CRYPTOGRAPHY HANDOUT 05

BLOCK CIPHERS

1. Matrix Facts

- The *determinant* of a 2×2 matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\det(M) = ad - bc$.
- The *inverse* of a matrix M is denoted M^{-1} and is the one in which $MM^{-1} = M^{-1}M = I$, where I is the identity matrix. For a 2×2 matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the inverse is $M^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

2. Hill Cipher

1. Choose an $n \times n$ matrix M.
2. Break the plaintext into vectors of length n (using $a = 0, b = 1, \cdots, z = 25$).
3. To encrypt: multiply each vector by M and reduce $\bmod 26$.
4. To decrypt: use multiplication with M^{-1}.

Example. Suppose we know that $n = 2$ and the following plaintext and ciphertext correspondence:

plaintext	`howareyoutoday`
CIPHERTEXT	`ZWSENIUSPLJVEU`

3. Properties of Good Cryptosystems (Claude Shannon)

- **Diffusion**: if we change a character of the plaintext, then several characters of the ciphertext change too (and vice versa).
- **Confusion**: the key isn't related to the ciphertext in an easy way, and each character of the ciphertext should depend on several parts of the key.