Classical Cryptosystems

Definition. An \( n \)-block cipher is a cryptosystem with
\[ \mathcal{P} = \mathcal{C} = \Sigma^n, \]
for some finite set \( \Sigma \).

The set \( \Sigma \) is called the alphabet of the cipher, and
the elements of \( \Sigma^n = \underbrace{\Sigma \times \cdots \times \Sigma}_n \) are called words.

Examples: 1) Caesar’s cryptosystem (ca. 50BC):
\[ \Sigma = \mathbb{Z}/26\mathbb{Z} \text{ and } n = 1. \]
Moreover, \( \mathcal{K} = \Sigma \) and
\[ E_k(x) = x + k \pmod{26} \text{ and } D_k = x - k \pmod{26}. \]

2) Vigenère’s cipher (16th century):
\[ \Sigma = \mathbb{Z}/m\mathbb{Z} \text{ and } n \geq 1. \]
Moreover, \( \mathcal{K} = \mathcal{P} \) (viewed as vectors) and
\[ E_{\vec{k}}(\vec{x}) = \vec{x} + \vec{k} \pmod{m} \text{ and } D_{\vec{k}} = \vec{x} - \vec{k} \pmod{m}. \]

3) Hill’s cipher (1926):
\[ \Sigma = \mathbb{Z}/m\mathbb{Z} \text{ and } n \geq 1. \]
Moreover, \( \mathcal{K} = \text{GL}_n(\Sigma) \) (set of invertible \( n \times n \) matrices) and
\[ E_A(\vec{x}) = A\vec{x} \pmod{m} \text{ and } D_A = A^{-1}\vec{x} \pmod{m}. \]

Definition: An affine block cipher is \( n \)-block cipher
with \( \Sigma = \mathbb{Z}/m\mathbb{Z}, n \geq 1, \mathcal{K} = \text{GL}_n(\Sigma) \times \mathcal{P}, \) and
\[ E_{A,\vec{b}}(\vec{x}) = A\vec{x} + \vec{b}, \quad D_{A,\vec{b}} = A^{-1}\vec{x} - A^{-1}\vec{b}, \]
where we compute mod \( m \), i.e., in \( \mathbb{Z}/m\mathbb{Z} \).
**Question:** When is an $n \times n$ matrix $A \in M_n(\mathbb{Z}/m\mathbb{Z})$ invertible?

**Lemma:** Let $R$ be a commutative ring and $A \in M_n(R)$ an $n \times n$-matrix with entries in $R$. Then the following conditions are equivalent.

(i) $A$ is invertible, i.e., there exists $B \in M_n(R)$ such that $AB = BA = I$.

(ii) $\det(A) \in R^\times$.

(iii) The associated linear map $L_A : R^n \to R^n$ is bijective. Here $L_A$ is given by $L_A(\vec{x}) = A\vec{x}$.

**Example:** The matrix $A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{Z})$ has determinant $\det(A) = 3 \cdot 3 - 2 \cdot 2 = 5$.

If we view $A$ as a matrix mod $m$, then we see that

$A \in \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \iff 5 \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \gcd(5, m) = 1 \iff 5 \nmid m$.

To find $A^{-1}$, we use the usual cofactor formula which yields $A^{-1} \equiv \frac{1}{5} \begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix} \mod m$.

In particular, if $m = 26$, then $\frac{1}{5} \equiv 21 \mod 26$ and $\frac{3}{5} \equiv 21 \cdot 3 \equiv 11 \mod 26$, so $A^{-1} \equiv \begin{pmatrix} 11 & 10 \\ 10 & 11 \end{pmatrix} \mod 26$. 