Name: Solutions

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

1. **[3 parts, 2 points each]** Caeser shift cypher

   (a) Complete the substitution table for the Caeser/shift cypher with key $k = 7$.

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

   (b) Using the key $k = 7$, encrypt the message "Abort Operation".

HIVYA VWLYH APVU ⇒ **HIVYA VWLYH APVU**

   (c) Using the key $k = 7$, decrypt the message `HZZLA JVTWY VTPZL K`.

ASSET COMPR OMISE D ⇒ **asset compromised**

2. **[4 points]** Let $d = \gcd(5293, 3397)$. Use the extended Euclidean algorithm to compute d and find integers u and v such that $d = (5293 \cdot u) + (3397 \cdot v)$.

$5293 = (1)(3397) + 1896$

$3397 = (1)(1896) + 1501$

$1896 = (1)(1501) + 395$

$1501 = (3)(395) + 316$

$395 = (1)(316) + 79$

$316 = (4)(79) + 0$

$d = 79$

$79 = 395 - (1)(316)$

$= 395 - (1)[1501 - (3)(395)]$

$= (4)(395) - (1)(1501)$

$= (4)[1896 - (1)(1501)] - (1)(1501)$

$= (4)(1896) - (5)(1501)$

$= (4)(1896) - (5)[3397 - (1)(1896)]$

$= (9)(1896) - (5)(3397)$

$= (9)[5293 - (1)(3397)] - (5)(3397)$

$= (9)(5293) - (14)(3397)$

$u = 9, \quad v = -14$