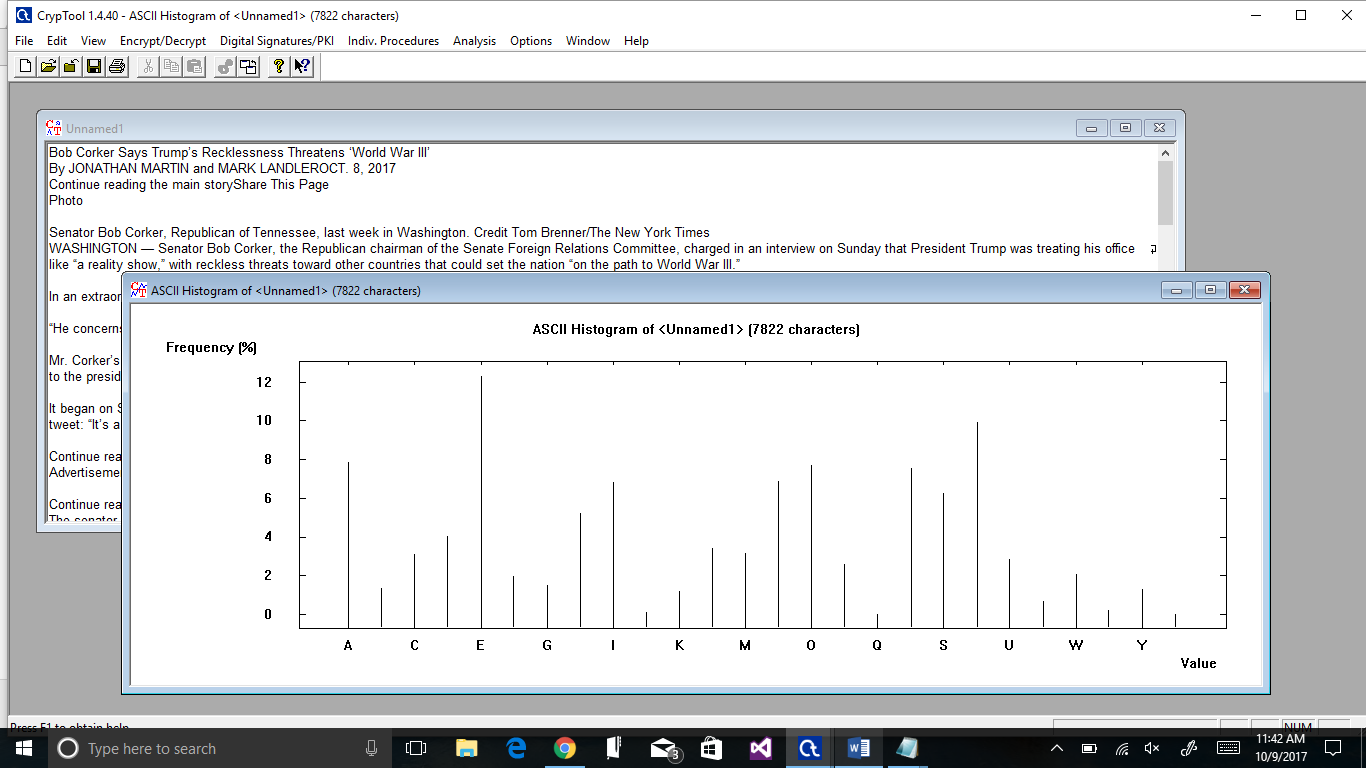
# Crypto Assignment

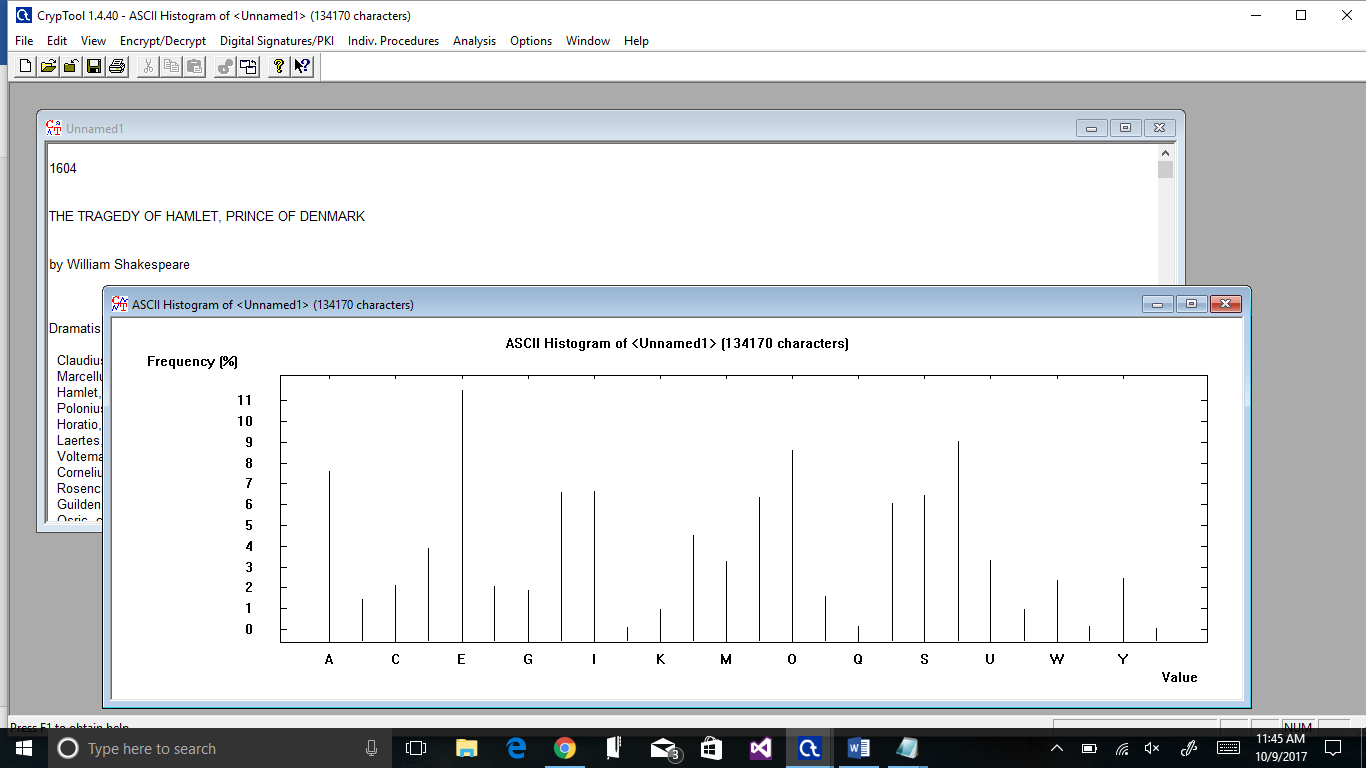
|  |
| --- |
| * This is an individual assignment, and is worth 20 points. * The due date and time is Tuesday, October 10 4:00 pm (section 01) / 7:00 pm (section 76). * You need to provide your answers to the “Crypto-Assignment-Outcome.docx” file. Change the file name following the naming convention suggested below. * Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Crypto-Assignment-ImG.docx). If you do not follow the convention, I will deduct 0.5. * DO NOT DISCUSS THIS ASSIGNMENT WITH OTHERS. |

## Task 1 (4 points)

Prepare the two English texts. One is supplied by the professor (Hamlet.txt). For the other, go to [www.nytimes.com](http://www.nytimes.com) and pick any article of your interest, and create a text file using the article.

* (1.5 points) Create a histogram for each text that display the relative frequency of letters in a graphical form. For this, go to Analysis > Tools for Analysis. Provide the two histograms in screenshots.

