Solution 7.1 We have $\mathcal{M} = \{$"Buy Volvo","Sell Volvo"$\}$ as plaintext set.

$$P_I = \frac{1}{4} \geq \frac{|\mathcal{M}|}{|\mathcal{C}|} \Rightarrow |\mathcal{C}| \geq 8$$

We shall choose a crypto with 8 different ciphertexts. If we make them binary we can make them as in the table to the right.

		Plaintext	
	Ciphertext	"Buy Volvo"	"Sell Volvo"
Key	0	000	001
	1	010	011
	2	101	100
	3	111	110

Solution 7.2 The system has four equiprobable keys, i.e., $f_K(k) = \frac{1}{4}\ \forall k$. Every ciphertext appears in two rows in the table. If an impersonator chooses a ciphertext randomly it will be accepted with probability $P_I = \frac{1}{2}$. Every ciphertext occurs in every column in the table. If a ciphertext is observed, the attacker can by looking at the rows in which the ciphertext occurs choose the most probable and in this way maximize the probability that a substitution will be accepted. This gives $P_S = \max f_M = 0.89$.

$$\left.\begin{array}{rl} P_I = & 2^{-I(\underline{C};\underline{K})} \\ I(\underline{C};\underline{K}) = & H(\underline{K}) - H(\underline{K} \mid \underline{C}) = 4\frac{1}{4}\log 4 - 4\frac{1}{4}h(0.89) = 1.5 \end{array}\right\} \Rightarrow P_I \geq 2^{-1.5} \simeq 0.35$$

Solution 7.3

a) We know that $P_D = \max(P_I, P_S) \geq \sqrt{P_I \cdot P_S}$. We have from the lower bounds that

$$P_I \cdot P_S \geq 2^{-I(\underline{C};\underline{K})} \cdot 2^{-H(\underline{K}|\underline{C})} = 2^{-H(\underline{K})}.$$

Since $H(\underline{K}) \leq \log|\mathcal{K}|$ it follows that

$$P_I \cdot P_S \geq \frac{1}{|\mathcal{K}|}$$

which gives

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

b) The ciphertext is generated as $\underline{c} = \underline{c}_1\underline{c}_2 = (m + k_1, mk_1 + k_2)$. We get the following table:

	$\underline{m}$ \ $\underline{c} = (c_1, c_2)$	00	01	10	11
$\underline{k} = (k_1, k_2)$	00	0	-	1	-
	01	-	0	-	1
	10	-	1	0	-
	11	1	-	-	0

Suppose $P(m = 0) = p$.
First we see that $P_I = 1/2$ since a ciphertext is always accepted in 2 cases out of 4. Further we see that

$$P_S = \max(p, 1 - p)$$

since if we have observed a ciphertext our best strategy is to guess that it was the most probable message that was sent in the ciphertext.

The squre root bound in a) gives $P_D \geq \frac{1}{\sqrt{4}} = \frac{1}{2}$. Thus, we have equality in a) if and only if $p = 1 - p = \frac{1}{2}$.

Solution 8.1

For an arbitrary field $\mathbb{F}_q, q > n$, Shamir's (k, n)-scheme can be described as follows.

D chooses n distinct elements in the field $\mathbb{F}_q$, denoted $x_i, 1 \leq i \leq n$.

1. D wishes to share the secret $K \in \mathbb{F}_q$. D chooses randomly $k-1$ elements in the field $\mathbb{F}_q$, denoted $a_1, a_2, ..., a_{k-1}$. Put $a_0 = K$.

2. D computes $y_i = a(x_i) \in \mathbb{F}_q$, for $1 \le i \le n$, where

$$a(x) = \sum_{j=0}^{k-1} a_j x^j.$$

3. D gives person P_i the part y_i.

A $(2,4)$-threshold scheme constructed over the field $\mathbb{F}_{2^3}$ with secret $K = 1$ and primitive polynomial $f(x) = x^3 + x + 1$, can for example be the following.

