1. Given a key $K = (a, b)$ the encryption transformation is $e_K(x) = ax + b \mod 27$. From the given plaintext we get two equations for solving the key:

$$a \cdot 17 + b \equiv 17 \pmod{27}$$
$$a \cdot 14 + b \equiv 11 \pmod{27}$$

from where

$$a \cdot 3 \equiv 6 \pmod{27},$$

or equivalently, $a \equiv 2 \pmod{9}$.

Hence, we get three solutions modulo 27: $a = 2, 11, \text{ or } 20$. The corresponding solutions for $b$ are $b = 10, 19, \text{ and } 1$, respectively. When decrypting the ciphertext, the key $(a, b) = (11, 19) = L.T. \text{ reveals the survivor’s name ROBINSON CRUSOE.}$ (Linus Torvalds was one of the developers of the new processor “Crusoe” at Transmeta.)

2. Let $A_k$ be the event that a plaintext block has exactly $k$ zeroes. Let $B_k$ be the event that the ciphertext has $k$ zeroes, $k = 0, 1, \ldots, 8$. Then using the definition of conditional probability

$$p(z = 0 \mid B_k) = \frac{p(z = 0, B_k)}{p(B_k)} = \frac{p(z = 0, A_k)}{p(z = 0) p(A_k) + p(z = 1) p(A_{8-k})} = \frac{\frac{1}{2}p^k (1 - p)^{8-k}}{1 + \left(\frac{p}{1-p}\right)^{8-2k}}$$

since $p(z = 0) = p(z = 1) = \frac{1}{2}$, and the key is independent of the plaintext. If $p < \frac{1}{2}$, that is $p < 1 - p$, then the conditional probability of $z = 0$ decreases with $k$ and is maximized with $k = 0$. If $p > \frac{1}{2}$, that is $p > 1 - p$, then the conditional probability of $z = 0$ increases with $k$ and is maximized with $k = 8$. If $p = \frac{1}{2}$, that is $p = 1 - p$, then the conditional probability of $z = 0$ equals $\frac{1}{2}$, for all $k = 0, 1, \ldots, 8$. In this case we do not get any information about the key by counting the number of zeroes and ones in the ciphertext. Note also that, for all values of $p$, $p \neq 0, 1$, a ciphertext, which has four zeroes and four ones, does not give any information about the key, that is, $p(z = 0 \mid B_4) = \frac{1}{2}$.

3. a) See the text book.

b) $\left(\frac{2}{21}\right) = -1$, since $21 \equiv 3 \pmod{8}$. On the other hand, $2^{21-1} = 1024 \equiv 16 \pmod{21}$. Since $\left(\frac{2}{21}\right) \neq 2^{\frac{21-1}{2}}$, we conclude that 21 is not Euler pseudo-prime to the base 2.
4. \(2000 = 16 \cdot 125,\) and \(\gcd(16,125) = 1.\) We need to find a number \(a\) such that

\[
\begin{align*}
    a - 29 & \equiv 0 \pmod{16} \\
    a + 29 & \equiv 0 \pmod{125},
\end{align*}
\]

or what is the same,

\[
\begin{align*}
    a & \equiv 13 \pmod{16} \\
    a & \equiv 96 \pmod{125}.
\end{align*}
\]

The solution is \(a = 221 = 96 + 125 = 13 + 13 \cdot 16,\) which verifies the condition \(221^2 \equiv 841 \pmod{2000}.\) Clearly also \(-a = 1779 \pmod{2000}\) is a solution.

5. a) Your public key is

\[
\beta = a^a = x^7 = x^3x^4 = x^3(x + 1) = x^4 + x^3 = x^3 + x + 1 = 1011.
\]

b) First you compute, using your secret key, \(\beta^k = (a^k)^a = (x^2)^7 = x^{14}.\) Then you observe that \(x^{14}x = x^{15} = 1,\) or what is the same, \(\beta^{-k} = x.\) Hence

\[
X = X(\beta^k x) = (X\beta^k)x = (x^3 + x^2 + x)x = x^4 + x^3 + x^2 = x^3 + x^2 + x + 1 = 1111.
\]