Homework 6, due September 22

(1) `B%dHQ2tANU8qXC/BaiZ Cd6=!s*{tlzgPPFe>=yskd1VT2CIg.Bn)+@hiy,C$0jr8igj5O[(i{`

`M'IBTQQO\]GqQDABfob?6]AE!}+lcr5i;NSpC=mU‘n?\T#SEP‘ad*N<r[u+2C2_Z$i]XFa(X3{`

(2) (Page 57, problem 18) Let a, b, c, d, e, f be integers mod 26. Represent a block of plaintext as a pair (x, y) (mod 26). The corresponding ciphertext (u, v) is

$$(x\ y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e\ f) \equiv (u\ v) \pmod{26}.$$

Describe how to carry out a chosen plaintext attack on this system and find the key a, b, c, d, e, f. You should state explicitly what plaintexts you choose and how to recover the key.

(3) The following ciphertext was encrypted by a Hill cipher with matrix

$$\begin{bmatrix} 1 & 0 & 5 \\ 7 & -1 & 9 \\ 4 & 6 & 3 \end{bmatrix}.$$

`22 15 0 16 22 8 5 22 14 13 20 10 10 6 8 2 4 7 8 16 22`

Decrypt.

(4) (Page 61, problem 11) The following sequence was generated by a linear feedback shift register. Determine the recurrence that generated it.

```
1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1,
1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0,
0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1,
1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0
```