Name: Solutions

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

1. **[3 points]** Describe what it means for a symmetric cipher to be immune to a chosen plaintext attack.

Given plaintext/ciphertext pairs $(m_1, c_1), \ldots, (m_n, c_n)$ encrypted with a key k, it is difficult to compute $d_k(c)$ for any ciphertext c not in $\{c_1, \ldots, c_n\}$

2. Recall the multiplicative cipher: $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_p^*$ and

$$e_k(m) = k \cdot m \qquad\qquad d_k(c) = k^{-1} \cdot c.$$

(a) **[3 points]** Alice and Bob choose $p = 17$ and $k = 2$. Encrypt the message 12, and decrypt the ciphertext 15.

Encrypt 12: $e_2(12) = 2 \cdot 12 = 24 = \boxed{7}$

Decrypt 15: Need to find k^{-1}; $2 \cdot k^{-1} \equiv 1 \mod 17$,

or equivalently $2 \cdot k^{-1} \equiv 18 \pmod{17}$, so $k^{-1} = 9$.

~~$d_2(15) = k^{-1} \cdot 15 = 9 \cdot 15 = 9 \cdot (-3) = -27$~~

$d_2(15) = k^{-1} \cdot 15 = 9 \cdot (-2) = -18 = -1 = \boxed{16}$.

(b) [**4 points**] Alice and Bob choose $p = 53$ and select a secret key. Eve intercepts the ciphertext 10 and manages to recover the plaintext message 14. Find the key that Alice and Bob have selected.

We know $e_k(m) = c$, so $km = c$ and

$k(14) = 10$.

We need $(14)^{-1}$. Let's use Extended Euclidean Alg:

$53 = 3 \cdot 14 + 11$

$14 = 1 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

So $1 = 3 - 1 \cdot 2 = 3 - 1(11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11$

$= 4(14 - 1 \cdot 11) - 1 \cdot 11 = 4 \cdot 14 - 5 \cdot 11$

$= 4 \cdot 14 - 5(53 - 3 \cdot 14) = 19 \cdot 14 - 5 \cdot 53$

So $(14)^{-1} = 19$. Therefore $k \cdot (14)(19) = (10)(19)$

$k = 190$

$k = \boxed{31}$.