1.

(a) ENCRYPT MATH

$X \longrightarrow 6x+8\ [\mathrm{mod}\ 29]$ Ex. $F=5 \rightarrow 38 \equiv 9 = J$

$M = 12 \longrightarrow 6(12)+8 = 80 \bmod 29 \equiv 22$ (W)
$A = 0 \longrightarrow 6(0)+8 = 8 \bmod 29 \equiv 8$ (I)
$T = 19 \longrightarrow 6(19)+8 = 122 \bmod 29 \equiv 6$ (G)
$H = 7 \longrightarrow 6(7)+8 = 50 \bmod 29 \equiv 21$ (V)

MATH $\longrightarrow$ WIGV

(b) V♡ Find $6^{-1}$ $6y \equiv 1 \bmod 29$

$V = 21$ $6(5) \equiv 1 \bmod 29 \rightarrow 6^{-1} \equiv 5 \bmod 29$
$♡ = 27$ $d_k = 5(y-8) \bmod 29$

$21 = 5(21-8) = 65 \bmod 29 \equiv 7$ (H)
$27 = 5(27-8) = 95 \bmod 29 \equiv 8$ (I)

V♡ $\xrightarrow[d_k]{}$ HI

(c)

$$\left.\begin{aligned} 0 &= 6(0)+8 \equiv 8 \bmod 30 \\ 5 &= 6(5)+8 \equiv 8 \bmod 30 \\ 10 &= 6(10)+8 \equiv 8 \bmod 30 \end{aligned}\right\} \text{Result}$$

MANY Characters would go to same value, making decryption impossible

**1.44.** Consider the Hill cipher defined by (1.11),

$$e_k(m) \equiv k_1 \cdot m + k_2 \pmod p \qquad \text{and} \qquad d_k(c) \equiv k_1^{-1} \cdot (c - k_2) \pmod p,$$

where $m$, $c$, and $k_2$ are column vectors of dimension $n$, and $k_1$ is an $n$-by-$n$ matrix.

(a) We use the vector 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 $m = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.
  (ii) What is the matrix $k_1^{-1}$ used for decryption?
  (iii) Decrypt the message $c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$.

(a)

(i) $e_k(m) \equiv k_1 \cdot m + k_2 \bmod p$

$$k_1 \cdot m = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1\times 2 + 3\times 1 \\ 2\times 2 + 2\times 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 6 \end{bmatrix}$$

$c = k_1 \cdot m + k_2 \bmod 7$

$$\hookrightarrow \begin{bmatrix} 5 \\ 6 \end{bmatrix} + \begin{bmatrix} 5 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 10 \bmod 7 \\ 10 \bmod 7 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} \bmod 7$$

(ii) Inv. $\dfrac{1}{\det(k)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod p$

$\det(k) = 1(2) - (3)(2) = -4 \equiv 3 \bmod 7$

$3x \equiv 1 \bmod 7 \to 3(5) = 15 \equiv 1 \bmod 7$

$3^{-1} \equiv 5 \bmod 7$

$$5 \cdot \begin{bmatrix} 2 & -3 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 10 & -15 \\ -10 & 5 \end{bmatrix} \bmod 7 \equiv \begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix} \bmod 7$$

(iii) $d_k \to c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$ $\quad d_k(c) = k_1^{-1} \cdot (c - k_2) \bmod p$

$$\begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix} \cdot \left( \begin{bmatrix} 3 \\ 5 \end{bmatrix} - \begin{bmatrix} 5 \\ 4 \end{bmatrix} \right) \to \begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} -2 \\ 1 \end{bmatrix} \bmod 7$$

$$\to \begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} -2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 3(-2) + 6(1) \\ 4(-2) + 5(1) \end{bmatrix} = \begin{bmatrix} 0 \\ -3 \end{bmatrix} \bmod 7 \equiv \begin{bmatrix} 0 \\ 4 \end{bmatrix} \bmod 7$$

**1.46.** (a) Convert the 12 bit binary number 110101100101 into a decimal integer between 0 and $2^{12} - 1$.
(b) Convert the decimal integer $m = 37853$ into a binary number.
(c) Convert the decimal integer $m = 9487428$ into a binary number.
(d) Use exclusive or (XOR) to "add" the bit strings $11001010 \oplus 10011010$.

