Problem 1

(a) WRONG (For example, since $P_1(1) = 0$)

(b) WRONG (Since $P_1(2) = 0$)

(c) WRONG (the period is 4)

(d) CORRECT (check that $P_2(x)$ is irreducible + observe that ord$(\alpha) \in \{1, 7\}$ and it is not 1)

(e) CORRECT (Compute the cycle set: factored polynomials: $P_1 = (1+D)^3$, $P_2(D) = x^3 + x+1$. Then $S_1 = 2(1)\oplus 1(2)\oplus 1(4)$ according to the cycle set formula and $S_2 = 1(1)\oplus 1(7)$. Finally compute $S = S_1 \otimes S_2$ or observe directly that there will be one cycle of length 14. $S = [2(1) \oplus 1(2) \oplus 1(4)] \otimes [1(1) \oplus 1(7)] = 2(1) \oplus 2(7) \oplus 1(2) \oplus 1(14) \oplus 1(4) \oplus 1(28)$

Problem 2

(a) Given formulas:

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

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

Computing

$$H_0 = \log L = \log 5.$$

$$H(M) = -3/4 \log(1/4) - 2/8 \log(1/8) = 9/4.$$

$$H(K) = \log(|\mathcal{K}|) = \log(5^2) = 2 \log 5.$$

Finally,

$$N_0 = H(K)/D = \frac{2 \log 5}{(\log 5 - 9/4)} \approx 64 \text{ symbols.}$$

(b) $n \in \{1, 2\}$, since perfect secrecy requires $H(K) \geq H(M_1 \cdots M_n)$, so $n \leq 2$ and for $n \in \{1, 2\}$ it is a Vernam cipher which is know to have perfect secrecy.

(c) We note that $P(C = c) = P(i \text{ even})P(M+K_0 = c)+P(i \text{ odd})P(M+K_1 = c) = (P(M+K_0 = c) + P(M + K_1 = c))/2$. So if empirically $P(C = 2) \approx 1/4$ and $P(C = 3) \approx 1/4$ then most likely $P(M + K_0 = 2) = 1/4$, $P(M + K_1 = 2) = 1/4$, $P(M + K_0 = 3) = 1/4$, $P(M + K_1 = 3) = 1/4$. So both $2 - K_0$ and $3 - K_0$ must be among the most probable symbols (0,1,2), giving $K_0 \in \{1, 2\}$. Same for K_1. Finally, matching with the remaining knowledge given in the problem, we see that the two possible keys are $(1, 2)$ or $(2, 1)$.

(d) It is a better way is to record the number of occurences for each alphabet, in this case in two tables, one for even i and one for odd i.

Problem 3

(a) We have $k = 4$ and so we have an unknown polynomial $a(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ over $\mathbb{F}_{37}$. We know the following system of linear equations:

$$\begin{aligned} 3 &= a_0 + 2a_1 + 4a_2 + 8a_3 \\ 10 &= a_0 + 3a_1 + 9a_2 + 8a_3 \\ 6 &= a_0 + 4a_1 + 16a_2 + 7a_3 \\ 6 &= a_0 + 7a_1 + 11a_2 + a_3 \end{aligned}$$

Solving steps:

$$\left(\begin{array}{cccc|c} 1 & 2 & 4 & 8 & 3 \\ 1 & 3 & 9 & 8 & 10 \\ 1 & 4 & 16 & 7 & 6 \\ 1 & 7 & 11 & 1 & 6 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & 4 & 8 & 3 \\ 0 & 1 & 5 & 0 & 7 \\ 0 & 2 & 12 & 18 & 3 \\ 0 & 5 & 7 & 12 & 3 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & 4 & 8 & 3 \\ 0 & 1 & 5 & 0 & 7 \\ 0 & 0 & 2 & 18 & 8 \\ 0 & 0 & 1 & 12 & 6 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & 4 & 8 & 3 \\ 0 & 1 & 5 & 0 & 7 \\ 0 & 0 & 2 & 18 & 8 \\ 0 & 0 & 0 & 6 & 4 \end{array}\right).$$

So $6a_3 = 4$ gives $a_3 = 7$. More calculations give $a_2 = 17$, $a_1 = 17$, and finally $K = a_0 = 16$. The answer is $K = 16$.

(b) Eve observes $M = (0, 0, 0, 9)$ leading to knowledge of e_1 since $t = e_1 + s_1e_2 + s_2e_2^2 + s_3e_2^3$ and so $9 = e_1 + 0 \cdot e_2 + 0 \cdot e_2^2 + 0 \cdot e_2^3$ and $e_1 = 9$. Now

$$P_S = \max_{M'} P(M' \text{ valid} | (0,0,0,9) \text{ observed}) = \max_{M'} \frac{\text{Number of } e_2 \text{ for which } M' \text{ is valid}}{\text{Total Number of } e_2 \text{ values}}$$

The condition for M' to be valid is $t = 9 + s_1e_2 + s_2e_2^2 + s_3e_2^3$ for the choice of t. Because this is a degree 3 polynomial in the unknown e_2, it can have at most three solutions. So the maximum P_S is $3/37$ and we just need to find a message M' giving this probability. Putting $t = 9$, we have the condition $s_1e_2 + s_2e_2^2 + s_3e_2^3 = 0$ and we should then choose (s_1, s_2, s_3) such that this equation has three solutions. So for example $e_2(e_2+1)(e_2+2) = 2e_2 + 3e_2^2 + e_2^3$ has three solutions, so we can set $M' = (2, 3, 1, 9)$.

