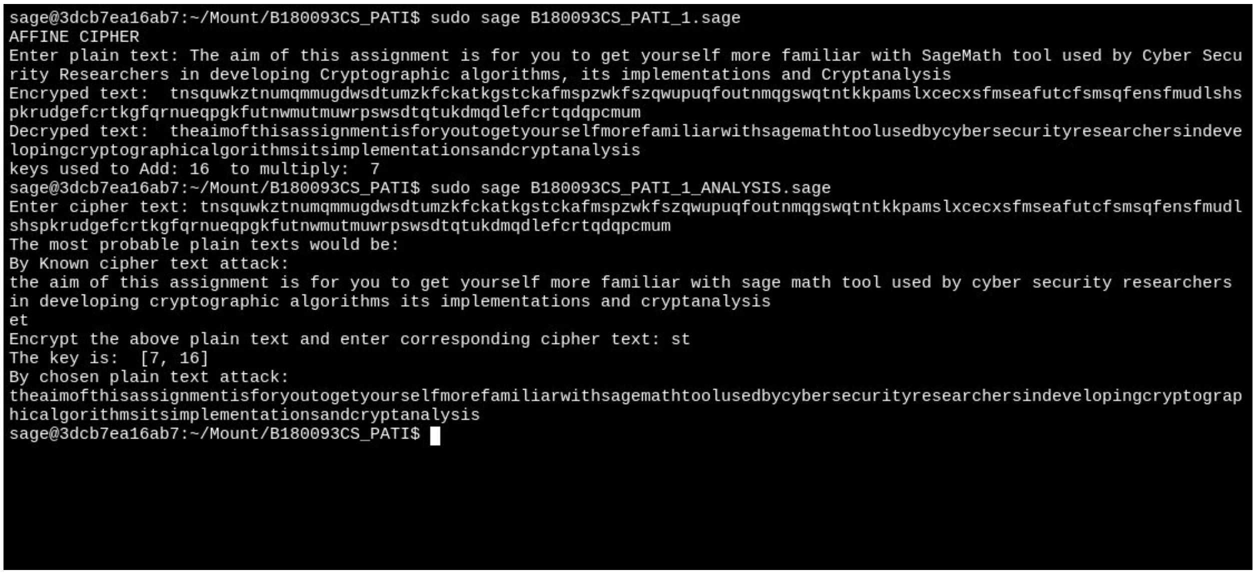
CS4021 - NUMBER THEORY AND CRYPTOGRAPHY

Note points and Screenshots

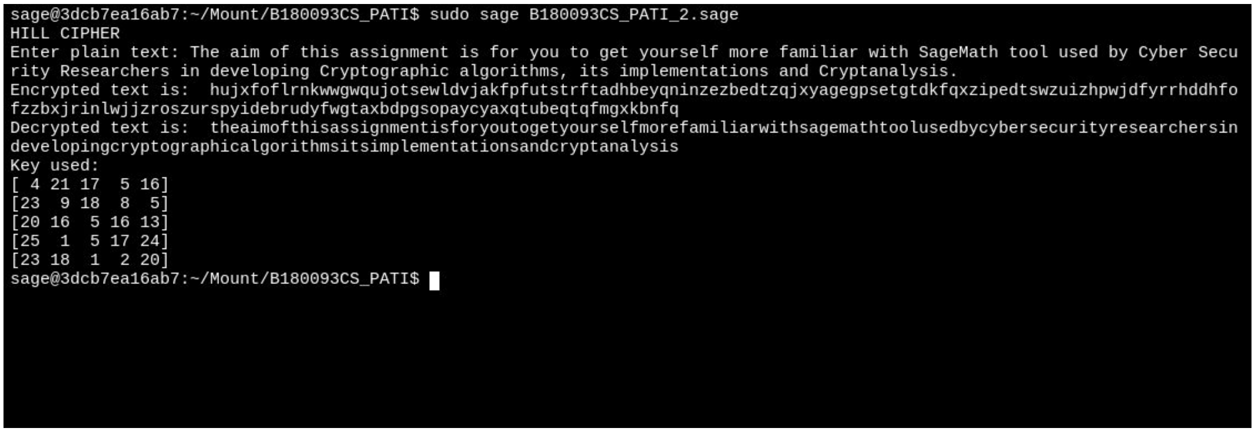
Pati Chandana
B180093CS

- All sage codes should be run using the “sage filename” command.