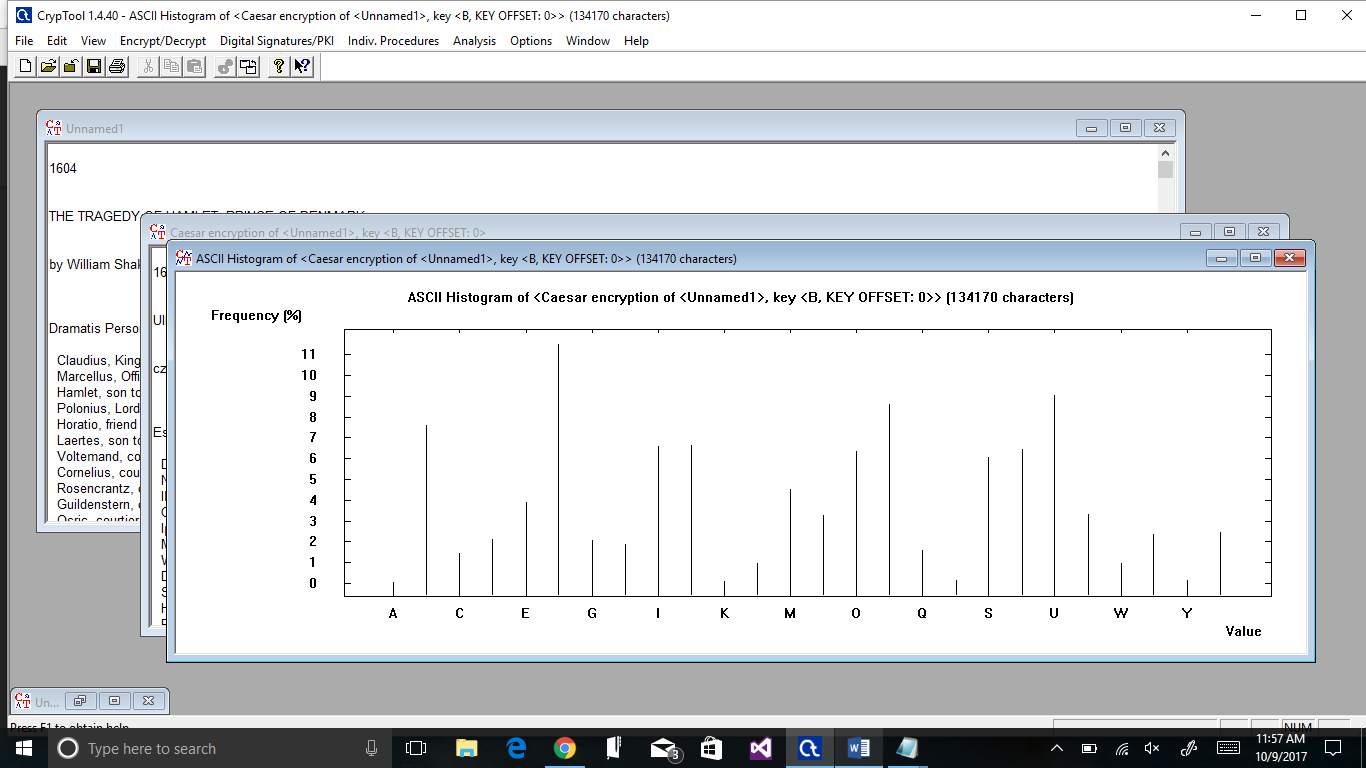




* (1.5 points) Do the two histograms depend significantly on the texts you have provided?
  + **No they are significantly similar based on the histograms.**
* (1 point) Calculate the entropy of each text. For this, Analysis > Tools for Analysis > Entropy. What would you conclude from the comparison of the entropies?
  + **Hamlet entropy was 4.19 and the New York Times article was 4.14 so I could conclude that the two text files had similar composition of letters and Hamlet had a slightly longer text than the NYT article.**

## Task 2 (4 points)

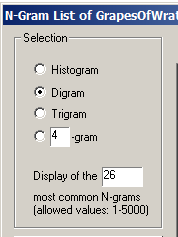
Encrypt the “Hamlet.txt” file using the Caesar cipher. Obtain the histogram of the encrypted text.



