Solutions to final exam in CRYPTOGRAPHY on 17 December 2002.

Problem 1

a) Unicity distance $N_0 = H(K)/D$

$$\begin{aligned}
H(K) &= H(k_1, k_2, k_3) = 3 \\
D &= H_0 - H_\infty = H_0 - H(M) \\
H_0 &= \log 3 \\
H(M) &= -\tfrac{1}{2}\log\tfrac{1}{2} - p \cdot \log p - (\tfrac{1}{2} - p)\log(\tfrac{1}{2} - p) \\
&= \tfrac{1}{2} - p\log 2p - \tfrac{1}{2}(1-2p)\log(1-2p) + p + \tfrac{1}{2} - p \\
&= 1 + \tfrac{1}{2}(-2p\log 2p - (1-2p)\log(1-2p)) \\
&= 1 + \tfrac{1}{2}h(2p) \\
D &= \log 3 - (1 + \tfrac{1}{2}h(2p))
\end{aligned}$$

So, $\frac{3}{\log\frac{3}{2} - \frac{1}{2}h(2p)} > 20$, or $3 > 20 \cdot (\log\frac{3}{2}) - \frac{1}{2}h(2p))$

hence, $h(2p) > \frac{20 \cdot \log\frac{3}{2} - 3}{20 - \frac{1}{2}} = 2\log\frac{3}{2} - \frac{3}{10} \approx 0.58^5 \cdot 2 - 0.3 = 1.17 - 0.3 = 0.87$

$h(2p) = 0.87 \Rightarrow 0.291 \leq 2p \leq 0.709 \Rightarrow 0.15 \leq p \leq 0.35$

$2p = 0.709$

(6p)

b) When $p = 0$, $P(M = 1) = 0$.

There are only two possible plaintexts $M = 0$ and $M = 2$.

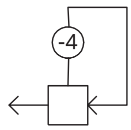
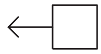
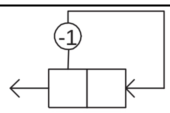
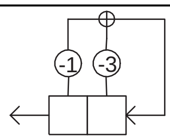
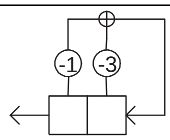
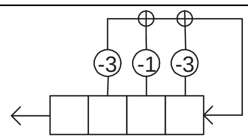
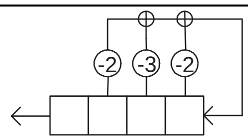
Let $\phi(M) = \begin{cases} 0, \text{ if } M = 0 \\ 1, \text{ if } M = 2 \end{cases}$

Then $C_i = \phi(M_i) + K_{i \bmod 3} (\mathrm{mod} 2)$ has infinite unicity distance.

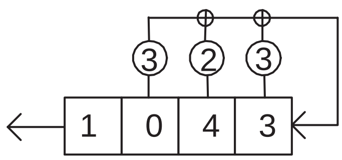
(4p)

Problem 2

a) The sequence is $s = (1, 0, 4, 3, 2, 4, 0)$ over $\mathbf{F}_5$. To find the shortest linear feedback shift register we use Massey's algorithm:

S_N	d	$C_1(z)$	$C(z)$	L	Shift Register	$C_0(z)$	d_0	e	N
–	–	–	1	0	$\leftarrow$	1	1	1	0
1	1	1	$1 + 4z^{-1}$	1		1	1	1	1
0	4	$*$	1	$*$		$*$	$*$	2	2
4	4	1	$1 + z^{-2}$	2		1	4	1	3
3	3	$*$	$1 + 3z^{-1} + z^{-2}$	$*$		$*$	$*$	2	4
2	0	$*$	$*$	$*$		$*$	$*$	3	5
4	3	$1 + 3z^{-1} + z^{-2}$	$1 + 3z^{-1} + z^{-2} + 3z^{-3}$	4		$1 + 3z^{-1} + z^{-2}$	3	1	6
0	3	$*$	$1 + 2z^{-1} + 3z^{-2} + 2z^{-3}$	$*$		$*$	$*$	2	7

So the final shift feedback register looks like that:

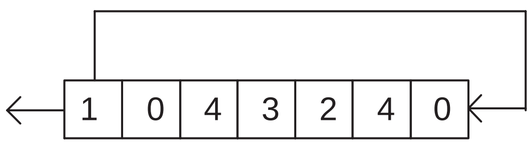


(6p)

b) The sequence is $s = [1, 0, 4, 3, 2, 4, 0]^\infty$ over $\mathbf{F}_5$.