- Each cipher technique’s analysis is coded in separate files which have B180093CS_PATI_QNO.sage name.
- Encryption decryption functions are implemented in the same file, B180093CS_PATI_QNO.sage is the file name for each.
- Each code, where each cipher technique is implemented asks for plain text only, the code automatically generates the necessary key randomly and uses it to encrypt the user entered plain text and passes that encrypted text and key to decrypt the same. This is just to avoid the conditions in some, where encryption and decryption works for only certain key ranges.
- In case, one wants to encrypt or decrypt with their own keys, comment the random key generator code lines written.
- All the functions run user friendly, by printing necessary messages for the user to understand well.
- While encryption, all the non-alphabetic characters i.e. special characters and numbers would be removed from the user entered plain text and then would be encrypted. Therefore, users can’t witness such characters in the decrypted or encrypted text in any cipher methods, implemented here.
- Each cipher technique implemented sage file has two functions primarily “ciphermethodname_encryption” and “ciphermethodname_decryption” which take plain text and keys, cipher text and keys, to return encrypted and decrypted texts respectively.

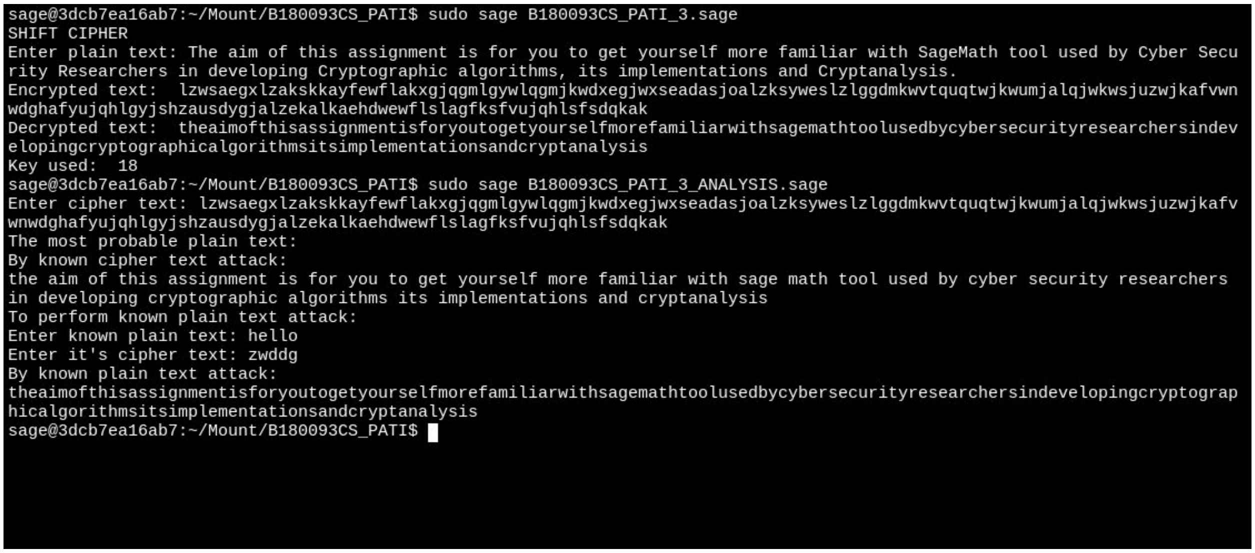
SCREENSHOTS:



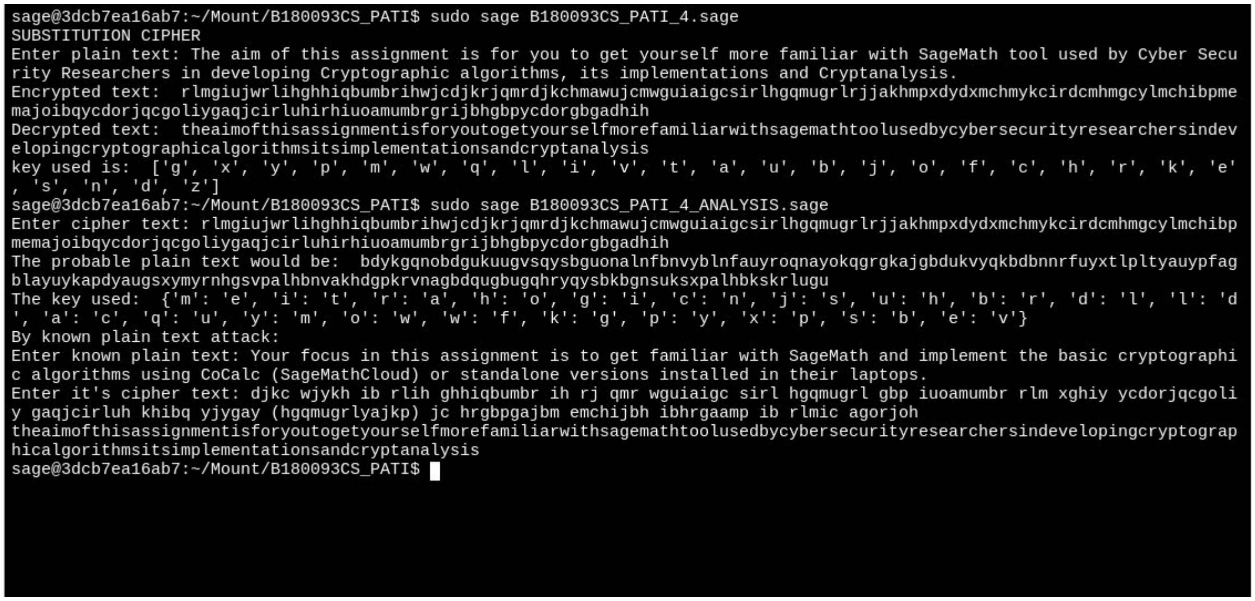