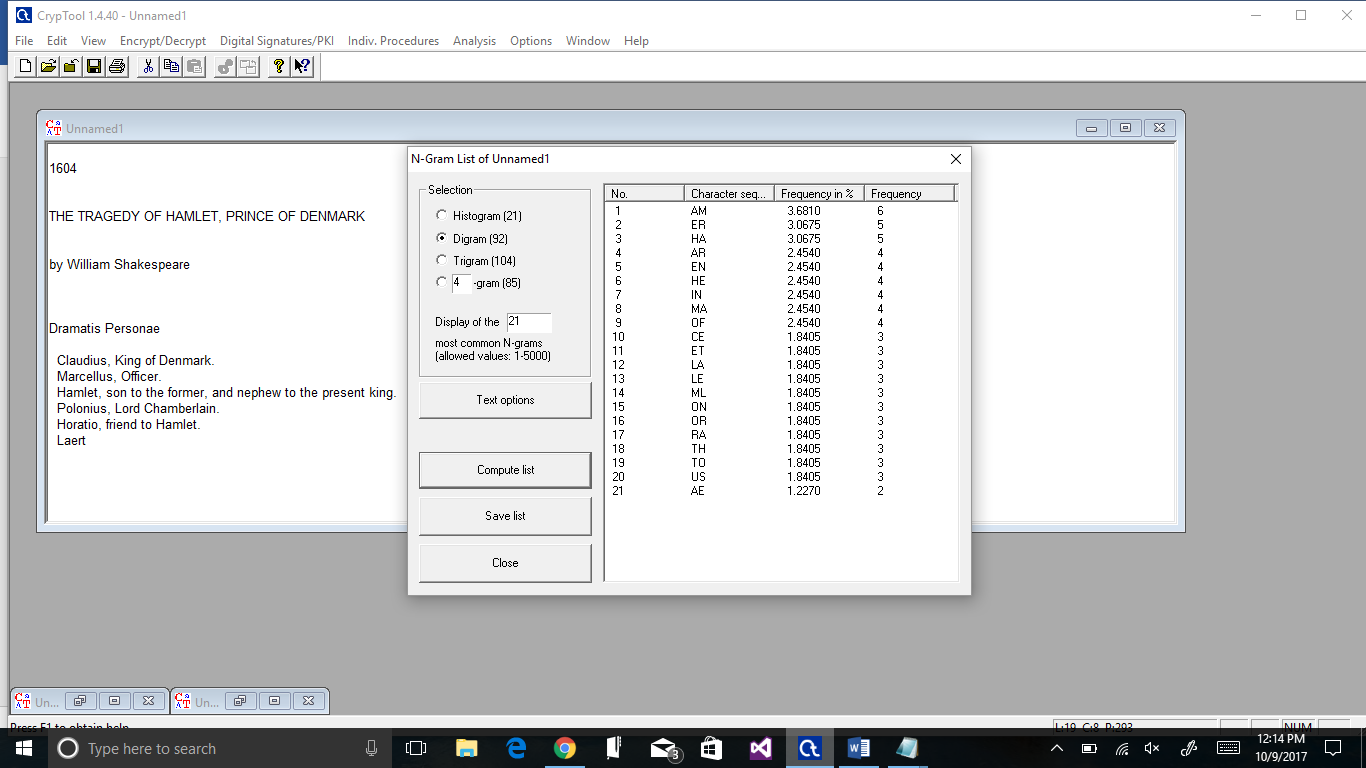
* (2 points) What are the characteristic features of the obtained distribution compared with the original text? Provide a screenshot to support your answer.
  + **The letters have been shifted to the right in their character frequencies.**
* (2 points) How would you apply the features you have discovered in cracking the key?
  + **By comparing the encrypted histogram with the original you can discover how many letters the text has been shifted and adjust them back accordingly to crack the key.**

