Problems in cryptography, set 3

1. Let \( p(x) \) be a polynomial irreducible in \( \mathbb{Z}_p \). You can extend the \( \mathbb{Z}_p \) with root \( a \) of the polynomial \( p(x) \), to a field \( \mathbb{F} \), whose elements have the form
\[
x_{k-1}a^{k-1} + \cdots + x_1a + x_0,
\]
where \( k \) is the degree of the polynomial \( p(x) \), and \( x_0, \ldots, x_{k-1} \in \mathbb{Z}_p \). How would you implement arithmetic operations in \( \mathbb{F} \)?

2. (a) Show that in any finite field \( \mathbb{F} \), there is a natural number \( p \), that one added to itself \( p \) times is equal 0.
(b) Show that the minimum such \( p \) is a prime number.
(c) Show that the field \( \mathbb{F} \) is a linear space over \( \mathbb{Z}_p \). It implies that the number of elements of \( \mathbb{F} \) is \( p^k \), where \( k \) is the dimension of the space.

3. (a) Show that if a finite field \( \mathbb{F} \) has \( m \) elements, then
\[
\prod_{y \in \mathbb{F} \setminus \{0\}} y = \prod_{y \in \mathbb{F} \setminus \{0\}} xy = x^{m-1} \prod_{y \in \mathbb{F} \setminus \{0\}} y
\]
and this implies that \( x^{m-1} = 1 \) for all \( x \in \mathbb{F} \).
(b) Show that if \( k \) is the smallest natural power that \( x^k = 1 \), and \( l \) is the smallest natural power that \( y^l = 1 \) for \( x, y \in \mathbb{F} \), then there is a \( z \in \mathbb{F} \), that \( n = \text{lcm}(k, l) \) is the smallest natural power that \( z^n = 1 \).
(c) Show that if \( k \) is the least common multiple of all the smallest powers \( l \) of \( x \in \mathbb{F} \setminus \{0\} \) that \( x^l = 1 \), then there is a \( y \in \mathbb{F} \) for which \( k \) is the smallest natural power that \( y^k = 1 \). Moreover, for all \( x \in \mathbb{F} \setminus \{0\} \) we have \( x^k = 1 \). Prove also that \( k|n - 1 \).
(d) Show that, since the polynomial \( x^k - 1 \) in a field has at most \( k \) roots, we have \( k = m - 1 \) and there exists \( y \) such that all the elements \( x \in \mathbb{F} \setminus \{0\} \) take the form \( x = y^t \). This means that the multiplicative group the finite field is always cyclic.

4. What is the order of the group \( \mathbb{Z}_p^* \), consisting of invertible elements modulo \( p^k \) (\( p > 2 \) is a prime number). What order in this group has the element \( p + 1 \)? Show that it is a cyclic group.

5. Show that if \( \alpha > 2 \), the group \( \mathbb{Z}_{2^\alpha}^* \) is not cyclic, but 5 generates a subgroup consisting of half of its elements (exactly those congruent to 1 mod 4).

6. The AES S-box calculates the byte value \( b \) in such a way that
- If \( b \neq 0 \), then \( c = b^{-1} \) in the field \( \mathbb{F}_{2^8} \), which is the field of polynomials over \( \mathbb{Z}_2 \) with arithmetic operations modulo some fixed irreducible polynomial of degree eight. If \( b = 0 \), then \( c = 0 \).
- Let \( c = c_0c_1c_2c_3c_4c_5c_6c_7 \). Then \( d_i = c_i \oplus c_{i+4} \oplus c_{i+5} \oplus c_{i+6} \oplus c_{i+7} \) where the indices are added modulo 8.
- The result of S-box of the \( e = d \oplus 01100011 \).

What is the inverse transformation to this S-box?