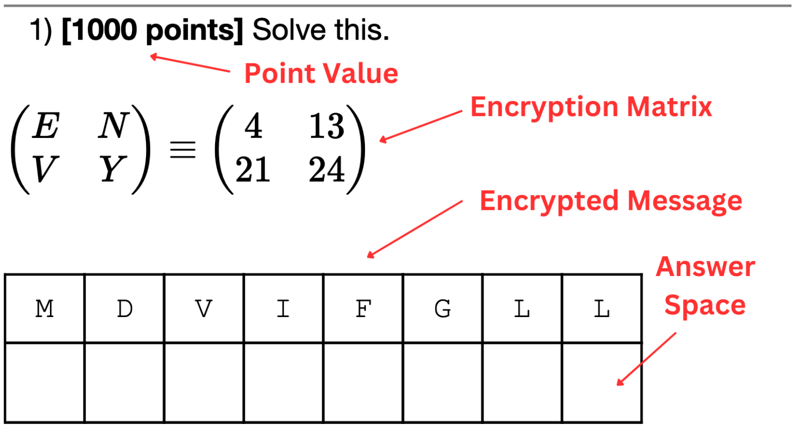
How to Decode a 2x2 Hill Cipher
A Guide for New MHS Science Olympiad Codebusters Members

As a new member of Mason High School's Science Olympiad Codebusters team, you might feel overwhelmed with the number and complexity of the ciphers you are required to know how to crack. The Hill cipher is no exception, and it's an especially tricky cipher because its decoding requires modular arithmetic and matrix operations, both of which are undergraduate level skills. Regardless, it's an incredibly important cipher to master – almost 20% of a typical Codebusters test are Hill ciphers.

Before learning how to crack a Hill cipher, it's important to understand the general mechanism of a Hill cipher. A Hill cipher is a mathematical substitution cipher that uses matrix multiplication to encrypt and decrypt text. The encryption matrix of a Hill cipher is a square matrix (usually represented by a word) that is used to transform the plaintext into ciphertext and vice-versa. Because of this, assuming two people have a shared knowledge of the key, they can send messages back and forth that are incredibly difficult to crack.

In order to prepare you to solve Hill cipher Codebusters questions in a Science Olympiad invitational competition context, this handout will teach you how to:

1. Calculate the decryption matrix.
2. Set up the decryption calculations.
3. Multiply the decryption matrix with the fragmented cipher.
4. Write the resulting vectors as a sequence of plaintext fragments.



1) **[1000 points]** Solve this.

$$\begin{pmatrix} E & N \\ V & Y \end{pmatrix} \equiv \begin{pmatrix} 4 & 13 \\ 21 & 24 \end{pmatrix}$$

M	D	V	I	F	G	L	L

Figure 1: An example cipher on the Science Olympiad Toebes platform. Figures 2 through 10 are subsets of Figure 1. All visuals created by Ravi Bandaru.

Steps to Solving the Hill Cipher

1. Calculate the decryption matrix.

   (i) Write down the numerical form of the encryption matrix.

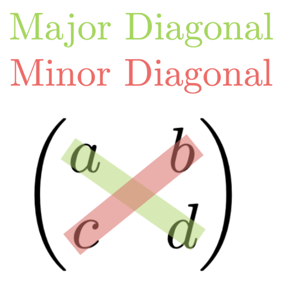


Figure 2: Encryption matrix structure and layout.

   (ii) Calculate the determinant of the matrix using the formula $ad - bc$.

   ! If the determinant is not coprime to 26 (i.e., they share a common factor other than 1), the cipher cannot be decoded. You can end the steps here and simply write "UNABLE TO DECODE" on the question packet to receive full points.

$$\det \begin{pmatrix} 4 & 13 \\ 21 & 24 \end{pmatrix} = (4 \times 24 - 21 \times 13) \\ = \boxed{-177}$$

Figure 3: Calculation of determinant of example cipher encryption matrix. Step 1.(ii).

   (iii) Take the modulus of the determinant with respect to 26.

   In other words, add or subtract multiples of 26 until the result is between 0 and 25.

$$-177 \mod 26 = -177 + 7 \times 26 \\ = \boxed{5}$$

Figure 4: Calculation of modulus of example cipher's determinant. Step 1.(iii).

   (iv) Find the modulo 26 multiplicative inverse of the determinant using the reference table on the tables sheet of the test.

   ! If the determinant does not have a corresponding modular multiplicative inverse in the tables sheet, **STOP**. Recheck whether the determinant is coprime to 26.

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

Figure 5: Using the table in the Toebes packet to find the modular multiplicative inverse of the example cipher. Step 1.(iv).

(v) Calculate the adjugate of the encryption matrix.

  i. **Swap** the positions of the entries on the **major** diagonal.

  ii. **Change the signs** of the entries on the **minor** diagonal.

$$\operatorname{adj}\begin{pmatrix} 4 & 13 \\ 21 & 24 \end{pmatrix} = \begin{pmatrix} 24 & -13 \\ -21 & 4 \end{pmatrix}$$

Figure 6: Adjugate of encryption matrix of example cipher. Step 1.(v).

(vi) Multiply the multiplicative inverse with the adjugate of the encryption matrix.

