Problem 1

(a) CORRECT (For example, since $P_1(0) = P_1(1) = 1$)
(b) WRONG (Since $P_1(1) = 0$)
(c) CORRECT ($\mathbb{F}_{2^2}$ is generated by $\alpha^2 = \alpha + 1$. Again, $P_1(x) \neq 0$ for $x \in \{0, 1, \alpha, \alpha + 1\}$)
(d) WRONG ($P_2(x) = (x^3 + x^2 + 1)(x^2 + x + 1)$)
(e) WRONG (No finite field with 33 elements can exist, since $33 = 11 \cdot 3$ (only prime powers))

Problem 2

(a) Given formulas:

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

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

Computing

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

$$H(M) = -1/2 \log(1/2) - 1/4 \log(1/4) - 2 * (1/8 \log(1/8)) = 7/4.$$

$$H(K) = \log(|\mathcal{K}|) = \log(5^{32}) = 32 \log 5.$$

Finally,

$$N_0 = H(K)/D = \frac{32 \log 5}{(\log 5 - 7/4)} \approx 130 \text{ symbols.}$$

(b) 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. So the answer is around 130 ciphertext symbols.
(c) In a known-plaintext attack, every ciphertext symbol C_i gives Eve knowledge of one key symbol $K_{i \bmod l}$. So after receiving 32 ciphertext symbol with a known plaintext we know the key. The answer is 32.
(d) If we want a new scheme with finite key size we need to make $D = 0$. This can be done if we precode the source and map to a new and larger alphabet, called *homphonic coding*. Let the new alphabet be $\mathbb{Z}_8$ and let $\phi(M, r)$ be the map from $\mathbb{Z}_5$ to $\mathbb{Z}_8$ using randomness r. Let $\phi(M = 0, r)$ map to one of the symbols in $\{0, 1, 2, 3\}$, all with equal probability, $\phi(M = 1, r)$ map to one of the symbols in $\{4, 5\}$, with equal probability, $\phi(M = 2, r) = 6$, and finally $\phi(M = 3, r) = 7$. Note that ϕ is invertible. Now if $M' = \phi(M, r)$ we have $P(M = m') = 1/8$ and M' is uniformly distributed. Using a cryptosystem like

$$C_i = M'_i + K_{i \bmod l} \mod 8, \quad 0 \leq i \leq n - 1,$$

gives $D = 0$ and $N_0 = \infty$.

Problem 3

(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 blocks are the same, Eve knows that it must have been I_1 as plaintext, otherwise it must have been I_2.

(b) Counter mode works by encryption a counter to create a keystream and then adding it to the plaintext, for example $Z_1 = E_K(\mathbf{1}), Z_2 = E_K(\mathbf{2}), \ldots$, where $\mathbf{i}$ is the 16-bit block corresponding to the binary representation of i, etc. Encryption is done by $C_i = M_i + Z_i$.

(c) A bit-oriented stream cipher encrypts by $c_i = m_i + z_i$. 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

$$Z = 1000100000001000, 01111111\ldots$$

and if $M = I_2$ then

$$Z = 1000100000001000, 10000000\ldots$$

We need to find out which one is the correct on. What we know is that the linear complexity for the stream cipher is ≤ 8. This means that the stream cipher can be replaced by an LFSR of length at most 8. 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 >8 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
0	1		1		picture			2	2
0	0							3	3
0	0							4	4
1	1	1	$1+D^4$	4	picture	1	1	1	5
0	0							2	6
0	0							3	7
0	0							4	8
0	1	$1+D^4$	1	5	picture	$1+D^4$	1	1	9
0	0							4	10
0	0							4	11
0	0							4	12
1	1	1	$1+D^4+D^8$	8	picture	1	1	1	13
0	0							2	14
0	0							3	15
0	0							4	16
0	1			**>8**					

So it must be $M = I_2$.

