```
> # Answer to question 3 of homework 2, i.e., Exercise 1.24 page 42¶
> with(linalg):¶
> fc:=proc(L)↵
    local Ans;↵
    # This function converts alphabetic symbols into integers mod
  26↵
    Ans:=`ERROR`;↵
    if  L=`a` then Ans:=0;↵
    elif L=`b` then Ans:=1;↵
    elif L=`c` then Ans:=2;↵
    elif L=`d` then Ans:=3;↵
    elif L=`e` then Ans:=4;↵
    elif L=`f` then Ans:=5;↵
    elif L=`g` then Ans:=6;↵
    elif L=`h` then Ans:=7;↵
    elif L=`i` then Ans:=8;↵
    elif L=`j` then Ans:=9;↵
    elif L=`k` then Ans:=10;↵
    elif L=`l` then Ans:=11;↵
    elif L=`m` then Ans:=12;↵
    elif L=`n` then Ans:=13;↵
    elif L=`o` then Ans:=14;↵
    elif L=`p` then Ans:=15;↵
    elif L=`q` then Ans:=16;↵
    elif L=`r` then Ans:=17;↵
    elif L=`s` then Ans:=18;↵
    elif L=`t` then Ans:=19;↵
    elif L=`u` then Ans:=20;↵
    elif L=`v` then Ans:=21;↵
    elif L=`w` then Ans:=22;↵
    elif L=`x` then Ans:=23;↵
    elif L=`y` then Ans:=24;↵
    elif L=`z` then Ans:=25;↵
    end if;↵
    RETURN(Ans);↵
  end proc:¶
> P:=matrix(1,18,[a,d,i,s,p,l,a,y,e,d,e,q,u,a,t,i,o,n]);↵
  C:=matrix(1,18, [d,s,r,m,s,i,o,p,l,x,l,j,b,z,u,l,l,m]);¶
```

$$P := [a \quad d \quad i \quad s \quad p \quad l \quad a \quad y \quad e \quad d \quad e \quad q \quad u \quad a \quad t \quad i \quad o \quad n]$$¶

$$C := [d \quad s \quad r \quad m \quad s \quad i \quad o \quad p \quad l \quad x \quad l \quad j \quad b \quad z \quad u \quad l \quad l \quad m]$$¶

```
> X:=matrix(1,18):    Y:=matrix(1,18):↵
  for N from 1 to 18 do↵
```

```
    X[1,N]:=fc(P[1,N]):
    Y[1,N]:=fc(C[1,N]):
  od:
  evalm(X);evalm(Y);
```

$$[0 \quad 3 \quad 8 \quad 18 \quad 15 \quad 11 \quad 0 \quad 24 \quad 4 \quad 3 \quad 4 \quad 16 \quad 20 \quad 0 \quad 19 \quad 8 \quad 14 \quad 13]$$

$$[3 \quad 18 \quad 17 \quad 12 \quad 18 \quad 8 \quad 14 \quad 15 \quad 11 \quad 23 \quad 11 \quad 9 \quad 1 \quad 25 \quad 20 \quad 11 \quad 11 \quad 12]$$

```
> XX:=matrix(3,6):  YY:=matrix(3,6):
  for i from 0 to 2 do  for j from 0 to 5 do
    XX[i+1,j+1]:=X[1,3*j+i+1]:
    YY[i+1,j+1]:=Y[1,3*j+i+1]:
  od:  od:
  XX:=transpose(XX):  YY:=transpose(YY):
  evalm(X);evalm(XX);evalm(Y);evalm(YY);
```

$$[0 \quad 3 \quad 8 \quad 18 \quad 15 \quad 11 \quad 0 \quad 24 \quad 4 \quad 3 \quad 4 \quad 16 \quad 20 \quad 0 \quad 19 \quad 8 \quad 14 \quad 13]$$

$$\begin{bmatrix} 0 & 3 & 8 \\ 18 & 15 & 11 \\ 0 & 24 & 4 \\ 3 & 4 & 16 \\ 20 & 0 & 19 \\ 8 & 14 & 13 \end{bmatrix}$$

$$[3 \quad 18 \quad 17 \quad 12 \quad 18 \quad 8 \quad 14 \quad 15 \quad 11 \quad 23 \quad 11 \quad 9 \quad 1 \quad 25 \quad 20 \quad 11 \quad 11 \quad 12]$$