Problem 4

(a) In ECB mode, the plaintext is split in blocks and each block is encrypted with the block cipher, $M = M_1, M_2, \cdots$ and $C = C_1, C_2, \ldots$, where $C_i = E_K(M_i)$. It is not a good choice because if two blocks in the plaintext are the same, then so are the corresponding ciphertext blocks. In this case, if the first two ciphertext blocks are the same, Eve knows that it must have been I_1 as plaintext, as it has repeated plaintext blocks; otherwise it must have been I_2. The answer is then I_2.

(b) In CBC mode $C_i = E_K(M_i + C_{i-1})$, where we assume the block cipher behaves like a random permutation on the input alphabet which in this case is of size 2^8. Under the assumption that image I_1 was sent, we can compute all the input blocks to the block cipher, call them $x'_1, x'_2, \ldots$. If I_2 was sent, it will correspond to another sequence of input blocks $x''_1, x''_2, \ldots$. Now we again use the observation that if an input block is repeated, the ciphertext must be the same. Due to the birthday paradox we know that in a sequence of input blocks, we have a repetition of a previous block after observing roughly the square root of the number of possible input blocks. So $(2^8)^{1/2} = 16$. So if we find for $i \neq j$: $x'_i = x'_j$ and $c_i = c_j$ OR $x''_i = x''_j$ and $c_i \neq c_j$, then most likely I_1 was the transmitted image. Similar conditions for I_2. Collisions of the typ $x'_i = x'_j$ or $x''_i = x''_j$ are expected to appear after, say, 10-20 blocks. *The lesson to learn: A too small block size can influence on security.*

(c) A bit-oriented stream cipher encrypts by $c_i = m_i + z_i$. All symbols are now considered to be in $\mathbb{F}_{2^8}$. There are only two possible plaintexts I_1 or I_2. So from the observed ciphertext, there are only two possible keystreams; if $M = I_1$ then

$$Z = 00000001, 10000000, 10011010, \ldots$$

and if $M = I_2$ then

$$Z = 00000001, 10000001, 10011010, \ldots$$

In $\mathbb{F}_{2^8}$ this corresponds to $Z = 1, \alpha^7, \alpha^7 + \alpha^4 + \alpha^3 + \alpha, \ldots$ for I_1 and $Z = 1, \alpha^7 + 1, \alpha^7 + \alpha^4 + \alpha^3 + \alpha, \ldots$ for I_2.
We need to find out which one is the correct on. What we know is that the linear complexity for the stream cipher is ≤ 1. This means that the stream cipher can be replaced by an LFSR of length at most 1. So one way of solving our problem is to apply the BM-algorithm to one of the possible key streams. If the BM-algorithm delivers a shortest LFSR of length >1 then we know that this is not the correct keystream. We try the $M = I_1$ case.

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^7	α^7+1		$1+\alpha^7 D$		picture			2	2
$\alpha^7+\alpha^4+\alpha^3+\alpha$	0							3	3

Above, we computed $\alpha^{14} = \alpha^7 + \alpha^4 + \alpha^3 + \alpha$.
The same for the $M = I_2$ case (you do not need to do this).

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^7+1	α^7		$1+(\alpha^7+1)D$		picture			2	2
$\alpha^7+\alpha^4+\alpha^3+\alpha$	$\alpha^7+\alpha^4+\alpha^3+\alpha+(\alpha^7+1)^2 \neq 0$			≥ 2				3	3

So it must be $M = I_1$.

Problem 5

(a) For example, the Fermat test means computing $a^{p-1} \bmod p$ for some $1 \leq a \leq p-1$, and check if it equals 1. If p is a prime, it must always be so. For example, computing $2^{1020} \bmod 1021 = 1$, $3^{1020} \bmod 1021 = 1$, and a few more, gives that with high probability that p is a prime.

(b)

$$\phi(n) = (p-1)(q-1) = 126 \cdot 1020 = 128520.$$

Pick $e = 11$ since $\gcd(128520, 11) = 1$ (other choices are possible). The secret d is the inverse of e modulo $\phi(n)$, i.e., $d \cdot e = 1 \bmod \phi(n)$. We compute it through Euclidean algorithm to be $d = 35051$.

(c) Computing $C = 19753^{11}$. Square and multiply means first squaring by computing

$$M = 19753, M^2 = 19753^2 = 13006, M^4 = (M^2)^2 = 13006^2 = 70268, M^8 = (M^4)^2 = 70268^2 = 2131,$$

all calculations in $\mathbb{Z}_{129667}$. Then observe that

$$C = 19753^{11} = 19753^{8+2+1} = 19753^8 \cdot 19753^2 \cdot 19753 = 2131 \cdot 13006 \cdot 19753 = 27484.$$

(d) From the project, we know that we can rewrite as $574^2 - 447^2 = 0 \bmod n$ meaning that $(574 - 447)(574 + 447) = K \cdot p \cdot q$ in the integers, for some K. By computing $\gcd(574 - 447, n)$ we have a chance of getting p or q. In this case we are lucky because $\gcd(574 - 447, 129667) = 127$ and so $127|129667$ and n is factored.