MATH 233: ASSIGNMENT 2

DUE: FRIDAY, FEBRUARY 9, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2023

Problem 1 (2.8.14)**.** The ciphertext `XVASDW` was encrypted using an affine function $\alpha x + 1 \pmod{26}$. Determine α and decrypt the message. (**The plaintext should be meaningful**.)

Problem 2 (2.8.16, modified)**.** You are trying to encrypt using the affine function $13x + 22 \pmod{26}$.

(a) Encrypt `hate` and `love`. Why is decryption impossible?

(b) How many (not necessarily meaningful) three-letter words are encrypted to `WWW`?

Problem 3 (2.8.20)**.** Suppose you have a language with only the three letters a, b, c, and they occur with frequencies .9, .09, and .01, respectively. The ciphertext `BCCCBCBCBC` was encrypted by the Vegenère cipher (the shifts are now mod 3, not mod 26). Find the plaintext.

Problem 4 (2.8.28)**.** The ciphertext

`BP EG FC AI MA MG PO KB HU`

was encrypted using the Playfair cipher with keyword *archimedes*. (Spaces were inserted for convenience, so you may ignore them.) Find the plaintext.

Problem 5. You intercepted the following three ciphertexts

`FAGGXFVFGVAVAFGGXXDXVGXA`

`FAGGXFVAGVAVAFGAXXDXVGVF`

`FAGGXFAAGVAVAFFVXXDXVGAV`

which were encrypted using the ADFGVX cipher with the following 6×6 matrix.

	A	D	F	G	V	X
A	p	g	5	c	3	e
D	n	b	q	j	o	z
F	2	r	8	s	l	a
G	0	f	t	m	1	d
V	6	v	i	w	9	k
X	u	y	x	4	h	7

You do not know the keyword, but you know that it is one of the following words.

ton, end, map, very, beat, done, light, build, model

It is likely that the plaintexts are meaningful sentences and they are identical except for the last few letters. Find the correct keyword and the plaintext corresponding to the first ciphertext.