1. Linear ciphers are less secure than non-linear ones because ciphers that are linear with respect to some field have keys that are more easily decipherable via linear interpolation or Gaussian elimination using knowledge of several plaintext-ciphertext pairs.

2. A block cipher is a mapping of n-bit plaintext blocks to n-bit ciphertext blocks with $n \in \mathbb{Z}_{26}$ and typically requires cutting of the plaintext into such blocks. A stream cipher does not typically require plaintext cutting and is a direct mapping of an n-bit plaintext to an n-bit ciphertext.

3. Software efficient: HC-128: 128 bit keys Rabbit: 128 bit keys Salsa20/12: 128 and 256 bit keys Sosemanuk: 128 and 256 bit keys

   Hardware/Memory efficient: Grain v1: 80-bit and 128-bit keys Mickey 2.0: 80-bit keys Trivium: 80-bit keys

4. $$A^{-1} = \begin{bmatrix} 11 & 15 \\ 1 & 20 \end{bmatrix}$$

5. Key = P, ITISTIMETOTAKESECURITYSERIOUSLY

6. (a) 10001 (b) 5, no (c) $1 + C_0x + C_1x^2 + C_2x^3$

7. See attached:

   (a)

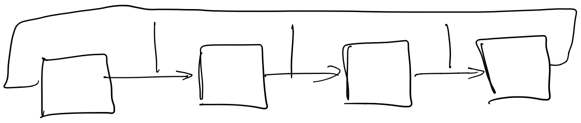
   (b)

   (c) $1 + C_0x + C_1x^2 + C_2x^3$, period = 17

7) {$\underbrace{1001000}_{A}$ 0010100 0010000 1001011 0110001 1111010 0111110 1010100}

$\frac{0}{1}$ $\frac{0}{1}$ $\frac{0}{1}$

a)



1
0
0
1
0
0
0

b)

c)

d)

e)