

# Vigenère **vvhq** Example

Ciphertext:

vvhqwvvrhmusgjgthkihtssejchlsfcbgvwcrlyqtfsvgahwkcuhauglqhnsrlrljshbltspisprd  
 xljsveeghlqwkasskuwepwqtwwspgoelkcqyfnsvgljsniqkgnrgybwlwgoviokhkazkqkxzgyhcec  
 meiujoqkwfwvfeqhkijrclrlkbienqfrjljsdhgrhlsfqtwlauqrhwdmwlglusgikkflryvcwvspgpm  
 lkassjvoqxeeggveggzmljcxljsvpaivwikvrdrygfrjljslveggvegggeiapuuisfpbtgnwwmucz  
 rvtwglrwugumnczville

In class, for potential key length = 5, in positions equivalent to 1 mod 5 (1, 6, 11, 16, 21, ...) we obtained frequencies

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
0	0	7	1	1	2	9	0	1	8	8	0	0	3	0	4	5	2	0	3	6	5	1	0	1	0

with highest relative frequencies:  $G = 9$ ,  $J = K = 8$ ,  $C = 7$ . So we should consider possibilities  $e \mapsto G, J, K$ , or  $C$ .

	a	b	c	d	e	f	g	h	i	j	k	l	m
English %	8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	4.0	2.4
$e \mapsto G$	C	D	E	F	G	H	I	J	K	L	M	N	O
$e \mapsto J$	F	G	H	I	J	K	L	M	N	O	P	Q	R
$e \mapsto K$	G	H	I	J	K	L	M	N	O	<b>P</b>	<b>Q</b>	R	S
$e \mapsto C$	Y	Z	A	B	C	D	E	F	G	H	I	J	K

	n	o	p	q	r	s	t	u	v	w	x	y	z
English %	6.7	7.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.3	0.1	2.0	0.1
$e \mapsto G$	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
$e \mapsto J$	S	T	U	V	W	X	Y	Z	A	B	<b>C</b>	D	E
$e \mapsto K$	T	U	V	W	X	Y	Z	A	B	C	D	E	F
$e \mapsto C$	L	M	N	O	P	Q	R	S	T	U	V	W	X

Now you try to refute  $e \mapsto C$ .