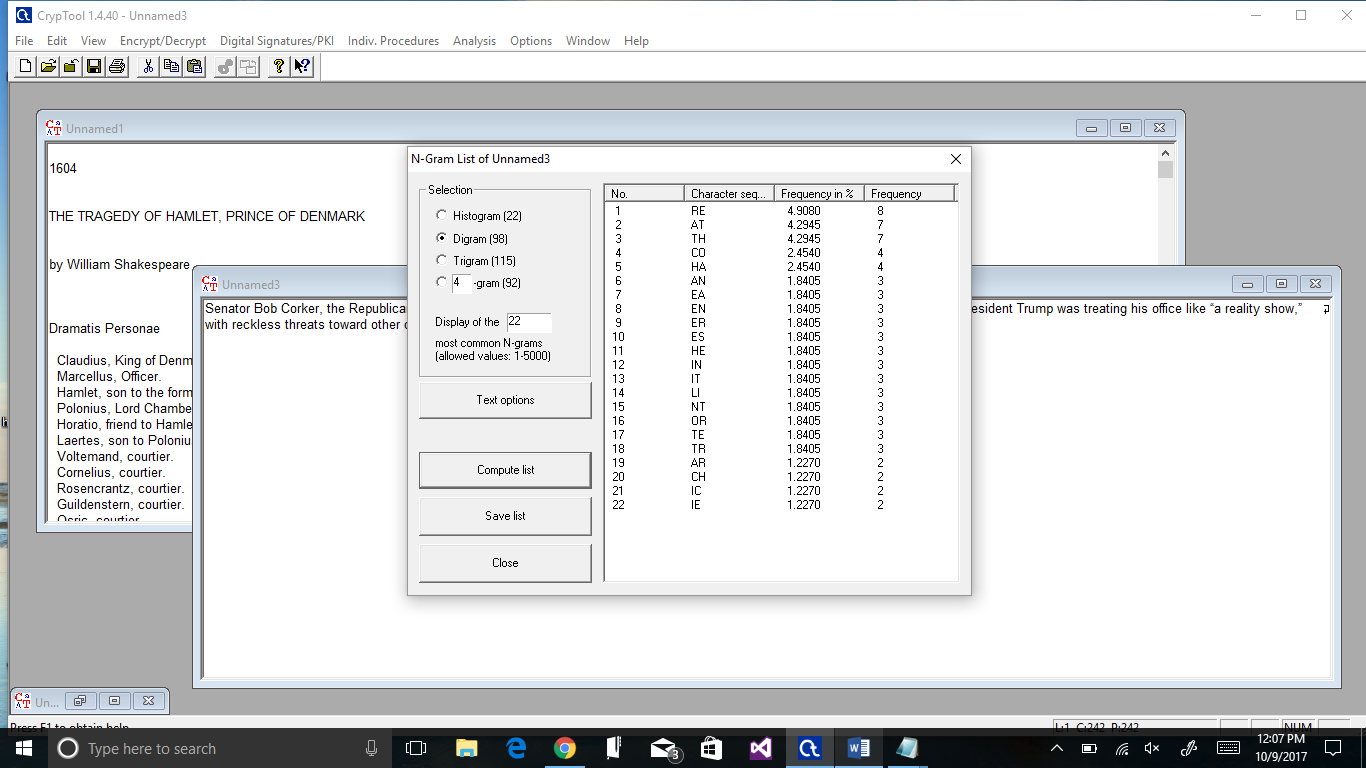
## Task 3 (4 points)

Using the texts in Task 1, create subtexts by taking a small subset from the two texts (e.g., the first 200 letters). And compute the frequency distribution of **digrams**. For this, go to Analysis > Tools for Analysis > N-Gram, and select Digram.



* (1.5 points for Hamlet.txt) Summarize your observation of the frequency distribution. Also, provide a screenshot of the frequency distribution.



* + **There were 22 character sequences in 200 characters with the most frequent being RE at 8 and the lowest being IE at 2.**
* (1.5 points for a NYT article) Summarize your observation of the frequency distribution. Also, provide a screenshot of the frequency distribution.
  + 

**The character sequence RE occurred most frequently inside the 200 characters, with AT and TH following behind. There are 22 character sequences with the lowest frequency being 2 and the highest being 8.**

