1.2. Decrypt each of the following Caesar encryptions by trying the various possible shifts until you obtain readable text.

(a) LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH

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

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

I THINKTHAT I SHALLNEVERSEE A BILLBOARD LOVELY AS A TREE

~~KVLK~~

~~JWij~~

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

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

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

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

1.3. For this exercise, use the simple substitution table given in Table 1.11.

(a) Encrypt the plaintext message

```
The gold is hidden in the garden.
```

(b) Make a decryption table, that is, make a table in which the ciphertext alphabet is in order from A to Z and the plaintext alphabet is mixed up.

(c) Use your decryption table from (b) to decrypt the following message.

(a) IBX FEPA QL BQAAXW QW IBX FSVAXW

the gold is hidden in the garden

IBX FEPA QL BQAAXWQWIBX FSVAXW

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

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

(c) IBXLX JVXIZ SLLDE VAQLL DEVAU QLB

these cretp asswo rdiss wordf ish

the secret password is swordfish

1.7. Use a calculator and the method described in Remark 1.9 to compute the following quotients and remainders.

(a) 34787 divided by 353.

$\frac{34787}{353} = 98.5467 \to 0$

$34787 = 353(98) + 193$

FOR REMAINDER: $r = a - b \cdot q$

$34787 - 353 \cdot 98 \to r = 193$

$q = 98$

(b) 238792 divided by 7843.

$238792 = 7843(30) + 3502$

$\frac{238792}{7843} = 30.4466$

$r = a - b \cdot q$

$238792 - 7843(30)$

$r = 3502$

$q = 30$

1.9. Use the Euclidean algorithm to compute the following greatest common divisors.

(a) gcd(291, 252).

(b) gcd(16261, 85652).

(a) $\frac{291}{252} = 1.15$ $\quad r = a - b \cdot q$

$r = 291 - 252 \cdot (1) = 39$

$39\overline{)252}$ 6 r 18

-234

18

$291 = 252(1) + 39$

$252 = 39(6) + 18$

$39 = 18(2) + 3 \leftarrow GCD = 3$

$18 = 3(6) + 0$

$18\overline{)39}$ 2 r 3

-36

3

(b) $85652 = 16261(5) + 4347$

$16261 = 4347(3) + 3220$

$4347 = 3220(1) + 1127$

$3220 = 1127(2) + 966$

$1127 = 966(1) + 161 \leftarrow GCD = 161$

$966 = 161(6) + 0$

1.10. For each of the $\gcd(a, b)$ values in Exercise 1.9, use the extended Euclidean algorithm (Theorem 1.11) to find integers u and v such that $au + bv = \gcd(a, b)$.

(a) $\gcd(291, 252) = 3$

$39 = a - 1b$

$18 = -6a + 7b$

$b = (a - 1b) \cdot 6 + 18$

$b = 6a - 6b + 18$

$-6a + 6b$

$-6a + 7b = 18$

$a - 1b = (-6a + 7b) \cdot 2 + 3$

$a - 1b = -12a + 14b + 3$

$+12a - 14b$

$13a - 15b = 3$

$13(291) - 15(252) = 3 = \gcd(291, 252)$

(b) $\gcd(16261, 85652) = 161$

$85652 = 16261(5) + 4347$

$16261 = 4347(3) + 3220$

$4347 = 3220(1) + 1127$

$3220 = 1127(2) + 966$

$1127 = 966(1) + 161$ ← GCD = 161

$966 = 161(6) + 0$

$4347 = a - 5b$

$b = (a - 5b) \cdot 3 + 3220$

$b = 3a - 15b + 3220$

$-3a + 16b = 3220$

INTO LINE 3:

$a - 5b = (-3a + 16b) \cdot 1 + 1127$

$+3a - 16b$

$4a - 21b = 1127$

INTO LINE 4:

$-3a + 16b = (4a - 21b) \cdot 2 + 966$

$8a - 42b$

$-11a + 58b = 966$

$4a - 21b = (-11a + 58b) \cdot 1 + 161$

$+11a - 58b$

$15a - 79b = 161$

$-79(16261) + 15(85652) = 161$

$= \gcd(16261, 85652)$