Problem 4

(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 $2^{2016} mod 2017 = 1$, $3^{2016} mod 2017 = 1$, and a few more, gives that with high probability, p is a prime.

(b)

$$\phi(n) = (p-1)(q-1) = 112 \cdot 2016 = 225792.$$

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.

$$\begin{aligned} 225792 &= 25 \cdot 9031 + 17 \\ 25 &= 17 \cdot 1 + 8 \\ 17 &= 8 \cdot 2 + 1 \end{aligned}$$

Reverse direction,

$$\begin{aligned} 1 &= 17 - 8 \cdot 2 \\ &= 17 - (25 - 17 \cdot 1) \cdot 2 = 17 \cdot 3 - 25 \cdot 2 \\ &= (225792 - 25 \cdot 9031) \cdot 3 - 25 \cdot 2 = 225792 \cdot 3 - 27095 \cdot 25. \end{aligned}$$

This means that $-27095 \cdot 25 = 1$ modulo 225792, and so $d = (-27095) = 198697$.

(c) Computing $C = 123^{25}$. Square and multiply means first squaring by computing

$$M = 123, M^2 = 123^2 = 15129, M^4 = (M^2)^2 = 15129^2 = 53957, M^8 = (M^4)^2 = 53957^2 = 122916, M^16 = (M$$

all calculations in $\mathbb{Z}_{227921}$
Then observe that

$$C = 123^{25} = 123^{16+8+1} = 123^{16} \cdot 123^8 \cdot 123 = 143729 \cdot 122916 \cdot 123 = 196207.$$

(d) (difficult) Eve knows d (and also e). Picking any x she can form $x^{e \cdot d} = x^{1+k \cdot \phi(n)} = x$. But because she knows d she can also compute $e \cdot d - 1$ and form $x^{e \cdot d - 1} = x^{k \cdot \phi(n)} = 1$. Because $e \cdot d - 1$ is an even number she can also compute $(e \cdot e - 1)/2$. So by letting $X = x^{(e \cdot e - 1)/2}$ for some x and putting $Y = 1$ she can generate pairs such that $X^2 = Y^2$. If $X = x^{(e \cdot d - 1)/2} \neq 1$ a factor of n will come from computing $\gcd(X - 1, n)$. If $X = x^{(e \cdot d - 1)/2} = 1$, Eve can divide again and try $X = x^{(e \cdot d - 1)/4}$, etc.

Problem 5

(a) We have $k = 3$ and so we have an unknown polynomial $a(x) = a_0 + a_1 x + a_2 x^2$ over $\mathbb{F}_{37}$. We know the following system of linear equations:

$$\begin{aligned} 30 &= a_0 + 2a_1 + 4a_2 \\ 20 &= a_0 + 3a_1 + 9a_2 \\ 7 &= a_0 + 7a_1 + 7^2 a_2 \end{aligned}$$

Solving this gives $K = a_0 = 10$.

(b) Eve observes $M = (0, 0, 10)$ leading to knowledge of e_1 since $t = e_1 + s_1 e_2 + s_2 e_2^2$ and so $10 = e_1 + 0 \cdot e_2 + 0 \cdot e_2^2$ and $e_1 = 10$. Now

$$P_S = \max_{M'} P(M' \text{ valid} | (0, 0, 10) \text{ observed}) = \max_{M'} \frac{\text{Number of } e_2 \text{ for which } M' \text{ is valid}}{\text{Total Number of } e_2 \text{ values}}$$

The condition for M' to be valid is $t = 10 + s_1 e_2 + s_2 e_2^2$ for the choice of t. Because this is a degree 2 polynomial in the unknown e_2, it can have at most two solutions. So the maximum P_S is $2/37$ and we just need to find a message M' giving this probability. Putting $t = 10$, we have the condition $s_1 e_2 + s_2 e_2^2 = 0$ or $e_2(s_1 + s_2 e_2)$, which can have two solutions. So for example $M' = (1, 1, 10)$.