1 Problem statement

Create a program than can encrypt text using the Hill cipher, given an encryption key with $m = 2$, and which can then compute the decryption key and decrypt the cyphertext.

2 Algorithms

2.1 Modular inverse

Brute force algorithm

```
Require: $gcd(a, n) = 1$
Ensure: $b \cdot a \equiv 1 \mod n$
  procedure MOD_INVERSE(a,n)                              ▷ Complexity: $\theta(2^n)$
      for i=1,n do
          if $a \cdot i \equiv 1 \mod n$ then
              mod_inverse ← i
          end if
      end for
  end procedure
```

2.2 Invertion of 2x2 matrix

Cramer's rule

```
Require: $gcd(det(A), n) = 1$
Ensure: $BA = AB = I \mod n$
  procedure INVERT_MATRIX(A,n)                            ▷ Complexity: $\theta(m!)$
      invert_matrix ← $mod\_inverse(a * d - b * c) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
  end procedure
```

2.3 Encryption

```
Require: $gcd(det(K), n) = 1$
  procedure ENCRYPT(K,x,n)                                ▷ Complexity: $\theta(m^3)$
      invert_matrix ← $xK$
  end procedure
```

2.4 Decryption

```
Require: $gcd(det(K'), n) = 1$
  procedure DECRYPT(K',y,n)                    ▷ Complexity: $\theta(m^3)$
      invert_matrix ← $yK'$
  end procedure
```

3 Test data

Using the 27 letter alphabet and the key $1, 23, 10, 13$, if we encrypt the word LABORATORY we get VSQYAVHGYJ