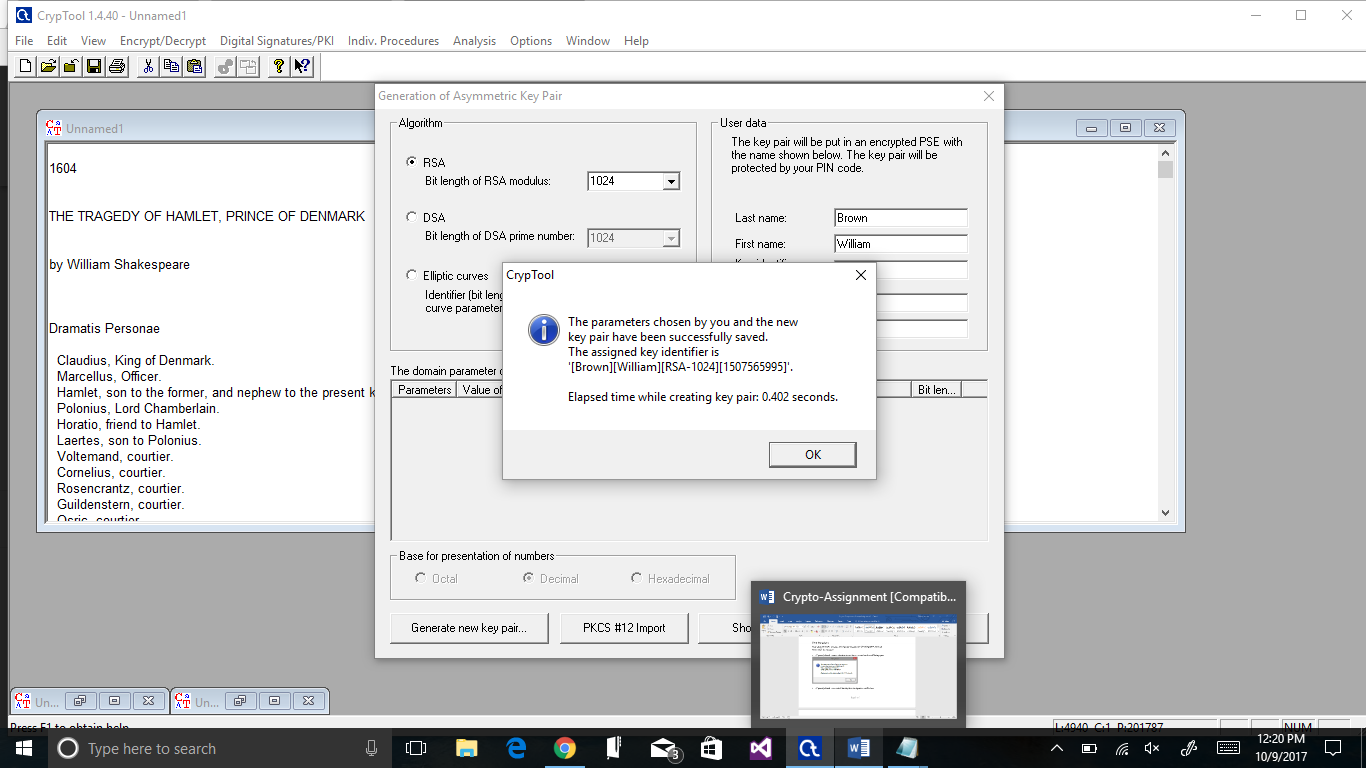
* (1 point) Compare and contrast the two frequency distributions.

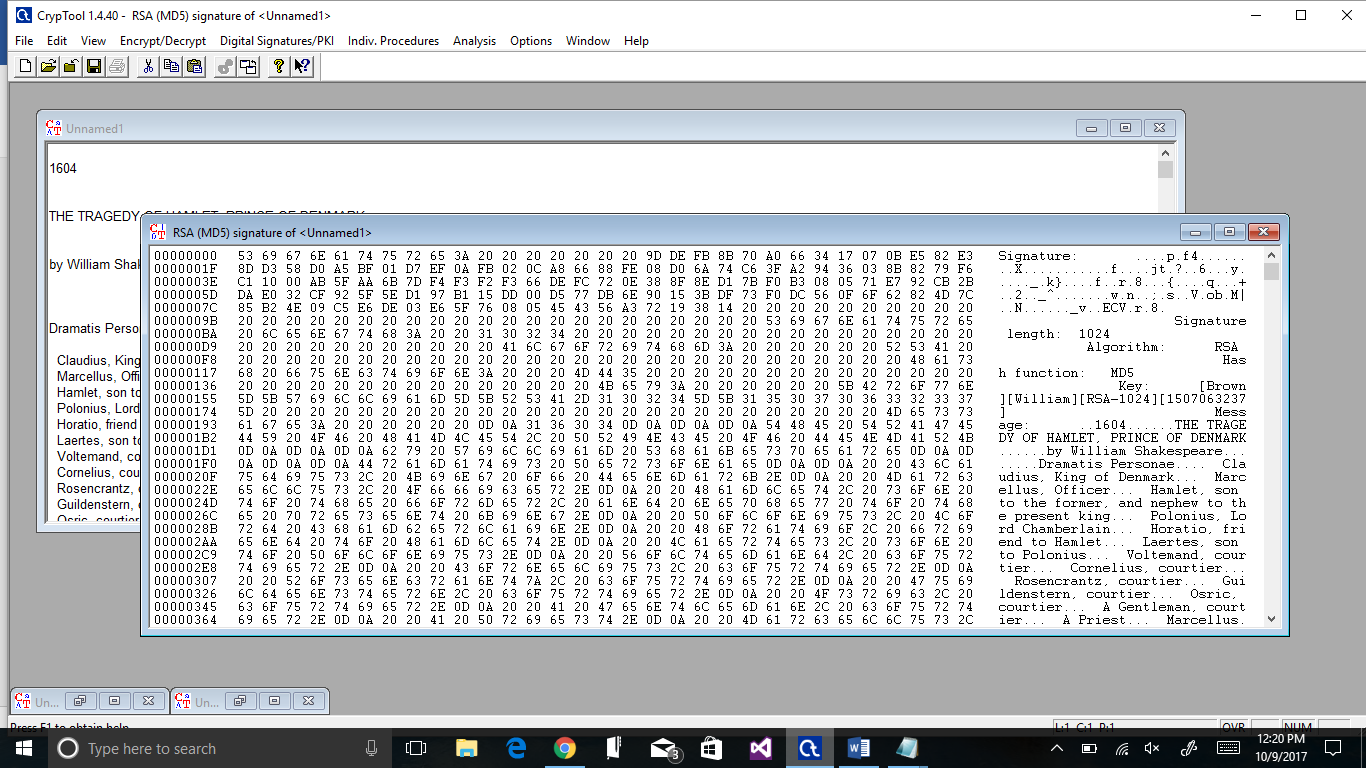
**The NYT article had more frequent combination of letters but they had around the same patterns of descending frequencies.**