(a) 110101100101
11 10 9 8 7 6 5 4 3 2 1 0

$\rightarrow 2^0 \cdot 1 + 2^2 \cdot 1 + 2^5 \cdot 1 + 2^6 \cdot 1 + 2^8 \cdot 1 + 2^{10} \cdot 1 + 2^{11} \cdot 1$

$\rightarrow 110101100101_2 = 3429$

(b) $m = 37853 \rightarrow$ Binary

If remainder - 1
No remainder - 0

| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 32768 | 16384 | 8192 | 4096 | 2048 | 1024 | 512 | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

$1001001111011101_2 = 37853_{10}$

(d) XOR $\oplus$

$$\begin{array}{r} 11001010 \\ \oplus\ 10011010 \\ \hline 01010000 \end{array}$$

$\rightarrow$ Answer: $01010000_2$

**1.48.** Explain why the cipher

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

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 that the corresponding plaintext is $m = 0010010000101100$.

$e_k(m) = k \oplus m$
$\hookrightarrow c = k \oplus m \rightarrow k = c \oplus m$

$$\begin{array}{r} 1001010001010111 \\ \oplus\ 0010010000101100 \\ \hline \end{array}$$

$k = 1011000001111011_2$

**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 congruence $2^x \equiv 13 \pmod{23}$.

(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.)

(a) $2^x \equiv 13 \bmod 23$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16$

$2^5 = 32 \equiv 9 \bmod 23$

$2^6 = 18 \bmod 23$

$2^7 = 36 \equiv 13 \bmod 23$ , $x = 7$

$\log_2(13) \equiv 7 \bmod 23$

(b) $\log_{10}(22)$ $p = 47$

$10^1 = 10$

$10^2 = 100 \equiv 6 \bmod 47$

$10^3 = 6 \cdot 10 \equiv 13 \bmod 47$

$10^4 = 13 \cdot 10 \equiv 36 \bmod 47$

$10^5 = 36 \cdot 10 \equiv 31 \bmod 47$

$10^6 = 31 \cdot 10 \equiv 27 \bmod 47$

$10^7 = 27 \cdot 10 \equiv 35 \bmod 47$

$10^8 = 35 \cdot 10 \equiv 21 \bmod 47$

$10^9 = 210 \equiv 22 \bmod 47$

$\log_{10}(22) \equiv 11 \bmod 47$

(c) $627^x \equiv 608 \bmod 941$

$627^{18} \bmod 941 \equiv 608$ , $n = 18$

$\log_{627}(608) \equiv 18$

6. $p = 13,\ g = 6$

Alice sends Bob $A = 2$
secret exp - $b = 4$

(a) $B = g^b \bmod p$

$\rightarrow B = 6^4 \bmod 13 \rightarrow 6^2 = 36 \bmod 13 \equiv 10 \bmod 13$
$\rightarrow 6^4 = 10 \cdot 2 = 100 \bmod 13$

$$\begin{array}{r} 100 \\ -91 \\ \hline 009 \end{array} \equiv 9 \bmod 13$$

Bob Sends $= 9 \bmod 13$

(b) $S = A^b \bmod p$

$S = 2^4 \bmod 13 \rightarrow 2^4 \equiv 3 \bmod 13$

$\hookrightarrow S = 3 \bmod 13$

(c) $g^x \equiv 2 \bmod 13$

$6^1 \equiv 6 \bmod 13$
$6^2 \equiv 10 \bmod 13$
$6^3 = 6 \times 10 \equiv 8 \bmod 13$
$6^4 = 8 \times 6 \equiv 9 \bmod 13$
$6^5 = 6 \times 9 \equiv 2 \bmod 13$

$6^5 = 2 \bmod 13$, Secret exp: $a = 5$