Construct the field using α s.t. $f(\alpha) = 0$ (see table). Since $k = 2$, the polynomial to use in the scheme is

$$a(x) = K + a_1 x = 1 + a_1 x.$$

For all $i \in \{1,2,3,4\}$ let the public shares $x_i = \alpha^i \in \mathbb{F}_{2^3}$. D chooses secretly $a_1 = \alpha^6$ or in polynomial notation $a_1 = \alpha^2 + 1$. D now has the polynomial

$$a(x) = 1 + \alpha^6 x.$$

D gives person 1 the part $y_1 = 1 + (\alpha^6)\alpha = 0$.
D gives person 2 the part $y_2 = 1 + (\alpha^6)\alpha^2 = 1 + \alpha^8 = 1 + \alpha = \alpha^3$.
D gives person 3 the part $y_3 = 1 + (\alpha^6)\alpha^3 = 1 + \alpha^9 = 1 + \alpha^2 = \alpha^6$.
D gives person 4 the part $y_4 = 1 + (\alpha^6)\alpha^4 = 1 + \alpha^{10} = 1 + \alpha^3 = \alpha$.

α^0	1
α^1	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$

Solution 8.2

We have the following parameters for a Shamir threshold scheme: $p = 19, x_i = i, \mathcal{B} = \{P_2, P_3, P_6\}$ and P_2, P_3, P_6 have the parts 8, 18 and 11. The secret follows from the expression

$$\begin{aligned}
K &= \sum_{i\in\mathcal{B}} y_i \prod_{j\in\mathcal{B}, j\neq i} \frac{x_j}{x_j - x_i} = \\
&= 8 \cdot \frac{3\cdot 6}{(3-2)\cdot(6-2)} + 18 \cdot \frac{2\cdot 6}{(2-3)\cdot(6-3)} + 11 \cdot \frac{2\cdot 3}{(2-6)\cdot(3-6)} \bmod 19 = \\
&= 8\cdot 18\cdot 4^{-1} + 18\cdot 12\cdot(-3)^{-1} + 11\cdot 6\cdot 12^{-1} \bmod 19 = \\
&= 8\cdot 18\cdot 5 + 18\cdot 12\cdot 6 + 11\cdot 6\cdot 8 \bmod 19 = \\
&= 17 \bmod 19.
\end{aligned}$$

Hence, the secret is 17.

Solution 8.3

We have $\Gamma_0 = \{\{P_1,P_2,P_4,P_5\}, \{P_1,P_2,P_3,P_4\}, \{P_1,P_3\}, \{P_3,P_5\}\}$. Suppose that $K \in \mathbb{Z}_m$. We use the following scheme.

We choose $a_1, a_2, a_3, a_4 \in \mathbb{Z}_m$ such that

$$K = a_1 + a_2 + a_3 + a_4.$$

We choose $b_1, b_2, b_3, b_4 \in \mathbb{Z}_m$ such that

$$K = b_1 + b_2 + b_3 + b_4.$$

We choose $c_1, c_2 \in \mathbb{Z}_m$ such that

$$K = c_1 + c_2.$$

We choose $d_1, d_2 \in \mathbb{Z}_m$ such that

$$K = d_1 + d_2.$$

We give P_1 the parts (a_1, b_1, c_1), P_2 the parts (a_2, b_2), P_3 the parts (b_3, c_2, d_1), P_4 the parts (a_3, b_4) and P_5 the parts (a_4, d_2). This gives a perfect scheme according to Benaloh and Leichter construction.

An even better solution is obtained if we observe that $\{P_1, P_3\} \subset \{P_1, P_2, P_3, P_4\}$ so a construction for $\Gamma_0' = \{\{P_1,P_2,P_4,P_5\}, \{P_1,P_3\}, \{P_3,P_5\}\}$ is sufficient, resulting in giving P_1 the parts (a_1, c_1) P_2 the parts (a_2), P_3 the parts (c_2, d_1), P_4 the parts (a_3) and P_5 the parts (a_4, d_2).