Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[3 parts, 2 points each]** Consider the affine cipher with key $k = (\alpha, \beta)$ whose functions are given by $e_k(m) = \alpha m + \beta$ and $d_k(c) = \alpha^{-1}(c - \beta)$ in $\mathbb{Z}_m$.

   (a) Specify the key space for this cipher as a product $A \times B$, where A is the set of all candidates for α and B is the set of all candidates for β.

   $A = \mathbb{Z}_m^*$ $\quad B = \mathbb{Z}_m$, $\quad$ so $\mathcal{K} = \mathbb{Z}_m^* \times \mathbb{Z}_m$.

   (b) Let $m = 38$, and let $k = (\alpha, \beta) = (15, 6)$. Decrypt the ciphertext $c = 22$.

   $22 = \alpha m + \beta$

   $22 = (15)m + 6$

   $15m = 16$

   Find $(15)^{-1}$: since modulus is not prime, we need EEA.

   $38 = (2)(15) + 8$

   $15 = (1)(8) + 7$

   $8 = (1)(7) + 1$

   $1 = 8 + (-1)(7)$

   $= 8 + (-1)(15 + (-1)(8))$

   $= (2)(8) + (-1)(15)$

   $= (2)[38 + (-2)(15)] + (-1)(15)$

   $= (2)(38) + (-5)(15)$.

   So $(15)^{-1} = -5$ and

   $15m = 16$

   $(-5)(15)m = (-5)(16)$

   $1m = -80 = -80 + 114 = \boxed{34}$

   (c) Eve obtains the plaintext/ciphertext pairs $(10, 22)$ and $(15, 25)$. Find the key (α, β).

   $22 = \alpha \cdot 10 + \beta$

   $25 = \alpha \cdot 15 + \beta$

   $3 = 5\alpha$

   We need 5^{-1} in $\mathbb{Z}_m$.

   Since $(15)(-5) = 1$ from part (b), we have $(-15)(5) = 1$ and so

   $5^{-1} = -15$.

   We compute $5\alpha = 3$

   $\alpha = 3 \cdot 5^{-1} = 3 \cdot (-15)$

   $= -45 = -7 = 31$

   and $22 = (31)(10) + \beta$

   $\beta = 22 - (31)(10)$

   $= 22 - (-7)(10)$

   $= 22 + 70 = 92 = 92 - 76 = 16$.

   So the key is $\boxed{(31, 16)}$.

2. **[2 parts, 2 points each]** Alice and Bob meet privately and decide to communicate using the exclusive-or cipher with a block size of 6 bits. They agree on a private key k.

   (a) Alice sends the first ciphertext $c_1 = 100110$ to Bob, which Eve intercepts. What can Eve conclude about the corresponding plaintext message m_1? Explain.

   Eve can reach $\boxed{\text{no conclusions}}$ about m_1. This is a <u>one-time pad</u>.

   (b) Bob responds to Alice with the second ciphertext $c_2 = 011101$, which Even intercepts. What can Eve conclude about the corresponding plaintext messages m_1 and m_2? Explain.

   Eve knows

   $$100110 = m_1 \oplus k$$
   $$011101 = m_2 \oplus k.$$

   Adding those together, Eve knows that

   $$(m_1 \oplus k) \oplus (m_2 + k) = \begin{array}{r} 100110 \\ \oplus 011101 \end{array}$$

   $$(m_1 \oplus m_2) \oplus (k \oplus k) = 111011$$

   $$m_1 \oplus m_2 \oplus 000000 = 111011$$

   $$\boxed{m_1 \oplus m_2 = 111011.}$$

   Although Eve does not know m_1 or m_2, she has significant, potentially compromising information about the plaintext messages.