CSC8101: Penetration Testing

Assignment-1

Problem solving

Created by: Deep Shah

Date: 26th March 2022

Question 3: Perform Cryptanalysis to find out the plain text.

The given cipher text is:

RQODMBIQAO VAAG QE HTQQG HMI PTCEIO EAAG LCIAX CI EQQE HAAO PXQGMFA IQQ RMFY YQEAK VQX VQQG CEG QETK VQQTO ACI OAAGO

Solution: We can begin using cryptanalysis by dividing the statement down into individual words and attempting to discover each one separately. Because decrypting the sentences is complex, this is a straightforward technique.

Therefore, the sentence will look something like this:

RQODMBIQAO/VAAG/ QE/ HTQQG/ HMI/ PTCEIO/ EAAG/ LCIAX/ CI/ EQQE/ HAAO/ PXQGMFA/ IQQ/ RMFY/ YQEAK/ VQX/ VQQG/ CEG/ QETK/ VQQTO/ ACI/ OAAGO.

- The first step is to find the simple and smaller words that can predicted easily. My choice is to start with the two small words **ACI** and **CI.**
- the reason for choosing these words is there are only few words which are this small and has same ending.

  Therefore,

Cipher Text	ACI	CI
Plain Text	EAT	AT

- This is how we got three letters for our dictionary. Such as A(cipher text) is equal to E(Plain text), C(cipher text) is equal to A(plain text) and I(cipher text) is equal to T(plain text).
- Because of this we get many more words which contains this letter such as:

Cipher text	Plain Text
VAAG	_EE_
EAAG	_EE_
IQQ	T_ _
HAAO	_EE_
HMI	_ _T

- By looking at the above table we can easily conclude that Q(cipher text) is equal to O(Plain text).
- Now we can fill many blanks from above table.

Cipher text	Plain Text
VAAG	_EE_
EAAG	_EE_
IQQ	TOO
HAAO	_EE_
HMI	_ _T
EQQE	_OO_
VQQG	_OO_

- Now if we apply the same first and second step again and trial and error method we can obtain the few more words like QE(cipher text) can be ON(plain text), HMI(cipher text) can be BUT(plain text) and G(cipher text) can be D(plain text)
  Therefore,

Cipher text	Plain Text
VAAG	_EED
EAAG	_EED
IQQ	TOO
HAAO	BEE_
HMI	BUT

EQQE	NOON
VQQG	_OOD

- Now the final dictionary can be like this:

Cipher Text	Plain Text	Cipher Text	Plain Text	Cipher text	Plain Text
A	E	B	T	C	A
D	Q	E	N	F	C
G	D	H	B	I	T
J		K	Y	L	W
M	U	N		O	S
P	P	Q	O	R	M
S		T	L	U	
V	F	W		X	R
Y	H	Z			

Cipher text =

RQODMBIQAO VAAG QE HTQQG HMI PTCEIO EAAG LCIAX CI EQQE HAAO PXQGMFA IQQ RMFY YQEAK VQX VQQG CEG QETK VQQTO ACI OAAGO

Plain text =

MOSQUITOES FEED ON BLOOD BUT PLANTS NEED WATER AT NOON BEES PRODUCE TOO MUCH HONEY FOR FOOD AND ONLY FOOLS EAT SEEDS.