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.