Problem 1

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

$$
\begin{aligned}
H(K) &= \log_2(3^{64}) \\
D &= H_0 - H_\infty = H_0 - H(M) \\
H_0 &= \log_2 3 \\
H(M) &= 3/2 \\
D &= \log_2 3 - 3/2
\end{aligned}
$$

So, the unicity distance is $N_0 = \frac{H(K)}{D} = \frac{\log_2(3^{64})}{\log_2 3 - 3/2} \approx 1194.$

(5p)

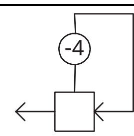
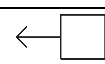
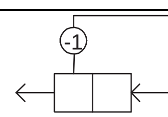
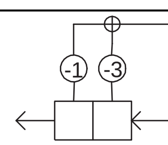
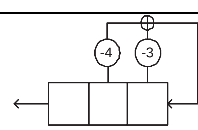
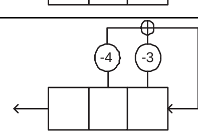
b) Perfect secrecy $\Rightarrow I(H;C) = 0$. This is true for $l \geq 3$ because it is "one time pad" Vernem cipher (see the book).

Study $l = 2$: For perfect secrecy $H(K) \geq H(M)$. But: $\left\{ \begin{array}{rcl} H(K) & = & l \cdot \log 3 \\ H(M) & = & 3 \cdot 1.5 \end{array} \right.$ $\Rightarrow$ no perfect secrecy for $l \leq 2$.

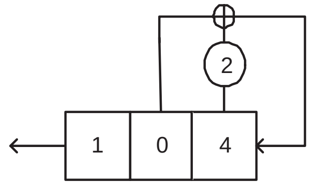
(5p)

Problem 2

a) The sequence is $s = (1, 0, 4, 3, 0, 3)$ 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	←	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
0	3	$1 + 3z^{-1} + z^{-2}$	$1 + 3z^{-1} + 4z^{-2}$	3		$1 + 3z^{-1} + z^{-2}$	3	1	5
3	0	$*$	$*$	$*$		$*$	$*$	2	6

So the final shift feedback register looks like that:

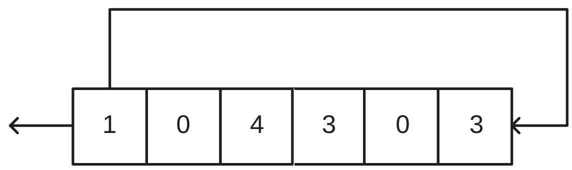


(5p)

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

$$S(z) = \frac{P(z)}{C(z)} = \frac{1 + 4z^{-2} + 3z^{-3} + 3z^{-5}}{1 - z^6}$$

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



(5p)

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

$$t = k_1 + m_1 k_2 + m_2 k_2^2$$

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

$$P(C \text{ accepted}) = P(t = k_1 + m_1 k_2 + m_2 k_2^2) =$$
$$= \frac{\left(\begin{array}{l}\text{Number of choices of } (k_1, k_2) \text{ such that} \\ t = k_1 + m_1 k_2 + m_2 k_2^2 \text{ holds}\end{array}\right)}{\text{Total number of choices of } (k_1, k_2)} = \frac{3}{3^2} = \frac{1}{3}$$

Thus $P_I = \frac{1}{3}$.

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

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

$$= \frac{\left| \left\{ (k_1, k_2) : \left\{\begin{array}{l} t = k_1 + m_1 k_2 + m_2 k_2^2 \\ t' - t = (m_1' - m_1) k_2 + (m_2' - m_2) k_2^2 \end{array}\right. \right\} \right|}{3} =$$

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

$$= \frac{|\ \{k_2 : t'' = k_2 m_1'' + k_2^2 m_2''\}\ |}{3} =$$

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

$$= \tfrac{2}{3}.$$

Then $P_S = \sum f(C) \cdot P(C' \text{ accepted}|C \text{ observed}) \ = \frac{2}{3}$

(5p)

b) In the Shamir scheme (3,5) over $\mathbf{F}_{97}$ the secret key $K = a_0$. We assume that $x_i = i$, then:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} a_0 + a_1 x_1 + a_2 x_1^2 \\ a_0 + a_1 x_2 + a_2 x_2^2 \\ a_0 + a_1 x_3 + a_2 x_3^2 \end{pmatrix} = \begin{pmatrix} 44 \\ 73 \\ 28 \end{pmatrix},$$

which transforms to the linear system of equations

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 44 \\ 1 & 2 & 4 & 73 \\ 1 & 3 & 9 & 28 \end{array} \right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 38 \\ 0 & 1 & 0 & 43 \\ 0 & 0 & 1 & 60 \end{array} \right).$$

Hence, the key $K = 38$.

