Problem 2- AutoKey Cipher by Brute Force

February 27, 2020

[4]:

```
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
```

[5]:

```
"""
2.28 Decrypt the following ciphertext, obtained from the Autokey Cipher, by␣
 ↪using exhaustive key search:
MALVVMAFBHBUQPTSOXALTGVWWRG
"""
cipher_text = "MALVVMAFBHBUQPTSOXALTGVWWRG"
```

[6]:

```
numeric_string = [0]*len(cipher_text)

for i in range(len(cipher_text)):
  numeric_string[i] = alphabet.index(cipher_text[i])

# do for keys from 0 to 26.
k = 0

while k < 26:

  # x1 = d_k(first numeric string) = (first numeric string - k) mod 26
  # x2 = d_x1(second numeric string) = (second numeric string - k) mod 26
  # x3 = d_x2(third ....)

  x_outs = [0]*len(cipher_text)
```

```
for i in range(len(x_outs)):
  # calculate current x
  if i==0:  # first iteration
    k_curr = k
  else:
    k_curr = x_outs[i-1]

  curr_x = (int(numeric_string[i]) - k_curr) % 26
  x_outs[i] = curr_x

decoded_text = [0]*len(cipher_text)
# turn back into plain english
for i in range(len(cipher_text)):
  decoded_text[i] = alphabet[x_outs[i]]

print(alphabet[k] + " plaintext: ")
print(' '.join(decoded_text))
k += 1
```

```
A plaintext:
M O X Y X P L U H A B T X S B R X A A L I Y X Z X U M
B plaintext:
L P W Z W Q K V G B A U W T A S W B Z M H Z W A W V L
C plaintext:
K Q V A V R J W F C Z V V U Z T V C Y N G A V B V W K
D plaintext:
J R U B U S I X E D Y W U V Y U U D X O F B U C U X J
E plaintext:
I S T C T T H Y D E X X T W X V T E W P E C T D T Y I
F plaintext:
H T S D S U G Z C F W Y S X W W S F V Q D D S E S Z H
G plaintext:
G U R E R V F A B G V Z R Y V X R G U R C E R F R A G
H plaintext:
F V Q F Q W E B A H U A Q Z U Y Q H T S B F Q G Q B F
I plaintext:
E W P G P X D C Z I T B P A T Z P I S T A G P H P C E
J plaintext:
D X O H O Y C D Y J S C O B S A O J R U Z H O I O D D
K plaintext:
C Y N I N Z B E X K R D N C R B N K Q V Y I N J N E C
L plaintext:
B Z M J M A A F W L Q E M D Q C M L P W X J M K M F B
M plaintext:
A A L K L B Z G V M P F L E P D L M O X W K L L L G A
N plaintext:
```

Z B K L K C Y H U N O G K F O E K N N Y V L K M K H Z

O plaintext:

Y C J M J D X I T O N H J G N F J O M Z U M J N J I Y

P plaintext:

X D I N I E W J S P M I I H M G I P L A T N I O I J X

Q plaintext:

W E H O H F V K R Q L J H I L H H Q K B S O H P H K W

R plaintext:

V F G P G G U L Q R K K G J K I G R J C R P G Q G L V

S plaintext:

U G F Q F H T M P S J L F K J J F S I D Q Q F R F M U

T plaintext:

T H E R E I S N O T I M E L I K E T H E P R E S E N T

U plaintext:

S I D S D J R O N U H N D M H L D U G F O S D T D O S

V plaintext:

R J C T C K Q P M V G O C N G M C V F G N T C U C P R

W plaintext:

Q K B U B L P Q L W F P B O F N B W E H M U B V B Q Q

X plaintext:

P L A V A M O R K X E Q A P E O A X D I L V A W A R P

Y plaintext:

O M Z W Z N N S J Y D R Z Q D P Z Y C J K W Z X Z S O

Z plaintext:

N N Y X Y O M T I Z C S Y R C Q Y Z B K J X Y Y Y T N