Solutions to final exam in CRYPTOGRAPHY on 16 December 1996

Problem 1

a) $H_0 = \log 17$, $H(M) = 3$, $H(\underline{K}) = \log 17$, $D = H_0 - H(M) = 4.09 - 3 = 1.09$, and $N_0 = H(\underline{K})/D = 4.09/1.09 = 3.75$.

b)

$$K = \sum_i y_i \prod_{j, j \neq i} x_j/(x_j - x_i) = 7\frac{2}{2-1}\frac{3}{3-1} + 11\frac{1}{1-2}\frac{3}{3-2} + 0\frac{1}{1-3}\frac{2}{2-3} = 5 \pmod{17}.$$

Problem 2

a) WRONG, since $p_1(x) = (x^2 + x + 1)^2$.

b) WRONG, since the cycles are $1(1) \oplus 1(3) \oplus 2(6)$.

c) CORRECT, since $S_1 \otimes S_2 = (1(1) \oplus 1(3) \oplus 2(6)) \otimes (1(1) \oplus \ldots)$.

d) CORRECT, since $p_1(x)$ generates the sequence and since the sequence starts with three 0's the length must be at least 4.

e) CORRECT, since $2^7 - 1 = 127$, a prime, and $\text{ord}(\alpha)|127$ for $p_2(\alpha) = 0$.

Problem 3

We get the following table:

A	0	0	F	α^4	$2\alpha+2$	L	α^9	$3\alpha+1$	Q	α^{14}	$4\alpha+2$	V	α^{19}	3α
B	1	1	G	α^5	$4\alpha+1$	M	α^{10}	$3\alpha+1$	R	α^{15}	$\alpha+2$	W	α^{20}	$3\alpha+4$
C	α	α	H	α^6	2	N	α^{11}	$3\alpha+2$	S	α^{16}	$3\alpha+3$	X	α^{21}	$2\alpha+4$
D	α^2	$\alpha+3$	I,J	α^7	2α	O	α^{12}	4	T	α^{17}	$\alpha+4$	Y	α^{22}	$\alpha+1$
E	α^3	$4\alpha+3$	K	α^8	$2\alpha+1$	P	α^{13}	4α	U	α^{18}	3	Z	α^{23}	$2\alpha+3$

The first five known letters of the plaintext gives us the first five symbols of the key sequence by $K_i = C_i - M_i$. So

$$(K_1, \ldots, K_5) = (1, \alpha, \alpha^7, \alpha^{13}, \alpha^{19}).$$

Using Massey's algorithm, we get $C(z) = 1 - \alpha^6 z^{-1}$ and $L = 2$. This must be a correct LFSR, since if not, then $d \neq 0$ for the sixth symbol and we would need a LFSR of length $6 - 2 = 4$ to generate the sequence, a contradiction.

Problem 4

a)

$$\begin{aligned} D_K(E_K(M)) &= (M^e)^d \pmod n \\ &= M^{ed} \pmod n \\ &= M^{1+\phi(n)} \pmod n \\ &= M \cdot M^{\phi(n)} \pmod n \\ &= M, \end{aligned}$$

since $M^{\phi(n)} = 1 \pmod n$ by Euler's theorem.

b) First, we calculate d to be 107. Then

$$\begin{aligned} D_K(E_K(22)) &= (22^3)^{107} \pmod{187} \\ &= 176^{107} \pmod{187} \\ &= 176 \cdot 176^2 \cdot 176^8 \cdot 176^{32} \cdot 176^{64} \pmod{187} \\ &= 176 \cdot 121 \cdot 33 \cdot 154 \cdot 154 \pmod{187} \\ &= 22 \pmod{187} \end{aligned}$$

c) $\phi(\phi(n)) = \phi((p-1)(q-1)) = \phi(4p_1q_1) = 2(p_1-1)(q_1-1)$.

d) If we can find $\phi(n)$ we have two equations $n = pq$ and $\phi(n) = (p-1)(q-1)$ in two unknowns. Hence we can solve for p or q. For example, put $q = n/p$ in the second equation and we obtain $\phi(n) = (p-1)(n/p-1)$, or $p^2 + p(\phi(n) - n - 1) + n = 0$. Showing vice versa is trivial.

Problem 5

a) 00000000

b) the same as encryption, but using partial key K_{3-i} in round i. For a formal derivation, see home exercise in DES laboratory lesson.

c) input x-or $= E(L_3) \oplus E(L_3^*) = 101010$. Output x-or $= R_3' \oplus L_0' = 1001$. There are 64 pairs $(B \oplus K_3, B \oplus K_3 \oplus 101010)$ with input x-or 101010 but only a few of them has output x-or 1001. These can be calculated from S and by subtracting $B = E(L_3)$ from the one coordinate, we get all possible values of K_3.