HOMEWORK 4

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (2.3) Let g be a primitive root for $\mathbb{F}_p$.
  (a) Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $gx = h \mod p$. Prove that $a = b \mod (p-1)$. Explain why this implies the map (2.1) on page 65 is well-defined.
  (b) Prove that
$$\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$$
for all $h_1, h_2 \in \mathbb{F}_p$.
  (c) Prove that
$$\log_g(h^n) = n \log_g(h)$$
for all $h \in \mathbb{F}_p$ and $n \in \mathbb{Z}$.

(2) (2.4) Compute the following discrete logarithms:
  (a) $\log_2(13)$ for the prime 23, i.e., $p = 23$, $g = 2$, and you must solve the the congruence $2^x = 13 \mod 23$.
  (b) $\log_{10}(22)$ for the prime $p = 47$.
  (c) $\log_{627}(608)$ for the prime $p = 941$. (Hint: Look in the second column of Table 2.1 on page 66.)

(3) (2.16) Verify the following assertions from Exmaple 2.16.
  (a) $x^2 + \sqrt{x} = \mathcal{O}(x^2)$
  (b) $5 + 6x^2 - 37x^5 = \mathcal{O}(x^5)$
  (c) $k^{300} = \mathcal{O}(2^k)$
  (d) $(\ln k)^{375} = \mathcal{O}(k^{0.001})$
  (e) $k^2 2^k = \mathcal{O}(e^{2k})$
  (f) $N^{10} 2^N = \mathcal{O}(e^N)$

(4) (1.44) Consider the Hill cipher defined by (1.11)
$$e_k(m) = k_1 \cdot m + k_2 \mod p \text{ and } d_k(m) = k_1^{-1} \cdot (c - k_2) \mod p$$
where m, c, and k_2 are column vectors of dimension n, and k_1 is an $n \times n$-matrix.
  (a) We use the Hill cipher with $p = 7$ and the key $k_1 = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ and $k_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$.
    (i) Encrypt the message $m_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.
    (ii) What is the matrix k_1^{-1} used for decryption?
    (iii) Decrypt the message $c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$.
  (b) Explain why the Hill cipher is vulnerable to a known plaintext attack.

(c) The following plaintext/ciphertext pairs were generated using a Hill cipher with the prime $p = 11$. Find the keys k_1 and k_2.

$$m_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \; c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}, \; m_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, \; c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}, \; m_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}, c_3 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}$$

(d) Explain how any simple substitution cipher that involves a permutation of the alphabet can be thought of as a special case of a Hill cipher.

(5) (1.48) Explain why the cipher

$$e_k(m) = k \oplus m \text{ and } d_k(c) = k \oplus c$$

defined by XOR of bit strings is not secure against a known plaintext attack. Demonstrate your attack by finding the private key used to encrypt the 16-bit ciphertext $c =$ 1001010001010111 if you know the corresponding plaintext is $m =$ 0010010000101100.