(5p)

Problem 4

a) We want to factor the RSA number $n = p \cdot q = 3844384501$, given that $3117761185^2 \equiv 1(\mathrm{mod} 3844384501)$.

Note that: $(3117761185 - 1) \cdot (3117761185 + 1) \equiv 0(\mathrm{mod} n)$, then:

$$\begin{aligned} p =& \gcd(3117761184, 3844384501) = 67801 \\ q =& \frac{n}{p} = 56701 \end{aligned}$$

(5p)

b) We want to prove that $n = 31803221$ is not a prime number, given that $2^{n-9} \equiv 27696377(\bmod n)$. By the little Fermat's theorem for any prime number p and $a \in \mathbf{Z}_p \Rightarrow a^{p-1} \equiv 1(\mathrm{mod} p)$.

By testing: $2^{n-9} \cdot 2^8 \equiv 27696377 \cdot 256 \equiv 29957450 \not\equiv 1(\bmod 31803221)$. Hence, n is not a prime number!

(5p)

Problem 5

Given $p(\alpha) = \alpha^2 + \alpha + 2 = 0$ over $\mathbf{F}_3$ is the generating polynomial of the field $\mathbf{F}_{3^2}$, we want to find the cycle characteristic of the polynomial $q(x) = x^3 + (\alpha+1)x^2 + (\alpha+1)x + 1$

1. Make the table of powers α^k, to make futher calculations easy:
   $p(\alpha) = \alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha^2 = -\alpha - 2 = 2\alpha + 1$

$$\begin{array}{ll} \alpha^1 = \alpha & \alpha^5 = 2\alpha \\ \alpha^2 = 2\alpha + 1 & \alpha^6 = \alpha + 2 \\ \alpha^3 = 2\alpha + 2 & \alpha^7 = \alpha + 1 \\ \alpha^4 = 2 & \alpha^8 = 1 \end{array}$$

2. Factor $q(x) = (x+a)(x^2 + bx + c)$ over $\mathbf{F}_{3^2}$, where $a, b, c \in \mathbf{F}_{3^2}$ – are some constants.

$$\left\{ \begin{array}{rcl} a+b & = & \alpha+1 \\ c+ab & = & \alpha+1 \\ ac & = & 1 \end{array} \right. \rightarrow \left\{ \begin{array}{l} a = c = 1 \\ b = \alpha \end{array} \right. \rightarrow q(x) = (x+1)(x^2 + \alpha x + 1),$$

   where $(x^2 + \alpha x + 1)$ is irreducible, since $\left\{ \begin{array}{r} ab{=}1 \\ a+b{=}\alpha \end{array} \right.$ has no solutions in $\mathbf{F}_{3^2}$.

3. Find cycle characteristic for $(x+1)$ by division:

$$\begin{array}{l|l} 1{+}2x & \overline{\;1{+}x\;} \\ \hline & 1 \\ & \underline{-(1{+}x)} \\ & \quad 2x \\ & \quad \underline{-(2x{+}2x^2)} \\ & \qquad\quad x^2 \quad \Rightarrow T = 2 \end{array}$$

   Thus, cycle characteristic is $1(1) \oplus 4(2)$.

4. Find cycle characteristic for $(x^2 + \alpha x + 1)$ through $T = \mathrm{ord}(\beta = \mathrm{RootOf}(x^2 + \alpha x + 1))$. The number of elements in the extension field $\mathbf{F}_{(3^2)^2}$ is $3^4 = 81$. Therefore, by the Lagrange's theorem, the order of β must divide $80 = 2^4 \cdot 5$!

$$\begin{aligned} \beta^1 &= x \\ \beta^2 &= -\alpha x - 1 = 2\alpha x + 2 \\ \beta^4 &= (\beta^2)^2 = (2\alpha x + 2)^2 = x + \alpha \\ \beta^8 &= (\beta^4)^2 = (x+\alpha)^2 = \alpha x + 2\alpha \\ \beta^{16} &= (\beta^8)^2 = (\alpha x + 2\alpha)^2 = 2x \\ \beta^5 &= \beta^4 \cdot \beta^1 = (x+\alpha) \cdot x = 2 \\ \beta^{10} &= \beta^8 \cdot \beta^2 = (\alpha x + 2\alpha) \cdot (2\alpha x + 2) = 1(!) \\ & \ldots \text{stop!} \end{aligned}$$

   The order of β is $T = 10$. Hence, the cycle characteristic is $1(1) \oplus 8(10)$.

5. Find the cycle characteristic for $q(x)$ by multiplication:
   $(1(1) \oplus 4(2)) \otimes (1(1) \oplus 8(10)) = 1(1) \oplus 8(10) \oplus 4(2) \oplus 64(10) = 1(1) \oplus 4(2) \oplus 72(10)$