

Name: _____

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.

2. [3 parts, 2 points each] Caesar shift cipher

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

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																										

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

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

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.