TIK-110.503 Foundations of Cryptology
Final exam
January 29, 2000
SOLUTIONS

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

$$a \cdot 17 + b \equiv 17 (\mathrm{mod} 27)$$
$$a \cdot 14 + b \equiv 11 (\mathrm{mod} 27)$$

from where

$$a \cdot 3 \equiv 6 (\mathrm{mod} 27), \text{ or equivalently, } a \equiv 2 (\mathrm{mod} 9).$$

Hence, we get three solutions modulo 27: $a = 2$, 11, or 20. The corresponding solutions for b are $b = 10$, 19, and 1, respectively. When decrypting the ciphertext, the key $(a, b) = (11, 19) =$ `L.T.` 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

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

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 xeroes 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 $21 \equiv 3 (\mathrm{mod} 8)$. On the other hand, $2^{\frac{21-1}{2}} = 1024 \equiv 16 (\mathrm{mod}\ 21)$. 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

$$\begin{aligned} a - 29 &\equiv 0(\text{mod} 16) \\ a + 29 &\equiv 0(\text{mod} 125), \end{aligned}$$

or what is the same,

$$\begin{aligned} a &\equiv 13(\text{mod} 16) \\ a &\equiv 96(\text{mod} 125). \end{aligned}$$

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

5. a) Your public key is

$$\beta = \alpha^a = x^7 = x^3 x^4 = x^3(x+1) = x^4 + x^3 = x^3 + x + 1 = 1011.$$

b) First you compute, using your secret key, $\beta^k = (\alpha^k)^a = (x^2)^7 = x^{14}$. Then you observe that $x^{14}x = x^{15} = 1$, or what is the same, $\beta^{-k} = x$. Hence $X = X(\beta^k x) = (X\beta^k)x = (x^3+x^2+x)x = x^4+x^3+x^2 = x^3+x^2+x+1 = 1111$.