Problem 1

(a) WRONG (For example, since $P_1(0) = 0$)
(b) WRONG (Since $P_1(2) = 0$)
(c) WRONG (P_2 is irreducible over $\mathbb{F}_3$, so $\mathbb{F}_{3^2}$ is generated by P_2 and $P_2(\alpha) = 0$.)
(d) WRONG (the period of the polynomial is computed to be 4)
(e) CORRECT (test with starting state $(1, 0, 0)$ or compute the full cycle set)

Problem 2

(a) Given formulas:

$$D = H_0 - H(M),$$

$$N_0 = H(K)/D.$$

Computing

$$H_0 = \log L = \log 4 = 2.$$

Message symbols are pairwise independent, and $H(M_i, M_{i+1}) = \log 4 = 2$ so

$$H(M) = H(M_0M_1 \cdots M_{63})/64 = (H(M_0M_1) + \ldots + H(M_{62}M_{63}))/64 = 32 \cdot 2/64 = 1.$$

$$H(K) = \log(|\mathcal{K}|) = \log(4^{64}) = 128.$$

Finally,

$$N_0 = H(K)/D = \frac{128}{(2-1)} \approx 128 \text{ symbols.}$$

The unicity distance is roughly the number of ciphertext symbols Eve needs in order to be able to uniquely determine the key in the information-theoretic Shannon model, which assumes ciphertext-only attacks.

(b) Considering again a pair of equations $C_i = M_i + K_i$ and $C_{i+1} = M_{i+1} + K_{i+1}$, we see that $M_i = M_{i+1}$ is an independent uniformly distributed random variable. So each pair gives us the equation $C_i - C_{i+1} = K_i - K_{i+1}$. After $2l$ symbols the right hand side will repeat. So it is enough to examine the system of linear equations given by l such equations. For l even is is obvious that there is no unique solutions (the corresponding matrix is not of full rank). For l odd we get the equations

$$\begin{pmatrix} 1 & -1 & \ldots & & & & \\ & & 1 & -1 & \ldots & & \\ & & & & \ddots & & \\ -1 & & & & \ldots & & 1 \\ & 1 & -1 & & \ldots & & \\ & & & \ldots & 1 & -1 & \end{pmatrix} \mathbf{K}^T = \hat{\mathbf{C}}.$$

Again, the matrix is not of full rank over $\mathbb{Z}_4$ and there is no unique solution for the key. Recall, N_0 is only a bound!

(c) If we want a new scheme with perfect secrecy, one could use the same key value for K_i and K_{i+1}. So use $\mathbf{K}' = (K'_0, K'_1, \ldots, K'_{l/2})$, for l even and set $K_{2i} = K_{2i+1} = K'_i$.

Problem 3

(a)

$$S(D) = \frac{1+D}{1+D^3} + \frac{1}{1+D^2} = \frac{D+D^2}{1+D^2+D^3+D^5}.$$

Computing gcd gives $\gcd(D+D^2, 1+D^2+D^3+D^5) = 1+D$ and

$$S(D) = \frac{D}{1+D+D^3+D^4}.$$

Shortest LFSR is then $1+D+D^3+D^4$.

(b) Direct use of B-M algorithm. It is useful to have a table of $\mathbb{F}_{2^4}$ for arithmetics!

s_N	d	$C_1(D)$	$C(D)$	L	LFSR	$C_0(D)$	d_0	e	N
$-$	$-$	$-$	1	0	$\leftarrow$	1	1	1	0
1	1	1	$1+D$	1	picture	1	1	1	1
α	$\alpha+1$		$1+\alpha D$		picture			2	2
α^2	0							3	3
α^{11}	α^5	$1+\alpha D$	$1+\alpha D+\alpha^5 D^3$	3	picture	$1+\alpha D$	α^5	1	4
α^{14}	α^9		$1+D+\alpha^2 D^2+\alpha^5 D^3$		picture			2	5
α^6	α^6		$1+D+\alpha^2 D^2+\alpha D^3$		picture			3	6
1	0		$1+D+\alpha^2 D^2+\alpha D^3$		picture			2	5

So shortest LFSR is then $1+D+\alpha^2 D^2+\alpha D^3$.

Problem 4

(a) Compute $6038438^2 = 13 \bmod 21769199$. In the same way, $10816226^2 = 17$, $13211263^2 = 3$, $4653427^2 = 16369054$, $21591962^2 = 12$, and $10795981^2 = 3$. We need to create a relation of the form $x^2 = y^2 \bmod n$, so

$$(13211263 \cdot 10795981)^2 = 3^2 \bmod 21769199$$

and from project 1 we know that by computing $\gcd(x - y, n)$ we have a chance of finding a factor. In our case $\gcd(17865853 - 3, 21769199) = 4523$ and we have found that $n = 4523 \cdot 4813$.

Problem 5

(a) The tag is $t = e_1 + s_1 e_2 + s_2 e_2^2$. We have observed $M = (0, 0, 10)$ which means that we learn that $e_1 = 10$. From the second channel message $M = (1, 0, 12)$ we learn $10 + 1 \cdot e_2 + 0 \cdot e_2^2 = 12$ which means that $e_2 = 2$. Having completely determined the key from these two channel messages, we can generate a correct tag for any message, for example $M = (0, 1, e_1 + 0 \cdot e_2 + 1 \cdot e_2^2)$ which gives $M = (0, 1, 14)$ and will be accepted with probability 1.

(b) If Eve knows the correct tag for two messages (m, t) and (m', t') a third message m'' can be built whose CBC-MAC will also be t'. This is simply done by XORing the first block of m' with t and then concatenating m with this modified m'; i.e., by making $m'' = m||[(m'_1 \oplus t)||m'_2|| \ldots ||m'_x]$ with tag $t'' = t'$. It also work with a single message by setting $m = m'$ and $t = t'$.

(c) The Merkle-Damgard construction of a hash function $h(x)$ uses a compression function $f(x)$ which operates on blocks of the message $\mathbf{m} = M_1||M_2|| \cdots ||M_n$ by $X_i = f(M_i, X_{i-1})$ and $h(\mathbf{m}) = \mathbf{X_n}$. By the proposed construction, given $(\mathbf{m}, MAC)$, Eve can just add one more block M_{n+1} to the message and compute a new MAC value as $f(M_{n+1}, MAC)$.