Problems in cryptology, week 6

Exercise 7.1 *Assume that the plaintexts "Buy Volvo" (BV) and "Sell Volvo" (SV) have the same probability. Construct a cryptosystem with a probability for a successful impersonation attack* $P_I = 1/4$.

Exercise 7.2 *Consider the following system for authentication.*

Key	Plaintext	
K	BV	SV
00	00	10
01	01	00
10	11	01
11	10	11

Assume that the key is chosen randomly with equal probability. The probabilities for the plaintexts "Buy Volvo" (BV) and "Sell Volvo" (SV) are $P(BV) = 1 - P(SV) = 0.89$. *Find* P_I, P_S *and Simmons' lower bound.*
Hint: The value of the binary entropy function, $h(p)$, *for* $p = 0.11$ *is* $h(0.11) = 0.5$.

Exercise 7.3 *For an impersonation attack Simmons's bound is*

$$P_I \geq 2^{-I(K;C)}.$$

For a substitution attack we have the bound

$$P_S \geq 2^{-H(K|C)}.$$

a) *Show that for* $P_D = max(P_I, P_S)$ *the following holds:*

$$P_D \geq \frac{1}{\sqrt{|K|}}$$

Hint: Consider $P_I \cdot P_S$.

b) *For a cryptosystem the ciphertext* $\underline{c}$ *is generated according to*

$$\underline{c} = (m + k_1, mk_1 + k_2)$$

where m, k_1, $k_2 \in \mathbb{F}_2$, m *is the plaintext and* $\underline{k} = (k_1, k_2)$ *is a two bit key. The keys are uniformly distributed. Show that the bound in a) has equality if* $P(m = 0) = 1/2$.

Exercise 8.1 *The Shamir Threshold Scheme is described for* $\mathcal{K} = \mathbb{Z}_p$ *but it works equally well over any field* $\mathbb{F}_q$. *Design a (2,4)-threshold scheme for* $\mathbb{F}_{2^3}$, *when* $K = 1$. *Construct the field using the primitive polynomial* $f(x) = x^3 + x + 1$ *over* $\mathbb{F}_2$.

Exercise 8.2 *Suppose that* $p = 19$, $k = 3$, $n = 6$, *and the public x-coordinates are* $x_i = i$, *for* $1 \leq i \leq 6$ *in a Shamir threshold scheme. Suppose that* $\mathcal{B} = \{P_2, P_3, P_6\}$ *pool their shares, which are 8, 18, and 11, respectively. Calculate the secret key* K.

Exercise 8.3 *Construct a perfect secret sharing scheme for the access structure*

$$\Gamma_0 = \{\{P_1, P_2, P_4, P_5\}, \{P_1, P_2, P_3, P_4\}, \{P_1, P_3\}, \{P_3, P_5\}\}.$$