Solutions to final exam in CRYPTOGRAPHY on 15 December 1997.

Problem 1

a) $C = 1 + \alpha^6$ $\qquad K = 1 + \alpha + \alpha^2$

Determining K^{-1} using Euklides algorithm gives

$$\begin{aligned} K^{-1} &= \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha \\ M = CK^{-1} &= (1+\alpha^6)(\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha) \\ &= \alpha^4 + \alpha^3 + \alpha + 1 \end{aligned}$$

b) If $K = 0$, the encryption function is not injective, and one cannot decrypt.

Problem 2

The sequence s is $\underbrace{110010010100000110100}_{\text{period } 21}1100\ldots$.

Since $L(s) \leq L(s_1)L(s_2) = 3 \cdot 2 = 6$, the shortest LFSR is of length at most 6.

Using Massey's algorithm we get after 12 symbols

$$c(z) = 1 + z^{-1} + z^{-2} + z^{-4} + z^{-6}.$$

This must be correct, since if not, the next update of L will give an LFSR of length more than 6, a contradiction.

Problem 3

a) $H(S_i) = \log 30$ $\qquad H(M_j) = 3 \cdot H(S_i) = 3 \cdot \log 30.$

b) Number of different keys: $\phi(\phi(n)) - 1 = 11375$
$H(K) = \log 11375$
$D = \log 46918 - 3 \cdot \log 30$
$N_0 = \frac{H(K)}{D} \approx 16,9$ message symbols.

c) $H(K) = 0.$

d) For an RSA-system the secret key can be calculated from the public key. The security of RSA is instead based on the intractability of factoring the parameter n, which is assumed to be a very hard problem, even though this has not been proved.

e) $n = 46918 = 23459 \cdot 2$
$\phi(n) = 23458$
Find d with Euklides algorithm:
$23458 = 1 \cdot 20107 + 3351$
$20107 = 6 \cdot 3351 + 1$
$\Rightarrow$
$1 = 20107 - 6 \cdot 3351 = 20107 - 6 \cdot (23458 - 20107) = -6 \cdot 23458 + 7 \cdot 20107$
$\Rightarrow d = 7$
$D_k(10164) = 10164^7 \bmod 46918 = 10164 \cdot 40378 \cdot 29302 \bmod 46918 = 10$

Problem 4

a) One example is the following:
Let the key $K = (K_1, K_2), K_1, K_2 \in \mathbb{F}_3$.
Let $C = (C_1, C_2), C_1, C_2 \in \mathbb{F}_3$, and $M \in \mathbb{F}_3$.
Construct the cipertext as

$$C = (M, M \cdot K_1 + K_2).$$

b) P_S is given the secret S. Construct a $(2,3)$-threshold scheme for participants $\{P_{12}, P_3, P_4\}$. The share for P_{12} is Y_{12}. This is shared by P_1 and P_2 as

$$Y_{12} = Y_1 + Y_2,$$

where Y_1 is the share of P_1 and Y_2 is the share of P_2.

Problem 5

a) Decoding is done by taking the partial keys K_i in reversed order:

round	L_i	R_i
0	0010	1110
1	1110	1000
2	1000	1111
3	1111	0000
Message	0000	1111

b) $E(R_2) \oplus E(R_2^*) = 110011$ input x-or
$L_0 \oplus L_0^* \oplus R_3 \oplus R_3^* = 0011$ output x-or

c) Possible keys $= \{0?00110p, 1?11111p\} =$
$= \{00001101,$
$01001100,$
$10111111,$
$11111110\}$

d) We have two alternatives from **c)**.
By testing we find the key to be 11111110.
