Homework Assignment 5

Due date: December 13, 2019

It is possible to collect up to 110 points in this homework.

1. Consider Shamir’s secret sharing scheme over \( \mathbb{F}_4 = \{0, 1, \beta, \beta^2\} \) with \( n = 3 \) and \( k = 3 \). Let \( \alpha_1 = 1, \alpha_2 = \beta \) and \( \alpha_3 = \beta^2 \). Assume that the secret \( s \) is selected randomly and uniformly in \( \mathbb{F}_4 \). User 1 knows that \( P(\alpha_1) = 0 \), user 2 knows that \( P(\alpha_2) = 0 \), and user 3 knows that \( P(\alpha_3) = \beta^2 \), where \( P(x) = a_2x^2 + a_1x + s \), \( a_i \in \mathbb{F}_4 \) are selected uniformly at random, and \( s \in \mathbb{F}_4 \).

(a) Show that if users 1 and 2 try to find \( s \), then any value of \( s \in \mathbb{F}_4 \) is equally probable.

(b) Show that all three users jointly can find \( s \). What is the value of \( s \)?

2. Alice communicates with Bob by using coset coding over \( \mathbb{F}_5 \). She wants to send a message \((s_1, s_2)\) securely. In order to do so, Alice picks a random solution \( \bar{x} = (x_1, x_2, x_3, x_4) \) of the system

\[
H \cdot \bar{x}^T = (s_1, s_2)^T,
\]

and sends it to Bob, where \( H \) is the parity-check matrix given by

\[
H = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4
\end{pmatrix}.
\]

(a) What are the parameters \( n, k \) and \( d \) of the code defined by \( H \)? Prove.

(b) How many different solutions \((x_1, x_2, x_3, x_4)\) can Alice choose from?

(c) Assume that wiretapper Eve intercepts \( x_2 = 3 \) and \( x_4 = 2 \). Show that Eve does not know anything about the syndrome \((s_1, s_2)\) that was sent. In other words, show that from Eve’s point of view, any syndrome \((s_1, s_2)\) is equally probable.

(d) Assume now that Eve intercepts \( x_1 = 1 \), in addition to \( x_2 = 3 \) and \( x_4 = 2 \). Show that now Eve has some knowledge about the syndrome \((s_1, s_2)\). It this knowledge sufficient to determine \((s_1, s_2)\) in a unique way?

(e) If additionally to (d), Eve knows that \( s_2 = 3 \), then what is \( s_1 \)?

3. Let \( a(x) \) and \( b(x) \) be two nonzero polynomials over a finite field \( \mathbb{F} \) such that \( \deg(a(x)) > \deg(b(x)) \). Consider the extended Euclid’s algorithm, which was presented in the lecture (for your convenience that algorithm also appears in the appendix at the end of this homework). Let \( \tau \) be the largest index \( i \) such that \( r_i(x) \neq 0 \). Show by induction on \( i \):

(a) For all \( i = 0, 1, 2, \cdots, \tau \) we have \( s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = (-1)^{i+1} \).

(b) For all \( i = -1, 0, 1, \cdots, \tau + 1 \) we have \( s_i(x)a(x) + t_i(x)b(x) = r_i(x) \).
(c) For all $i = 1, 2, \cdots, \tau + 1$ we have $\deg(t_i(x)) + \deg(r_{i-1}(x)) = \deg(a(x))$. (Hint: you can use (a) and (b).)

4. For a polynomial $a(x) = \sum_{i=0}^{n} a_i x^i$ over a finite field $F$ define a formal derivative of $a(x)$ to be

$$a'(x) = \sum_{i=1}^{n} i \cdot a_i x^{i-1}.$$ 

Let $a(x)$ and $b(x)$ be two polynomials (of possibly different degrees) over $F$, and $c \in F$. Show that:

(a) $(a(x) + b(x))' = a'(x) + b'(x)$.
(b) $(c \cdot a(x))' = c \cdot a'(x)$.
(c) $(a(x) \cdot b(x))' = a(x) \cdot b'(x) + a'(x) \cdot b(x)$.

Appendix

```
r_{-1}(x) = a(x); \quad r_0(x) = b(x);
s_{-1}(x) = 1; \quad s_0(x) = 0;
t_{-1}(x) = 0; \quad t_0(x) = 1;
```

```
for ( i = 1; r_{i-1}(x) \neq 0; i++ ) {
    r_{i-2}(x) = q_i(x) \cdot r_{i-1}(x) + r_i(x);
    s_{i-2}(x) = q_i(x) \cdot s_{i-1}(x) + s_i(x);
    t_{i-2}(x) = q_i(x) \cdot t_{i-1}(x) + t_i(x);
}
```

Extended Euclid’s algorithm.