```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_1.sage
AFFINE CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis
Encryped text:  tnsquwkztnumqmmugdwsdtumzkfckatkgstckafmspzwkfszqwupuqfoutnmqgswqtntkkpamslxcecxsfmseafutcfsmsqfensfmudlshs
pkrudgefcrtkgfqrnueqpgkfutnwmutmuwrpswsdtqtukdmqdlefcrtqdqpcmum
Decryped text:  theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindeve
lopingcryptographicalgorithmsitsimplementationsandcryptanalysis
keys used to Add: 16  to multiply:  7
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_1_ANALYSIS.sage
Enter cipher text: tnsquwkztnumqmmugdwsdtumzkfckatkgstckafmspzwkfszqwupuqfoutnmqgswqtntkkpamslxcecxsfmseafutcfsmsqfensfmudl
shspkrudgefcrtkgfqrnueqpgkfutnwmutmuwrpswsdtqtukdmqdlefcrtqdqpcmum
The most probable plain texts would be:
By Known cipher text attack:
the aim of this assignment is for you to get yourself more familiar with sage math tool used by cyber security researchers
in developing cryptographic algorithms its implementations and cryptanalysis
et
Encrypt the above plain text and enter corresponding cipher text: st
The key is:  [7, 16]
By chosen plain text attack:
theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindevelopingcryptograp
hicalgorithmsitsimplementationsandcryptanalysis
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ 
```



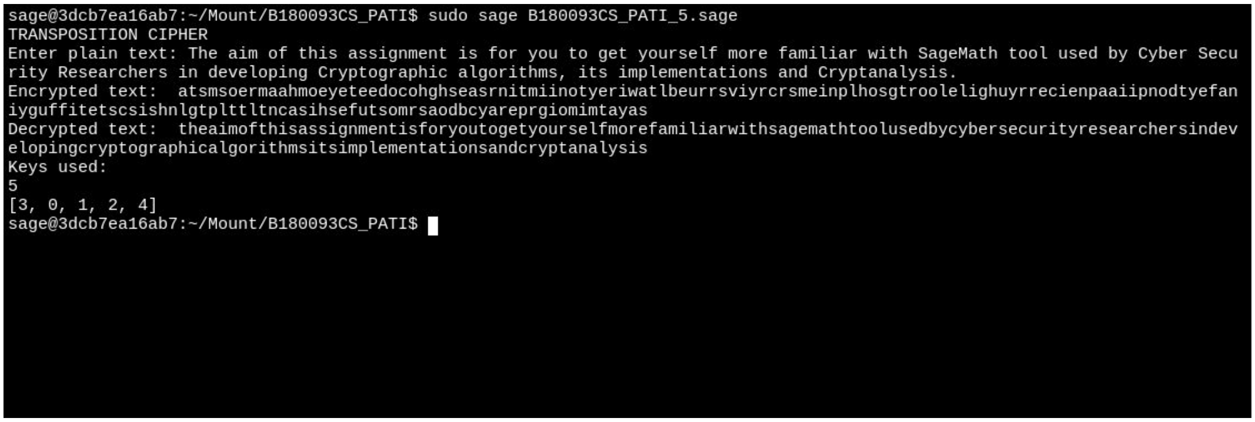
```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_2.sage
HILL CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis.