(vii) Take the modulus of the result with respect to 26. This is your decryption matrix.

$$\operatorname{adj}\begin{pmatrix} 4 & 13 \\ 21 & 24 \end{pmatrix} = \begin{pmatrix} 24 & -13 \\ -21 & 4 \end{pmatrix}$$

Figure 7: Final calculation of decryption matrix of example cipher. Steps 1.(vi) and 1.(vii).

2. Set up the decryption calculations.

(i) Break the encrypted message into 2-letter fragments.

> If there are an odd number of letters in the cipher, then breaking the encrypted message into 2-letter fragments is not possible and the cipher cannot be decoded. You can end the steps here and simply write "UNABLE TO DECODE" on the question packet to receive full points.

(ii) Convert the 2-letter fragments to numerical form based on their order in the alphabet starting with 0. (Ex. A=0, B=1, C=2, and so on).

> Use the relevant portion of the table sheet to quickly map the numbers.

(iii) Write the 2-letter fragments as numerical 2x1 column vectors next to the decryption matrix.

$$\begin{pmatrix} M \\ D \end{pmatrix} = \begin{pmatrix} 12 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix} V \\ I \end{pmatrix} = \begin{pmatrix} 21 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} F \\ G \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} L \\ L \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$$

Figure 8: Fragmentation and numerical conversion of encrypted message of example cipher. Steps 2.(i) and 2.(ii).

3. Multiply the decryption matrix with the fragmented cipher.
   - (i) Pair up the entries in the first row of the decryption matrix with entries in the column vector.
   - (ii) Multiply the pairs together.
   - (iii) Add the products.
   - (iv) Write the sum as the first entry in the resulting 2x1 column vector.
   - (v) Repeat the first two steps for the second row of the decryption matrix.
   - (vi) Write the sum as the second entry in the resulting 2x1 column vector.
   - (vii) Take the modulus of each of the entries in the matrices with respect to 26.

$$\begin{pmatrix} 10 & 13 \\ 1 & 6 \end{pmatrix} \times \begin{pmatrix} 12 \\ 3 \end{pmatrix} = \begin{pmatrix} 10 \times 12 + 13 \times 3 \\ 1 \times 12 + 6 \times 3 \end{pmatrix} = \begin{pmatrix} 159 \\ 30 \end{pmatrix} \mod 26 = \boxed{\begin{pmatrix} 3 \\ 4 \end{pmatrix}}$$

$$\begin{pmatrix} 10 & 13 \\ 1 & 6 \end{pmatrix} \times \begin{pmatrix} 21 \\ 8 \end{pmatrix} = \begin{pmatrix} 10 \times 21 + 13 \times 8 \\ 1 \times 21 + 6 \times 8 \end{pmatrix} = \begin{pmatrix} 314 \\ 69 \end{pmatrix} \mod 26 = \boxed{\begin{pmatrix} 2 \\ 17 \end{pmatrix}}$$

$$\begin{pmatrix} 10 & 13 \\ 1 & 6 \end{pmatrix} \times \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 10 \times 5 + 13 \times 6 \\ 1 \times 5 + 6 \times 6 \end{pmatrix} = \begin{pmatrix} 128 \\ 41 \end{pmatrix} \mod 26 = \boxed{\begin{pmatrix} 24 \\ 15 \end{pmatrix}}$$

$$\begin{pmatrix} 10 & 13 \\ 1 & 6 \end{pmatrix} \times \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 10 \times 11 + 13 \times 11 \\ 1 \times 11 + 6 \times 11 \end{pmatrix} = \begin{pmatrix} 253 \\ 77 \end{pmatrix} \mod 26 = \boxed{\begin{pmatrix} 19 \\ 25 \end{pmatrix}}$$

Figure 9: Multiplication of decryption matrix with fragmented example cipher and subsequent modulation. Step 3.

4. Write the resulting vectors as a sequence of plaintext fragments. This will obtain the decoded message.

Use the relevant portion of the table sheet to quickly map the numbers.

! If the plaintext message has an odd number of letters, a “Z” will be added at the end to allow the cipher to be properly divided into fragments. Make sure to remove the “Z” at the end of the message if this is the case.

$$\begin{pmatrix} 3 \\ 4 \end{pmatrix} = \boxed{\begin{pmatrix} D \\ E \end{pmatrix}}$$

$$\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \boxed{\begin{pmatrix} C \\ R \end{pmatrix}}$$

$$\begin{pmatrix} 24 \\ 15 \end{pmatrix} = \boxed{\begin{pmatrix} Y \\ P \end{pmatrix}}$$

$$\begin{pmatrix} 19 \\ 25 \end{pmatrix} = \boxed{\begin{pmatrix} T \\ Z \end{pmatrix}}$$

$$\boxed{\text{“}DECRYPT\text{”}}$$

Figure 10: Plaintext conversion of example cipher, resulting in decoded message “DECRYPT". Step 5.

Conclusion

At the end of the Hill cipher-solving process, you will have extracted a coherent, decrypted phrase from an encryption. The Hill cipher may seem daunting, but with practice and a good understanding of its mechanism, it is possible to quickly and accurately decrypt ciphertexts. By following the instructions carefully and practicing regularly, you will be well-prepared to tackle Hill cipher Codebusters questions to place well in competitions.