Solutions to final exam in CRYPTOGRAPHY on 15 December 1998.

Problem 1

a)

$$H(M) = 3/2, H_0 = \log 3, D = H_0 - H(M) = \log 3 - 3/2.$$

NOw $H(K) = l$, $N_0 = l/D$ and we should have $N_0 > 200$, so

$$l > 200 \cdot D = 200 \cdot (\log 3 - 3/2) = 16.99.$$

Hence $l = 17$.

b) Use either homofonic coding or source coding. Homofonic coding: Construct a cipher with alphabet $\mathcal{M}'$ of size 4, e.g., $\mathcal{M}' = \{00, 01, 10, 11\}$. Then map the original source $\mathcal{M}$ to the new alphabet $\mathcal{M}'$ as follows. If $M = 0$ then choose $M' = 00$ with probability $1/2$ and $M' = 01$ with probability $1/2$. If $M = 1$ then choose $M' = 10$ and if $M = 2$ then choose $M' = 11$. Now $P(M') = 1/4$ and $H(M') = 2$, $H_0 = 2$ and $D = 0$ and $N_0 = \infty$.

Problem 2

a) A table of $\mathbb{F}_{2^3}$.

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

Using Massey's algorithm we get

$$c(z) = 1 + \alpha^5 z^{-1} + \alpha^6 z^{-2} + z^{-3}.$$

b) Multiplication of arbitrary element $\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2$ with α^6:

$$\alpha^6\beta = \beta_0(\alpha^2+1) + \beta_1 + \beta_2\alpha = \beta_0\alpha^2 + \beta_2\alpha + (\beta_0+\beta_1).$$

Similarly for α^5:

$$\alpha^5\beta = \beta_0(\alpha^2+\alpha+1) + \beta_1(\alpha^2+1) + \beta_2 = (\beta_0+\beta_1)\alpha^2 + \beta_0\alpha + (\beta_0+\beta_1+\beta_2).$$

DRAW A PICTURE!

Problem 3

a)

$$E(M) = M^e = 20000^{19} = 20000^{16+2+1} = 24067 \bmod 31897,$$

since $20000^2 = 11620$, $20000^4 = 4399$, $20000^8 = 21619$, $20000^{16} = 26317$.

b)

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

c) By Chinese remainder theorem, any $x \in \mathbb{Z}_n$ can be uniquely represented by $(x \bmod p, x \bmod q)$, for $n = pq$, p and q prime. Now $\gcd(M,n) \neq 1$, so we may assume $M = pa$ for some constant a. Now $M = pa$ is the element $(M \bmod p, M \bmod q) = (0 \bmod p, M \bmod q)$ and thus $M^{ed} \bmod n$ is $(0 \bmod p, M^{ed} \bmod q)$. But

$$M^{ed} = M^{1+\phi(n)\cdot K} = M \cdot (M^K)^{(p-1)(q-1)} = [\text{Fermat}] = M \bmod q,$$

and hence $M^{ed} \bmod n$ is $(0 \bmod p, M \bmod q)$ which is the element M.

Problem 4

a) Since $k=3$ the secret polynomial is of the form $a(x)=a_0+a_1x+a_2x^2$. The three shares give the following three equations.

$$\begin{aligned} a_0+a_1+a_2 &= 3 \\ a_0+4a_1+16a_2 &= 13 \\ a_0+7a_1+49a_2 &= 57 \end{aligned}$$

Solving this system of equations gives $a(x)=100+31x+39x^2$ and $K=a_0=100$.

b) Let $c=(m,t)$ and $c'=(m',t')$.

$$P_I=\max_c P(c \text{ valid})=\max_{m,t} P(m(k_1)+k_2=t)=\max_{m,t}\frac{|\{k_1,k_2: m(k_1)+k_2=t\}|}{2^{20}}=2^{-10}.$$

$$P_S=\sum_c P(c)\max_{c'} P(c' \text{ valid}|c \text{ valid})=\sum_{m,t} P(m,t)\max_{m',t'} P(m'(k_1)+k_2=t'|m(k_1)+k_2=t)=$$

$$\sum_{m,t} P(m,t)\max_{m',t'}\frac{|\{k_1,k_2: m(k_1)+k_2=t, m'(k_1)+k_2=t'\}|}{|\{k_1,k_2: m(k_1)+k_2=t\}|}=$$

$$\sum_{m,t} P(m,t)\max_{m'',t''}\frac{|\{k_1,k_2: m(k_1)+k_2=t, m''(k_1)=t''\}|}{2^{10}}=\max_{m'',t''}\frac{|\{k_1: m''(k_1)=t''\}|}{2^{10}}=\frac{3}{2^{10}},$$

where $m''=m'-m$, $t''=t'-t$ and the condition above is $m\neq m'$ (or $m''\neq 0$). Equality in the last step follows from the fact that a polynomial m'' with three zeros can always be found.

Problem 5

a) WRONG $p_1(z)=(z^{-3}+z^{-2}+1)^2$

b) WRONG $1(1)\bigoplus 1(7)\bigoplus 4(14)$

c) WRONG $p_2(z)$ is primitive.

d) CORRECT.

e) CORRECT If $p(\alpha)=0$ then $\mathrm{ord}(\alpha)|2^7-1=127$. But 127 is a prime and thus $\mathrm{ord}(\alpha)=127$.