Encrypted text is:  hujxfoflrnkwwgwqujotsewldvjakfpfutstrftadhbeyqninzezbedtzqjxyagegpsetgtdkfqxzipedtswzuizhpwjdfyrrhddhfo
fzzbxjrinlwjjzroszurspyidebrudyfwgtaxbdpgsopaycyaxqtubeqtqfmgxkbnfq
Decrypted text is:  theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersin
developingcryptographicalgorithmsitsimplementationsandcryptanalysis
Key used:
[ 4 21 17  5 16]
[23  9 18  8  5]
[20 16  5 16 13]
[25  1  5 17 24]
[23 18  1  2 20]
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ 
```



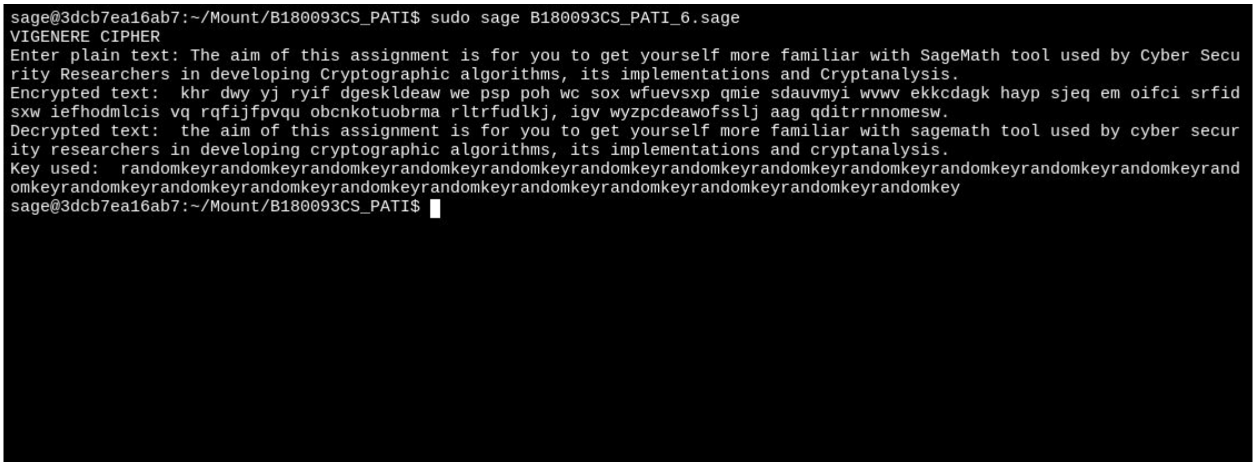
```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_3.sage
SHIFT CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis.
Encrypted text:  lzwsaegxlzakskkayfewflakxgjqgmlgywlqgmjkwdxegjwxseadasjoalzksyweslzlggdmkwvtquqtwjkwumjalqjwkwsjuzwjkafvwn
wdghafyujqhlgyjshzausdygjalzekalkaehdwewflslagfksfvujqhlsfsdqkak
Decrypted text:  theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindev
elopingcryptographicalgorithmsitsimplementationsandcryptanalysis
Key used:  18
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_3_ANALYSIS.sage
Enter cipher text: lzwsaegxlzakskkayfewflakxgjqgmlgywlqgmjkwdxegjwxseadasjoalzksyweslzlggdmkwvtquqtwjkwumjalqjwkwsjuzwjkafv
wnwdghafyujqhlgyjshzausdygjalzekalkaehdwewflslagfksfvujqhlsfsdqkak
The most probable plain text:
By known cipher text attack:
the aim of this assignment is for you to get yourself more familiar with sage math tool used by cyber security researchers
in developing cryptographic algorithms its implementations and cryptanalysis
To perform known plain text attack:
Enter known plain text: hello
Enter it's cipher text: zwddg
By known plain text attack:
theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindevelopingcryptograp
hicalgorithmsitsimplementationsandcryptanalysis
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$
```



```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_4.sage
SUBSTITUTION CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis.
