAGOOURFATHERadROUGHTFORTHOeTHjacOeTjeEeTAeExeATjOecOecEjuEgjezjdERTlAeggEgjcATEgTOTHEkROkOajTjOeTHATAzzfEeAREcREATEgErUAzeOxxEAREEeGAGEgjeAGREATcjujzxARTEaTjeGxHETHERTHATeATjOeORAeleATjOeaOcOecEjuEgAegaOgEgjcATEgcAezOeGEegURExEAREfETOeAGREATdATTzEFjEzgOFTHATxARxEHAuEcOfETOgEgjcATEAkORTjOeOFTHATFjEzgAaAFjeAzREaTjeGkzAcEFORTHOaExHOHEREGAuETHEjRzjuEaTHATTHATeATjOefjGHTzjuEjTjaAzTOGETHERFjTTjeGAegkROkERTHATxEaHOUzggOTHjadUTjeAzARGERaEeaExEcAeeOTgEgjcATExEcAeeOTcOeaEcRATExEcAeeOTHAzzOxTHjaGROUegTHEdRAuEfEezjujeGAeggEAgxHOaTRUGGzEgHEREHAuEcOeaEcRATEgjTFARAdOuEOURkOORkOxERTOAggORgETRAcTTHExORzgxjzzzjTTzEeOTEeORzOeGREfEfdERxHATxEaAlHEREdUTjTcAeeEuERFORGETxHATTHElgjgHEREjTjaFORUaTHEzjujeGRATHERTOdEgEgjcATEgHERETOTHEUeFjejaHEgxORmxHjcHTHElxHOFOUGHTHEREHAuETHUaFARaOeOdzlAguAecEgjTjaRATHERFORUaTOdEHEREgEgjcATEgTOTHEGREATTAamREfAjejeGdEFOREUaTHATFROfTHEaEHOeOREggEAgxETAmEjecREAaEggEuOTjOeTOTHATcAUaEFORxHjcHTHElGAuETHEzAaTFUzzfEAaUREOFgEuOTjOeTHATxEHEREHjGHzlREaOzuETHATTHEaEgEAgaHAzzeOTHAuEgjEgjeuAjeTHATTHjaeATjOeUegERGOgaHAzzHAuEAeExdjRTHOFFREEgOfAegTHATGOuERefEeTOFTHEkEOkzEdlTHEkEOkzEFORTHEkEOkzEaHAzzeOTkERjaHFROfTHEEARTH

The first highlight is “FOURSCOREANDSEVENYEARSAGO”. The second highlight is ‘NEVERFORGET’. Thus from this, I can map the following:

* ‘A’ => ‘S’
* ‘C’ => ‘C’
* ‘E’=>’N’
* ‘G’=>’D’
* ‘U’=>’V’
* ‘L’=>’Y’

This is my seventh conclusion. From here on, it’s obvious that the rest of the text is an excerpt from the Gettysburg Address by Lincoln. Thus, I just follow through the entire text and decipher the rest using a copy of the excerpt and achieve the rest of my mappings. They are:

* ‘X’=>’W’
* ‘D’=>’B’
* ‘Z’=>’L’
* ‘K’=>’P;
* ‘F’=>’M’
* ‘R’=>’Q’
* ‘M’=>’K’
* ‘J’=>’I’

These are my eighth conclusion. His mapping helps me write my decipher python script. I named it task3b\_exploit.py. The code for this script has been submitted online.

The final output is:

FOURSCOREANDSEVENYEARSAGOOURFATHERSBROUGHTFORTHONTHISCONTINENTANEWNATIONCONCEIVEDINLIBERTYANDDEDICATEDTOTHEPROPOSITIONTHATALLMENARECREATEDEQUALNOWWEAREENGAGEDINAGREATCIVILWARTESTINGWHETHERTHATNATIONORANYNATIONSOCONCEIVEDANDSODEDICATEDCANLONGENDUREWEAREMETONAGREATBATTLEFIELDOFTHATWARWEHAVECOMETODEDICATEAPORTIONOFTHATFIELDASAFINALRESTINGPLACEFORTHOSEWHOHEREGAVETHEIRLIVESTHATTHATNATIONMIGHTLIVEITISALTOGETHERFITTINGANDPROPERTHATWESHOULDDOTHISBUTINALARGERSENSEWECANNOTDEDICATEWECANNOTCONSECRATEWECANNOTHALLOWTHISGROUNDTHEBRAVEMENLIVINGANDDEADWHOSTRUGGLEDHEREHAVECONSECRATEDITFARABOVEOURPOORPOWERTOADDORDETRACTTHEWORLDWILLLITTLENOTENORLONGREMEMBERWHATWESAYHEREBUTITCANNEVERFORGETWHATTHEYDIDHEREITISFORUSTHELIVINGRATHERTOBEDEDICATEDHERETOTHEUNFINISHEDWORKWHICHTHEYWHOFOUGHTHEREHAVETHUSFARSONOBLYADVANCEDITISRATHERFORUSTOBEHEREDEDICATEDTOTHEGREATTASKREMAININGBEFOREUSTHATFROMTHESEHONOREDDEADWETAKEINCREASEDDEVOTIONTOTHATCAUSEFORWHICHTHEYGAVETHELASTFULLMEASUREOFDEVOTIONTHATWEHEREHIGHLYRESOLVETHATTHESEDEADSHALLNOTHAVEDIEDINVAINTHATTHISNATIONUNDERGODSHALLHAVEANEWBIRTHOFFREEDOMANDTHATGOVERNMENTOFTHEPEOPLEBYTHEPEOPLEFORTHEPEOPLESHALLNOTPERISHFROMTHEEARTH

**Task 4:**

Please see the attached yellow paper note.