## Task 4 (4 points)

First, generate a RSA key pair, and sign the “Hamlet.txt” file using MD5 and RSA.

Next, verify the signature.

* (2 points) Attach a screen shot that shows the successful creation of the key pair. 
* (2 points) Attach a screenshot that displays the signature verification.



## Task 5 (4 points)

Find the two ciphertexts of *the same* message below encrypted using one of the two classical ciphers available in CrypTool: Caesar and Vigenere. Do your best to match each ciphertext with a cipher that could have been used to obtain the given ciphertext.

* For Vigenere, you need to try different key sizes for the key.
* Do not discuss this task with anyone.
* (2 points) List the cipher and the key for Ciphertext 1.

**Derived Key: RRRRR, cipher is Vigenere, Hamlet’s to be or not to be**

* (2 points) List the cipher and the key for Ciphertext 2.

**Derived Key: KINGQUEEN cipher is Vigenere, Hamlet’s To be or not to be**

|  |  |
| --- | --- |
| **No** | **Cyphertext** |
| Ciphertext 1 | Yrd. Kf sv, fi efk kf sv- kyrk zj kyv hlvjkzfe:  Nyvkyvi 'kzj efscvi ze kyv dzeu kf jlwwvi  Kyv jczexj reu riifnj fw flkirxvflj wfiklev  Fi kf krbv ridj rxrzejk r jvr fw kiflscvj,  Reu sp fggfjzex veu kyvd. Kf uzv- kf jcvvg-  Ef dfiv; reu sp r jcvvg kf jrp nv veu  Kyv yvrikrtyv, reu kyv kyfljreu erklirc jyftbj  Kyrk wcvjy zj yvzi kf. 'Kzj r tfejlddrkzfe  Uvmflkcp kf sv nzjy'u. Kf uzv- kf jcvvg.  Kf jcvvg- gvityretv kf uivrd: rp, kyviv'j kyv ils!  Wfi ze kyrk jcvvg fw uvrky nyrk uivrdj drp tfdv  Nyve nv yrmv jylwwcvu fww kyzj dfikrc tfzc,  Dljk xzmv lj grljv. Kyviv'j kyv ivjgvtk  Kyrk drbvj trcrdzkp fw jf cfex czwv. |
| Ciphertext 2 | Riz. Ze vi, se xwg ze vi- xukb vy jbi uhoagoeh:  Alrdprx 'jcw rbltrx yh xlr wqaj ji wyspme  Zxy wpvxof gdx eveyef uv iyxekorukm jsedcak  El xs gksr ghgw etkqayj u win yn gxeofprc,  Iaj rs stcyavtw yrh grmz. Ze xmi- gy aykuj-  Rs zyzr; gdx fc n ctrkf ns wni er kdx  Xlr rmnxjuglr, kvq zxy xlbeantt hexhbiy yxigof  Dpnz vfiwu sa ukyl xs. 'Gsa n iehwyzwigoeh  Hiiycgro ns fr gqfn't. Ns hvo- bb ybyit.  Gy aykuj- tiempntsy xs qbmns: qs, xlrbm'f zxy vyo!  Pwe od nleg ctrkf ij hrkbu cxux heoizy cuc gbwm  Jnuh ai ukdr yxojjyol blv nlmf wwezqf gsvv,  Uhyj amzr ea cgkmi. Xuozr'y jbi vrcxrij  Nleg wixki wepnwqge ez ws yyvt ryzi. |