Math373 **Quiz 1** **Fri. Jan 21, 2022**

Name: Solutions

Directions: Show all work. No credit for answers without work.

1. [**2 points**] True or False: A substitution cipher is vulnerable to brute force attack by modern computers. Explain your answer.

FALSE. A brute force attack would have to try all 26! keys, which would take much too long. Substitution ciphers are vulnerable to attack by staistical analysis.

2. [**3 parts, 2 points each**] Caeser shift cipher

(a) Complete the substitution table for the Caeser/shift cypher with key $k = 15$.

						5					10					15										
plaintext	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
cyphertext	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

(b) Using the key $k = 15$, encrypt the message "Deploy the weapon".

STEAD|N IWT L|TPEDC

STEAD NIWTL TPEDC

(c) Using the key $k = 15$, decrypt the message THRPE TIDBD GGDL.

escap e|tomo rrow

escape tomorrow

3. [**2 points**] In the English language, the letters 'a', 'e', 'i', 'o', and 'u' are vowels and the other letters are consonants. How many substitution ciphers encode vowels with vowels and consonants with consonants? Explain.

There are 5! ways to encode vowels with vowels, and 21! ways to encode consonants with consonants.

Picking one of each gives a cipher that does both, so there are $\boxed{(5!)(21!)}$ such substitution ciphers.