Solutions to final exam in CRYPTOGRAPHY on 18 December 2001.

Problem 1

a)

$$S(z) = \frac{1 + 2z^{-2}}{1 - z^{-4}} = \frac{1}{1 + z^{-2}}.$$

Shortest LFSR is then $1 + z^{-2}$.

b) By Massey's algorithm we get $< C(z), L >=< 1 + 2z^{-1}, 3 >$.

Problem 2

a) $P_I = 2/5$.

b) $P_I \geq 2^{-I(C;K)} = \sqrt{2}/5$.

c) $P_I \geq 2^{-\inf I(C;K)} = 2/5$, (choose uniform message distribution).

d) $P_S = 0.89$.

e) We have perfecty secrect, since $I(M; C) = 0$.

Problem 3

Since $k = 2$ the secret polynomial is of the form $a(x) = a_0 + a_1 x$. The two shares give the two points $(\alpha^2, \alpha^5 + 1)$ and $(\alpha^3, \alpha + 1)$, which give the following system of equations over $\mathbb{F}_{2^8}$,

$$\begin{aligned} a_0 + \alpha^2 a_1 &= \alpha^5 + 1, \\ a_0 + \alpha^3 a_1 &= \alpha + 1. \end{aligned}$$

Solving for a_0, for example by multiplying first equation by α, gives

$$(\alpha + 1)a_0 = \alpha^6 + 1.$$

So $a_0 = (\alpha^6 + 1)(\alpha + 1)^{-1}$. Calculating $(\alpha + 1)^{-1}$ using Euclidean algorithm gives $(\alpha + 1)^{-1} = ...$, and finally $K = a_0 = ...$

Problem 4

a) Wrong, $N_0 = H(K)/D = \frac{64 \log 3}{\log 3 - 1.5}$.

b) Correct.

c) Correct.

d) Wrong, for perfect secrecy $H(K) \geq H(M)$.

e) Wrong, $K = (0, 0)$ is most probable.

Problem 5

a) A 64 bit plaintext that is cubed ($e = 3$) is a 192 bit number, much smaller than the

512 bit RSA number. This means that no modulo reduction occurs, and that the plaintext can be recovered by calculating the (ordinary) third root of C in $\mathbb{N}$. In the given example, $M = C^{1/3} = 1701$.

b) This is Phollard's $p-1$ facoring algorithm, which works when $p-1$ (or $q-1$) facors in only small prime powers.

Assume that $p_i^{e_i} \leq B$ for all i. Then $p-1|B!$ since the p_i's are distinct primes. Let $A = 2^{B!} \bmod n$. This means that $A \equiv 2^{B!} \pmod{n}$. Since $p-1|B!$ we have by Fermat's theorem $2^{B!} \equiv 1 \pmod{p}$. Since $p|n$ this means that $A \equiv 1 \pmod{p}$, or stated in other words, $A - 1 = p \cdot K$ for some K. But then p is a common factor in both $A-1$ and n, and since $A < n$ it can be calculated as $\gcd(A-1, n)$ unless $A = 1$.