Solutions to final exam in CRYPTOGRAPHY on 12 December 2000.

Problem 1
a)

$$mK = (\alpha, \alpha^2) \begin{pmatrix} \alpha^2 & \alpha+1 \\ \alpha^2+1 & 1 \end{pmatrix} = (1, \alpha).$$

b) If K is not invertible, unique decryption is not possible.

c)

$$|\mathcal{K}| = (q^2-1)(q^2-q),$$

where $q = 2^3$. It gives $H(K) = 11.78$, and $N_0 = \lceil 11.78/1 \rceil = 12$.

Problem 2
This is exactly the last exercise of Laboratory 1!

We construct two sequences, one over $\mathbb{Z}_2$ and one over $\mathbb{Z}_5$, which are combined through the Chinese remainder theorem to give a sequence over $\mathbb{Z}_{10}$.

We will receive a de Bruijn sequence if both sequences are de Bruijn. Let's start with the one over $\mathbb{Z}_2$. A de Bruijn sequence is obtained if we take a maximal length sequence (primitive feedback polynomial) and add the all zero state into the cycle. Take the primitive polynomial x^4+x+1 over $\mathbb{Z}_2$ as feedback polynomial. Then we have a state transition $1000 \to 0001$ which should be changed to the state transition $1000 \to 0000 \to 0001$. This is done by adding a nonlinear part f to the feedback. Let the LFSR state be denoted by s_3, s_2, s_1, s_0. Then $f(s_3, s_2, s_1, s_0) = s_2' s_1' s_0'$, where s_i' means inversion of the s_i variable.

Then we do the same for the sequence over $\mathbb{Z}_5$. Finally, we combine them. Let $\mathbf{u}$ be the de Bruijn sequence over $\mathbb{Z}_2$, and let $\mathbf{v}$ be the de Bruijn sequence over $\mathbb{Z}_5$. The resulting sequence w over $\mathbb{Z}_{10}$ is given by

$$w_i = 5 \cdot u + v.$$

DRAW A PICTURE, choose two starting states for the LFSRs, and produce 10 symbols of the sequence.

Problem 3
a)

C	$M=(0,0)$	$M=(0,1)$	$M=(1,0)$	$M=(1,1)$
$K=(0,0)$	$(0,0,0)$	$(0,1,0)$	$(1,0,0)$	$(1,1,0)$
$K=(0,1)$	$(0,0,0)$	$(0,1,1)$	$(1,0,1)$	$(1,1,0)$
$K=(1,0)$	$(0,0,1)$	$(0,1,1)$	$(1,0,1)$	$(1,1,1)$
$K=(1,1)$	$(0,0,1)$	$(0,1,0)$	$(1,0,0)$	$(1,1,1)$

$P_I = \frac{1}{2}$,

For all C we can find a ciphertext C' such that $P(C'\text{valid}|C) = 1$, e.g., $C = (0,0,0)$, $C' = (1,1,0)$. Thus, we get $P_S = 1$.

b) Since $k=3$ the secret polynomial is of the form $a(x) = a_0 + a_1 x + a_2 x^2$. The three shares give the following three equations,

$$\begin{aligned} a_0 + a_1 + a_2 &= 6, \\ a_0 + 3a_1 + 9a_2 &= 8, \\ a_0 + 5a_1 + 12a_2 &= 12. \end{aligned}$$

Solving this system of equations gives $a(x) = 9 + 10x^2$ and $K = a_0 = 9$.

Problem 4

a) Correct.

b) Correct, $p_2(z)$ primitive.

c) Wrong, $\mathbf{s_1} = [2]^\infty$.

d) Wrong, $L(\mathbf{s_1} + \mathbf{s_2}) \leq L(\mathbf{s_1}) + L(\mathbf{s_2}) = 1 + 3 = 4 < 6$.

e) Wrong, since $p_1(z)$ is not irreducible.

Problem 5

a) Two possible primes are $p = 4007$, $q = 4013$ giving $n = 16080091$. Since $gcd(3, \phi(n)) = 1$, we can choose $e = 3$.
public parameters: $(n, e) = (16080091, 3)$

b) $\phi(n) = (p-1)(q-1) = 16072072$

If we choose $e = 3$, then by using Euklides algorithm and Bezouts identity we get $d = 10714715$.
trapdoor parameters: $(\phi(n), d, p, q) = (16072072, 10714715, 4007, 4013)$

c)

$$D(E(M)) = C^d = (M^e)^d = M^{ed} = M^{1+k\phi(n)} = M \cdot (M^k)^{\phi(n)} = [\text{Euler}] = M \bmod n.$$