$$\begin{bmatrix} 3 & 18 & 17 \\ 12 & 18 & 8 \\ 14 & 15 & 11 \\ 23 & 11 & 9 \\ 1 & 25 & 20 \\ 11 & 11 & 12 \end{bmatrix}$$

```
> SWXX:=swaprow(XX,1,6);  SWYY:=swaprow(YY,1,6);
```

$$SWXX := \begin{bmatrix} 8 & 14 & 13 \\ 18 & 15 & 11 \\ 0 & 24 & 4 \\ 3 & 4 & 16 \\ 20 & 0 & 19 \\ 0 & 3 & 8 \end{bmatrix}$$

$$SWYY := \begin{bmatrix} 11 & 11 & 12 \\ 12 & 18 & 8 \\ 14 & 15 & 11 \\ 23 & 11 & 9 \\ 1 & 25 & 20 \\ 3 & 18 & 17 \end{bmatrix}$$

```
> XE:=submatrix(SWXX,[1,3,5],1..3);XO:=submatrix(SWXX,[2,4,6],1..3);
```

```
YE:=submatrix(SWYY,[1,3,5],1..3);YO:=submatrix(SWYY,[2,4,6],1..3);
```

$$XE := \begin{bmatrix} 8 & 14 & 13 \\ 0 & 24 & 4 \\ 20 & 0 & 19 \end{bmatrix}$$

$$XO := \begin{bmatrix} 18 & 15 & 11 \\ 3 & 4 & 16 \\ 0 & 3 & 8 \end{bmatrix}$$

$$YE := \begin{bmatrix} 11 & 11 & 12 \\ 14 & 15 & 11 \\ 1 & 25 & 20 \end{bmatrix}$$

$$YO := \begin{bmatrix} 12 & 18 & 8 \\ 23 & 11 & 9 \\ 3 & 18 & 17 \end{bmatrix}$$

```
> MX:=evalm(XE-XO);  MY:=evalm(YE-YO);
```

$$MX := \begin{bmatrix} -10 & -1 & 2 \\ -3 & 20 & -12 \\ 20 & -3 & 11 \end{bmatrix}$$

$$MY := \begin{bmatrix} -1 & -7 & 4 \\ -9 & 4 & 2 \\ -2 & 7 & 3 \end{bmatrix}$$

```
> # MX has an inverse mod 26 because its determinant is relatively
  prime to 26
  det(MX)mod 26;  igcd(det(MX),26);
```

$$3$$

$$1$$

```
> UMX:=map(mods, MX, 26); det(UMX) mod 26; # Please note the
  multiplicative inverse of 3 mod 26 is  9 mod 26
```

$$UMX := \begin{bmatrix} -10 & -1 & 2 \\ -3 & -6 & -12 \\ -6 & -3 & 11 \end{bmatrix}$$

$$3$$

```
> # The inverse of UMX mod 26 is computed as follows:
  IMX:=map(mods,evalm(9*adjoint(UMX)),26);
```

$$IMX := \begin{bmatrix} -8 & -7 & 8 \\ 9 & 2 & 10 \\ -9 & -8 & -7 \end{bmatrix}$$

```
> # We now check to see if we have really computed the inverse mod
  26
```

```
map(mods,evalm( IMX &* MX),26);
```

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

```
> # We can now determine the matrix A in the encrypting equation
  Y=XA+B  ==> A = IMX &* MY mod 26
  A:=map(modp,evalm(IMX &* MY),26);
```

$$A := \begin{bmatrix} 3 & 6 & 4 \\ 5 & 15 & 18 \\ 17 & 8 & 5 \end{bmatrix}$$

```
> # We now determine the affine part B of the encryption equation by
  solving the equation Y=MX + B for B
  ZY:=submatrix(YY,1..1,1..3);  ZX:=submatrix(XX,1..1,1..3);
```

$$ZY := [3 \quad 18 \quad 17]$$

$$ZX := [0 \quad 3 \quad 8]$$

```
> B:=map(modp, evalm(ZY - evalm(ZX &* A)), 26);
```

$$B := [8 \quad 13 \quad 1]$$

```
> # We new check to see f we have the correct answer by checking to
  see that YY = (XX &* A) +B
  map(modp,evalm(YY - evalm(XX &* A)),26);;
```

$$\begin{bmatrix} 8 & 13 & 1 \\ 8 & 13 & 1 \\ 8 & 13 & 1 \\ 8 & 13 & 1 \\ 8 & 13 & 1 \\ 8 & 13 & 1 \end{bmatrix}$$

```
>
```