The Hill Cipher

Eleanor Miranda

Dr. Ward Heilman (Mathematics Department)

Bridgewater State University

Introduction

- The Hill Cipher was created by Lester Hill in 1929 with the intention of making a more secure encryption system.
- The Hill cipher uses concepts from linear algebra, including matrix transformations over finite fields, to encrypt the plaintext into ciphertext, with the key being an *n* x *n* invertible matrix.
- It was one of the first general methods of encryption that applies linear algebra in a practical way.
- It suffers weaknesses to known plaintext attacks, having limited key space, and requiring an invertible key matrix.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1: The integers corresponding to the twenty-six-letter alphabet.

Encryption

1. Break the plaintext letters into pairs and convert them into integers using Table 1 (e.g., A=0, B=1, ..., Z=25). Also, choose a 2x2 invertible key matrix.
   - E.g., Encrypt the message "HI"
   - H = 7; I = 8
   - Key matrix: $A = \begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix}$
2. Convert the integer pairs into column matrices and multiply them by the key matrix, reducing the result mod 26.
   - $\begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} (9 \cdot 7) + (4 \cdot 8) \\ (6 \cdot 7) + (5 \cdot 8) \end{bmatrix} = \begin{bmatrix} 95 \\ 82 \end{bmatrix} = \begin{bmatrix} 17 \\ 4 \end{bmatrix} (mod 26)$
3. The resulting column matrices are then changed back into a string of integers, which are then converted back into letters using Table 1, producing the ciphertext message.
   - 17 = R; 4 = E; Ciphertext = "RE"

Decryption

1. Divide the letters up into pairs and convert them into the corresponding integers, as shown in Table 1.
2. Convert the integer pairs into column matrices and multiply them by the inverse of the key matrix, reducing the result mod 26.

$$A^{-1} = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}^{-1} = [det(A)]^{-1} \begin{bmatrix} K_4 & -K_2 \\ -K_3 & K_1 \end{bmatrix} \bmod 26$$

Figure 1: Finding the inverse of the key matrix.

3. Table 2 can be used to find the multiplicative inverse of the determinant mod 26. The integers in the resulting matrix are then reduced mod 26. *If the determinant of the key matrix is not relatively prime to mod 26, then it does not have a multiplicative inverse mod 26 and the ciphertext cannot be decrypted.*

3	5	7	17	19	25
9	21	15	23	11	25

Table 2: Multiplicative inverses mod 26.

4. The inverse of the key matrix is multiplied by the column matrices composed of the integers that correspond to the ciphertext.
5. The resulting column matrices are then changed back into a string of integers, which are then converted back into letters using Table 1, producing the original plaintext message.

Weaknesses

- It is vulnerable to known plaintext attacks. If the attacker knows some of the plaintext and its corresponding ciphertext, then it wouldn't be difficult to figure out the key using the information they already know.
- The Hill cipher has a small key space, as there are a limited number of possible keys that can be used.
- The encrypted message may not be able to be decrypted if the key matrix is not invertible, since the method of decryption is to apply the inverse of the key matrix to the ciphertext.

Decryption Example

This is an example of decrypting the ciphertext message "RE" which was found when encrypting the plaintext message "HI" in the first example.

1. Find the inverse of the key matrix A.

$$A^{-1} = \begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix}^{-1} = \frac{1}{(9 \cdot 5) - (4 \cdot 6)} \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} = \frac{1}{21} \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} =$$

$$= 5 \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} (mod 26) = \begin{bmatrix} 25 & -20 \\ -30 & 45 \end{bmatrix} = \begin{bmatrix} 25 & 6 \\ 22 & 19 \end{bmatrix} (mod 26)$$

2. Multiply this inverse matrix by the column matrix containing the ciphertext message and then reduce the result mod 26.
   - Ciphertext = "RE"
   - R = 17; E = 4

$$\begin{bmatrix} 25 & 6 \\ 22 & 19 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} (25 \cdot 17) + (6 \cdot 4) \\ (22 \cdot 17) + (19 \cdot 4) \end{bmatrix} = \begin{bmatrix} 449 \\ 450 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} (mod 26)$$

3. Translate the numbers from the column matrix, 7 and 8, back into letters.
   - 7 = H; 8 = I
   - Plaintext = "HI" (the original message that was encrypted in the first example)