Student Number: [redacted] Name: Bryan Hoang

1.

(a) **Answer:**
Using Table 1.11, the ciphertext of the plaintext message is

IBXFEPAQLBQAAXWQWIBXFSVAXW

(b) **Answer:**

Table 1: The associated decryption table of Table 1.11.

d	h	b	w	o	g	u	q	t	c	j	s	y	x	z	l	i	m	a	k	f	r	n	e	v	p
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

(c) **Answer:**
Using Table 1 to decrypt the message yields the following plaintext message:

`The secret password is sword fish.`

2.

(a) **Answer:**

Proof. Let $g = \gcd(a, b)$. Then $\exists\, A, B \in \mathbb{Z}$ such that $a = gA$ and $b = gB$. Then substituting the equations into the given one yields

$$\begin{aligned} 1 &= au + bv \\ &= gAu + gBv \\ &= g(Au + Bv) \end{aligned}$$

where $Au + Bv \in Z$. Therefore, g divides 1, implying that $g = 1$. □

(b) **Answer:**
It is not necessarily true that $\gcd(a, b) = 6$. For example, take $a = 1$ and $b = 2$. Then

$$a \cdot (-6) + b \cdot 6 = 6,$$

and yet $\gcd(a, b) = 1$.
Claim. In general, all possible values of $\gcd(a, b)$ divide 6, i.e., the RHS of $au + bv = 6$.

Proof. Suppose that $au + bv = c$ has a solution. Let $g = \gcd(a, b)$ and divide c by g with remainder to get

$$c = gq + r, \quad \text{with } q, r \in \mathbb{Z},\ 0 \leq r < g.$$

Then by the extended euclidean algorithm, we can find $x, y \in \mathbb{Z}$ such that $g = ax + by$. Then

$$\begin{gathered} au + bv = c = gq + r = (ax + by)q + r \\ \Rightarrow a(u - xq) + b(v - yq) = r. \end{gathered}$$

g divides the LHS since g divides both a and b, which implies that $g \mid r$. But if $0 \leq r < g$ and $g \mid r$, then we have that $r = 0$. Therefore, $c = gq$ which means that g divides c, where $c = 6$ for the specific example. □

Student Number: [redacted] Name: Bryan Hoang

(c) **Answer:**

(d) **Answer:**

Proof. Let's subtract one equation from the other to get

$$
\begin{aligned}
au + bv - au_0 - bv_0 &= 0 \\
a(u - u_0) &= -b(v - v_0). \qquad (1)
\end{aligned}
$$

Dividing both sides by g yields

$$\frac{a}{g}(u - u_0) = -\frac{b}{g}(v - v_0) \qquad (2)$$

We also have that

$$
\begin{aligned}
au + bv &= g \\
\Rightarrow \frac{a}{g}u + \frac{b}{g}v &= 1
\end{aligned}
$$

which, combined with part (a), gives $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$. By (**??**) □

3. **Answer:**

4. **Answer:**

5. **Answer:**

6. **Answer:**

7. **Answer:**

8. **Answer:**

9. **Answer:**

10. **Answer:**

11. **Answer:**

12. **Answer:**

Student Number: [redacted] Name: Bryan Hoang

13. **Answer:**

14. **Answer:**

15. **Answer:**