INF143A

Edyta

26 1 2022

Exercise 1 The following cipher text has been encrypted using the Caesar cipher. Reconstruct the plaintext and the secret key by exhaustive search.

Cnbcrwp xdc juu yxbbrkun tnhb dwcru rw cqrb fjh rb anonaanm cx jb j kadcn-oxaln bnjalq, xa ngqjdbcren bnjalq, jwm ljw rw yarwlryun kn jyyurnm jpjrwbc jwh lryqna. Rc bdllnnmb fqnw cqn wdvkna xo tnhb rb cxx bvjuu, r.n. fqnw cqn tnh byjln xo cqn lryqna rb bdoorlrnwcuh bvjuu.

Secret key: 17

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

Testing out all possible keys until in this way is referred to as a brute-force search or exehustive search, and can in principle be applied against any cipher. It succeeds when the number of keys is too small i.e when the key space of the cipher is sufficiently small.

Exercise 2 Exercise 2. A passage from a classic work of literature has been encrypted using a mono-alphabetic substitution cipher, producing the following ciphertext:

F zbon wtmw, wo wts yohhob mggjstsbifob, wtfi gtsbohsbob ou ntfwsbsii fi bow yobusiisa wo qs wts gjfhs mksbw fb srmkksjmwfbk wts wsjjoj ou oqlsywi owtsjnfis wsjjfqxs; boj wo wts cbfhmkfbmwfes hfba fi wtsjs mcktw ou wsjjoj fb wtois mggsmjmbysi ntois mnucxbsii wo mbowtsj hfba mxhoiw ioxsxv yobifiwi fb wtfi obs gtsbohsbob, sigsyfmxxv ntsb srtfqfwsa cbasj mbv uojh mw mxx mggjomytfbk wo hcwsbsii oj cbfesjimxfwv. Ntmw F hsmb qv wtsis wno iwmwshsbwi hmv gsjtmgi qs jsigsywfesxv sxcyfamwsa qv wts uoxxonfbk srmhgxsi.

Use frequency analysis to recover the plaintext and secret key.

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

Decrypted text:

I know that to the common apprehension, when phenomenon of whiteness is otherwise terrible nor to the unimaginative mind is there aught of terror in those appearances whose awfulness to another mind almost solely consists if this one phenomenon especially when exhibited under any form at all approaching to muteness of universality what I mean by there two statements may perhaps be respectively elucidated by the following examples.

Exercise 3 Write a simple implementation of the Vigenere cipher. Test it out by encrypting and decrypting a message. Try to break the encryption using the cryptanalysis tools at https://www.dcode.fr/vigenere-cipher.

wo bh pr qpt wp bh uhlt iv uhh ruhttlpn

Key 3 1 0

To be or not to be this is the question

Exercise 4

1.

DECRYPTION										
LETTER PLACE	7	4	11	11	14	19	7	4	17	4
PLAIN TEXT	**H**	**E**	**L**	**L**	**O**	**T**	**H**	**E**	**R**	**E**
LETTER PLACE	19	22	15	15	12	7	19	22	9	22
KEY	**T**	**W**	**P**	**P**	**M**	**H**	**T**	**W**	**J**	**W**
SUM	26	26	26	26	26	26	26	26	26	26
CIPHER	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**

K_1 = TWPPM HTWJW

2.

K_2 = TWPPM EMJPX

3.

K_3 = ETSHW YTAPQ

https://www.geocachingtoolbox.com/index.php?lang=en&page=oneTimePad

Exercise 5. Decrypt the ciphertext "IVSIKBFDGXQUMNBDVAZY" using the key "BERGEN" with the Playfair cipher.

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

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

Decrypted: APPLIEDCRYPTOGRAPBYX

http://rumkin.com/tools/cipher/playfair.php