Encrypted text:  rlmgiujwrlihghhiqbumbrihwjcdjkrjqmrdjkchmawujcmwguiaigcsirlhgqmugrlrjjakhmpxdydxmchmykcirdcmhmgcylmchibpme
majoibqycdorjqcgoliygaqjcirluhirhiuoamumbrgrijbhgbpycdorgbgadhih
Decrypted text:  theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindev
elopingcryptographicalgorithmsitsimplementationsandcryptanalysis
key used is:  ['g', 'x', 'y', 'p', 'm', 'w', 'q', 'l', 'i', 'v', 't', 'a', 'u', 'b', 'j', 'o', 'f', 'c', 'h', 'r', 'k', 'e'
, 's', 'n', 'd', 'z']
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_4_ANALYSIS.sage
Enter cipher text: rlmgiujwrlihghhiqbumbrihwjcdjkrjqmrdjkchmawujcmwguiaigcsirlhgqmugrlrjjakhmpxdydxmchmykcirdcmhmgcylmchibp
memajoibqycdorjqcgoliygaqjcirluhirhiuoamumbrgrijbhgbpycdorgbgadhih
The probable plain text would be:  bdykgqnobdgukuugvsqysbguonalnfbnvyblnfauyroqnayokqgrgkajgbdukvyqkbdbnnrfuyxtlpltyauypfag
blayuykapdyaugsxymyrnhgsvpalhbnvakhdgpkrvnagbdqugbugqhryqysbkbgnsuksxpalhbkskrlugu
The key used:  {'m': 'e', 'i': 't', 'r': 'a', 'h': 'o', 'g': 'i', 'c': 'n', 'j': 's', 'u': 'h', 'b': 'r', 'd': 'l', 'l': 'd
', 'a': 'c', 'q': 'u', 'y': 'm', 'o': 'w', 'w': 'f', 'k': 'g', 'p': 'y', 'x': 'p', 's': 'b', 'e': 'v'}
By known plain text attack:
Enter known plain text: Your focus in this assignment is to get familiar with SageMath and implement the basic cryptographi
c algorithms using CoCalc (SageMathCloud) or standalone versions installed in their laptops.
Enter it's cipher text: djkc wjykh ib rlih ghhiqbumbr ih rj qmr wguiaigc sirl hgqmugrl gbp iuoamumbr rlm xghiy ycdorjqcgoli
y gaqjcirluh khibq yjygay (hgqmugrlyajkp) jc hrgbpgajbm emchijbh ibhrgaamp ib rlmic agorjoh
theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindevelopingcryptograp
hicalgorithmsitsimplementationsandcryptanalysis
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$
```



```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_5.sage
TRANSPOSITION CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis.
Encrypted text:  atsmsoermaahmoeyeteedocohghseasrnitmiinotyeriwatlbeurrsviyrcrsmeinplhosgtrooleliguyrrecienpaaiipnodtyefan
iyguffitetscsishnlgtpltltncasihsefutsomrsaodbcyareprgiomimtayas
Decrypted text:  theaimofthisassignmentisforyoutogetyourselfmorefamiliarwithsagemathtoolusedbycybersecurityresearchersindev
elopingcryptographicalgorithmsitsimplementationsandcryptanalysis
Keys used:
5
[3, 0, 1, 2, 4]
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$
```



```
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ sudo sage B180093CS_PATI_6.sage
VIGENERE CIPHER
Enter plain text: The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Secu
rity Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis.
Encrypted text:  khr dwy yj ryif dgeskldeaw we psp poh wc sox wfuevsxp qmie sdauvmyi wvwv ekkcdagk hayp sjeq em oifci srfid
sxw iefhodmlcis vq rqfijfpvqu obcnkotuobrma rltrfudlkj, igv wyzpcdeawofsslj aag qditrrnnomesw.
Decrypted text:  the aim of this assignment is for you to get yourself more familiar with sagemath tool used by cyber secur
ity researchers in developing cryptographic algorithms, its implementations and cryptanalysis.
Key used:  randomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrand
omkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkeyrandomkey
sage@3dcb7ea16ab7:~/Mount/B180093CS_PATI$ 
```