MATH 233: ASSIGNMENT 3

DUE: FRIDAY, FEBRUARY 16, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1 (6.6.1)**.** The ciphertext `YIFZMA` was encrypted by a Hill cipher with matrix

$$\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix} \pmod{26}.$$

Find the plaintext.

Solution. Let A be the given matrix (mod 26). Then

$$\det A \equiv 9 \cdot 3 - 13 \cdot 2 \equiv 1 \pmod{26},$$

so

$$A^{-1} \equiv \begin{pmatrix} 3 & -13 \\ -2 & 9 \end{pmatrix} \pmod{26}.$$

Then

$$\begin{array}{lllll}
\mathtt{YI} & \to & \begin{pmatrix} 24 & 8 \end{pmatrix} A^{-1} \equiv \begin{pmatrix} 56 & -240 \end{pmatrix} \equiv \begin{pmatrix} 4 & 20 \end{pmatrix} & \to & \mathtt{eu} \\
\mathtt{FZ} & \to & \begin{pmatrix} 5 & 25 \end{pmatrix} A^{-1} \equiv \begin{pmatrix} -35 & 160 \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 \end{pmatrix} & \to & \mathtt{re} \\
\mathtt{MA} & \to & \begin{pmatrix} 12 & 0 \end{pmatrix} A^{-1} \equiv \begin{pmatrix} 36 & -156 \end{pmatrix} \equiv \begin{pmatrix} 10 & 0 \end{pmatrix} & \to & \mathtt{ka}
\end{array}$$

shows that the plaintext is `eureka`. □

Problem 2 (6.6.5)**.** Eve captures Bob's Hill cipher machine, which uses a 2×2 matrix M mod 26. She tries a chosen plaintext attack. She finds that the plaintext `ba` encrypts to `HC` and the plaintext `zz` encrypts to `GT`. What is the matrix M?

Solution. From the given information, we construct a matrix equation as

$$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} M \equiv \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \pmod{26}.$$

(We used -1 instead of $\mathtt{z} = 25$ for simplicity.) The first matrix is invertible mod 26, with inverse

$$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$

(note that it is the same as the original matrix), so

$$M \equiv \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \equiv \begin{pmatrix} 7 & 2 \\ -13 & -21 \end{pmatrix} \equiv \begin{pmatrix} 7 & 2 \\ 13 & 5 \end{pmatrix} \pmod{26}.$$

□

Note. Problems 3 and 4 are about designing the known plaintext attack for certain cryptosystems. For each problem, assume that you can use only one plaintext. You should choose the plaintext wisely, so that you are able to find the entire key(s) regardless of the ciphertext that you get. Furthermore, you should try to keep the length of your plaintext as short as possible. A full credit may not be given if your plaintext is too long.

Problem 3 (6.6.4)**.** Consider the following combination of Hill and Vigenère ciphers: The key consists of three 2×2 matrices, M_1, M_2, $M_3 \pmod{26}$. The plaintext letters are represented as integers mod 26. The first two are encrypted by M_1, the next two by M_2, the 5th and 6th by M_3. This is repeated cyclically, as in the Vigenère cipher. Explain how to do a chosen plaintext attack on this system. Assume that you know that three 2×2 matrices are being used. State explicitly what plaintext you would use and how you would use the outputs.

Solution. Use `babababababab` = 101010010101 as the plaintext, and suppose that the ciphertext is $c_1 c_2 \dots c_{12}$ (where each c_i is represented as an integer mod 26). Then we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} M_1 \equiv \begin{pmatrix} c_1 & c_2 \\ c_7 & c_8 \end{pmatrix} \quad \Rightarrow \quad M_1 \equiv \begin{pmatrix} c_1 & c_2 \\ c_7 & c_8 \end{pmatrix} \pmod{26},$$

and similarly

$$M_2 \equiv \begin{pmatrix} c_3 & c_4 \\ c_9 & c_{10} \end{pmatrix} \quad \text{and} \quad M_3 \equiv \begin{pmatrix} c_5 & c_6 \\ c_{11} & c_{12} \end{pmatrix} \pmod{26}.$$

□

Problem 4 (6.6.9)**.** Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} \equiv \begin{pmatrix} u & v \end{pmatrix} \pmod{26}.$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plaintext you choose and how to recover the key.

Solution. Use `aabaab` = 001001 as the plaintext. Then

$$\begin{aligned} \begin{pmatrix} 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} &\equiv \begin{pmatrix} e & f \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} &\equiv \begin{pmatrix} a+e & b+f \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} &\equiv \begin{pmatrix} c+e & d+f \end{pmatrix} \pmod{26}. \end{aligned}$$

Now suppose that the ciphertext is $x_1 x_2 x_3 x_4 x_5 x_6$, where each x_i is represented as an integer mod 26. Then from above, we can get

$$(a, b, c, d, e, f) \equiv (x_3 - x_1, x_4 - x_2, x_5 - x_1, x_6 - x_2, x_1, x_2) \pmod{26}.$$

□

Problem 5 (4.6.3)**.** Suppose a message m is chosen randomly from the set of all five-letter English words (so all five-letter words in the dictionary have the same probability) and is encrypted to a ciphertext c using an affine cipher mod 26, where the key is chosen randomly from the 312 possible keys. Compute the conditional probability

$$P(m = \texttt{hello} \mid c = \texttt{HHGZC}).$$

Use the result of this computation to determine whether or not affine ciphers have perfect secrecy.

Solution. Since two `l`'s in `hello` cannot encrypt to `G` and `Z` using the same affine cipher, the conditional probability is zero. Since $P(m = \texttt{hello})$ is nonzero, this shows that affine ciphers does not have perfect secrecy. □

Problem 6 (4.6.13)**.** Alice encrypts the messages m_1 and m_2 with the same one-time pad using only capital letters and spaces. (*Note.* For this problem, assume that each letter or space is converted to a 7-bit block without the parity bit, according to the ASCII code.) Eve knows this, intercepts the ciphertexts C_1 and C_2, and also learns that the decryption of m_1 is the following.

`THE LETTER * ON THE MAP GIVES THE LOCATION OF THE TREASURE`

Unfortunately for Eve, she cannot read the missing letter $*$. However, the 12th group of seven bits in C_1 is 1001101 and the 12th group in C_2 is 0110101. Find the missing letter. (Use `A` = 1000001, `B` = 1000010, ..., `Z` = 1011010 and space = 0100000.)

Solution. The 12th group of seven bits in $m_1 \oplus m_2$ is equal to that in $C_1 \oplus C_2$, which is

$$1001101 \oplus 0110101 = 1111000.$$

Since it begins with 1 and the 12th block of m_1 is known to be a letter, we can conclude that the 12th block of m_2 is the space (0100000) and consequently the 12th block of m_1 is

$$1111000 \oplus 01000000 = 1011000 = \texttt{X}.$$

□