Problem 1- Vignere Cipher Decryption

February 27, 2020

[8]:

```
import sys
sys.path.append('../')
import crypto_utils as utils
%load_ext autoreload
%autoreload 2

# probabilities of occurrence of 26 letters english alphabet
eng_alph_probs = [.082, .015, .028, .043, .127, .022, .020, .061, .070, .002, .
 ↪008, .040, .024, .067, .075, .019, .001, .060, .063, .091, .028, .010, .023,␣
 ↪.001, .020, .001]
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
The autoreload extension is already loaded. To reload it, use:
  %reload_ext autoreload
```

[10]:

```
cipher_text =␣
 ↪"JSJTEWXQVRFLOSNJRXCFXJSYTQZMNZFYILLGKRXNGJVVRMIMWGOAIBWOPSJYBSXVVRDQGYNROJWGQKBTTOLSPHBYBW
```

[11]:

```
# utils.index_of_coincidence('t', '6')
```

[12]:

```
k = 7
[y1,y2,y3,y4,y5,y6,y7] = utils.calc_ys(k, cipher_text)
print(utils.index_of_coincidence(y1))
print(utils.index_of_coincidence(y2))
print(utils.index_of_coincidence(y3))
print(utils.index_of_coincidence(y4))
print(utils.index_of_coincidence(y5))
print(utils.index_of_coincidence(y6))
print(utils.index_of_coincidence(y7))
```

```
0.07130494980962272
0.06894727561276671
0.08587550696526186
0.06894727561276671
0.06330453182860166
0.08040909892435197
0.06577323223417388
```

[13]:

```
# now calculate Mg(y)s
print("y1-")
utils.calc_M(y1)  # C looks like first letter with 0.068
print("y2-")
utils.calc_M(y2)  # O looks promising here 0.065
print("y3-")
utils.calc_M(y3)  # N here 0.072
print("y4-")
utils.calc_M(y4)  # F here 0.067
print("y5-")
utils.calc_M(y5)  # U here 0.065
print("y6-")
utils.calc_M(y6)  # S here 0.071
print("y7-")
utils.calc_M(y7)  # E here 0.066
# keyword is CONFUSE
```

```
y1-
A-G: 0.03 0.039 0.068 0.036 0.032 0.036 0.04
H-N: 0.033 0.038 0.045 0.03 0.033 0.037 0.053
O-U: 0.037 0.041 0.03 0.047 0.038 0.033 0.035
V-Z: 0.041 0.035 0.032 0.046 0.036
y2-
A-G: 0.039 0.044 0.034 0.044 0.042 0.036 0.032
H-N: 0.043 0.036 0.03 0.045 0.035 0.029 0.041
O-U: 0.065 0.035 0.031 0.045 0.042 0.031 0.032
V-Z: 0.041 0.031 0.036 0.034 0.047
y3-
A-G: 0.041 0.029 0.043 0.043 0.035 0.034 0.039
H-N: 0.03 0.032 0.053 0.039 0.026 0.038 0.072
O-U: 0.041 0.03 0.033 0.042 0.029 0.033 0.037
V-Z: 0.033 0.031 0.039 0.053 0.046
y4-
A-G: 0.035 0.045 0.03 0.028 0.041 0.067 0.038
H-N: 0.029 0.033 0.043 0.041 0.035 0.039 0.032
O-U: 0.038 0.038 0.047 0.035 0.036 0.04 0.047
V-Z: 0.037 0.03 0.037 0.037 0.043
y5-
A-G: 0.034 0.041 0.036 0.042 0.035 0.04 0.036
H-N: 0.044 0.039 0.046 0.036 0.031 0.033 0.04
O-U: 0.039 0.034 0.049 0.031 0.029 0.043 0.065
V-Z: 0.034 0.03 0.039 0.044 0.032
y6-
A-G: 0.032 0.031 0.037 0.05 0.039 0.042 0.036
H-N: 0.044 0.045 0.036 0.033 0.041 0.031 0.028
O-U: 0.044 0.035 0.028 0.042 0.071 0.039 0.03
V-Z: 0.041 0.047 0.03 0.034 0.037
```

```
y7-
A-G: 0.048 0.032 0.029 0.044 0.066 0.036 0.031
H-N: 0.041 0.042 0.034 0.036 0.036 0.029 0.038
O-U: 0.042 0.047 0.036 0.04 0.038 0.044 0.039
V-Z: 0.034 0.032 0.038 0.036 0.034
```

[14]:

```
shift = [alphabet.index("C"), alphabet.index("O"), alphabet.index("N"),␣
 ↪alphabet.index("F"), alphabet.index("U"), alphabet.index("S"), alphabet.
 ↪index("E")]
numerical_cipher_text = [0]*len(cipher_text)
for letter in range(len(cipher_text)):
  numerical_cipher_text[letter] = alphabet.index(cipher_text[letter])

# decrypt using keyword
for dec_let in range(len(numerical_cipher_text)):
  if dec_let % 7 == 0:
    numerical_cipher_text[dec_let:dec_let+7] = [(x - y)%26 for x, y in␣
 ↪zip(numerical_cipher_text[dec_let:dec_let+7], shift)]

for i in range(len(numerical_cipher_text)):
  numerical_cipher_text[i] = alphabet[numerical_cipher_text[i]]

print(''.join(numerical_cipher_text))
```

```
HEWOKETOHEARWOLVESINTHELOWHILLSTOTHEWESTOFTHEHOUSEANDHEKNEWTHATTHEYWOULDBECOMING
OUTONTOTHEPLAININTHENEWSNOWTORUNTHEANTELOPEANHOURLATERHEWASCROUCHEDINTHESNOWINTH
EDRYCREEKBEDHEWENTFORWARDONKNEESANDELBOWSANDWHENHEREACHEDTHELASTOFTHESMALLDARKJU
NIPERTREESHECROUCHEDQUIETLYTOSTEADYHISBREATHANDTHENRAISEDHIMSELFSLOWLYANDLOOKEDO
UTTHEYWERERUNNINGONTHEPLAINHARRYINGTHEANTELOPEANDTHEANTELOPEMOVEDLIKEPHANTOMSINT
HESNOWANDCIRCLEDANDWHEELEDANDTHEDRYPOWDERBLEWABOUTTHEMINTHECOLDMOONLIGHTANDTHEIR
BREATHSMOKEDPALELYINTHECOLDASIFTHEYBURNEDWITHSOMEINNERFIREANDTHEWOLVESTWISTEDAND
TURNEDANDLEAPTINASILENCESUCHTHATTHEYSEEMEDOFANOTHERWORLDENTIRETHEYMOVEDDOWNTHEVA
LLEYANDTURNEDANDMOVEDFAROUTONTHEPLAINUNTILTHEYWERETHESMALLESTOFFIGURESINTHATDIMW
HITENESSANDTHENTHEYDISAPPEARED
```