$$S(z) = \frac{P(z)}{C(z)} = \frac{1 + 4z^{-2} + 3z^{-3} + 2z^{-4} + 4z^{-5}}{1 - z^7}$$

Since $\gcd(P(z), C(z)) = 1$, then the shortest linear feedback shift register is



(4p)

Problem 3

a) The "ciphertext" is given as the plaintext and one parity check symbol t.

$$P_I = \max_C P(\ C \text{ accepted })$$

Note that a ciphertext is accepted only if

$$t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3$$

holds. Suppose $C = (m_1, m_2, m_3, t)$. Then

$$P(C \text{ accepted}) = P(t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3) =$$

$$= \frac{\begin{pmatrix} \text{Number of choices of } (k_1, k_2) \text{ such that} \\ t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3 \text{ holds} \end{pmatrix}}{\text{Total number of choices of } (k_1, k_2)} = \frac{13}{13^2} = \frac{1}{13}$$

Thus $P_I = \frac{1}{13}$.

(5p)

b) Suppose $C = (m_1, m_2, m_3, t)$ was sent and it is replaced by $C' = (m_1', m_2', m_3', t')$. Then $P(C'$ accepted $|C$ observed $)=$

$$= \frac{\left(\text{Number of keys } (k_1, k_2) \text{ for which } \begin{cases} t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3 \\ t' = k_1 + m_1' k_2 + m_2' k_2^2 + m_3' k_3^3 \end{cases} \right)}{\text{Number of keys } (k_1, k_2) \text{ for which } t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3} =$$

$$= \frac{\left| \left\{ (k_1, k_2) : \begin{cases} t = k_1 + m_1 k_2 + m_2 k_2^2 + m_3 k_3^3 \\ t' - t = k_1 + (m_1' - m_1) k_2 + (m_2' - m_2) k_2^2 + (m_3' - m_1) k_3^3 \end{cases} \right\} \right|}{13} =$$

$$= \left[\begin{array}{l} \text{For each value of } k_2 \text{ there is an unique value of } k_1 \\ \text{such that first equation is true} \end{array} \right] =$$

$$= \frac{\left| \{ k_2 : t'' = k_2 m_1'' + k_2^2 m_2'' + k_3^3 m_3'' \} \right|}{13} =$$

$$= \left[\begin{array}{l} \text{According to the hint, the equation above has at most three solutions.} \\ \text{And for any } C \text{ we can select } C' \text{ such that we have three solutions.} \end{array} \right] =$$

$$= \frac{3}{13}.$$

Then $P_S = \sum\ f(C) \cdot P(C' \text{ accepted} | C \text{ observed})\ = \frac{3}{13}$

(5p)

Problem 4

a) If $p(x)$ is not irreducible, it must be divisible by a polynomial of degree at most two. So we check $p(0) = p(1) = 1$ and since $x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $\mathbf{F}_2$, then we check $(x^2 + x + 1) \nmid (x^5 + x^2 + 1)$.

(4p)

b) Let $p(\alpha) = 0$. We know that $\mathrm{ord}(\alpha)|(2^5 - 1)$, and since 31 is prime, then $\mathrm{ord}(\alpha) = 31$, which implies $p(x)$ primitive.

(3p)

c) p(x) as a polynomial over $\mathbf{F}_2$ can be used to construct $\mathbf{F}_{2^5}$ with $\alpha^5 = \alpha^2 + 1$.
If $p(x)$ is a polynomial over the field $\mathbf{F}_{2^5}$, then $p(\alpha) = \alpha^5 + \alpha^2 + 1 = 0$ and α is a root of $p(x)$. Thus $p(x) = (x + \alpha)q(x)$ for some $q(x)$.

(3p)

Problem 5

a) THE PRESIDENT WILL SEND THE MONEY

(5p)

b) By definition, a transposition cipher permute the order in which the letters are written. In the lecture notes, columnwise transposition is demonstrated, but this is not the case here, according to the hint.

A regular transposition cipher just permutes letters inside a block. Then let us try different block sizes $3, 4, 5, \ldots$
For block size 5 we find:

OYORT ETDNS

In the second block, SEND looks like a possible word. This gives us the blockwise map

$$(M_1 M_2 M_3 M_4 M_5) \to (M_5 M_1 M_4 M_3 M_2)$$

and the plaintext is

TO ROY SEND THE TROUPS TONIGHT

(5p)
