

Math 400 Fall 2018
 Cryptology HW 3 Solutions
 Due Thursday, September 21

1. Let $(1, 2, 3, 4, 5) \mapsto (5, 3, 4, 1, 2)$ be the key to a permutation block cipher.
 - (a) Encrypt the plaintext `california`.
 - (b) Decrypt the ciphertext `VENIU TYSIR`.

Solution:

- (a) `IFALC IARN0`
 - (b) `unive rsity` or “university”.
2. (a) Compute the inverse of 7 modulo 26.
 - (b) Is the matrix $\begin{bmatrix} 1 & 5 \\ 3 & 2 \end{bmatrix}$ invertible? Why?
 - (c) Find the inverse of $\begin{bmatrix} 4 & 3 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

Solution:

- (a) By trial and error, we see that $7 \cdot 15 = 105 \equiv 1 \pmod{26}$. So 15 is an inverse of 7.
- (b) $\det A = 2 - 15 = -13$, and $(-13, 26) = 13 \neq 1$. So the matrix is not invertible.
- (c)

$$\begin{aligned} \left[\begin{array}{ccc|ccc} 4 & 3 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right] &\rightarrow \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 4 & 3 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right] &\rightarrow \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & -3 & 1 & -4 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right] \\ &\rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & -2 & 1 & -3 & 0 \\ 0 & 1 & 3 & -1 & 4 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right] &\rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -3 & 2 \\ 0 & 1 & 0 & -1 & 4 & -3 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right] \end{aligned}$$

We can multiply this back by the original matrix to check that it is in fact the inverse.

3. Encrypt the plaintext **random** using a Hill cipher with key $K = \begin{bmatrix} 1 & 4 & 2 \\ 3 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix}$.

Solution: **random** becomes 17-00-13 03-14-12. We compute

$$\begin{bmatrix} 1 & 4 & 2 \\ 3 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 17 \\ 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 43 \\ 77 \\ 56 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 25 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 4 & 2 \\ 3 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 12 \end{bmatrix} = \begin{bmatrix} 83 \\ 47 \\ 53 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 21 \\ 1 \end{bmatrix}$$

so we get the ciphertext **RZEFVB**.

4. The ciphertext **KQXUMU** was encrypted by a Hill cipher with key $\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$. What was the plaintext?

Solution: We have $\det K = 27 - 26 = 1$ so $K^{-1} = \frac{1}{1} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix}$. We can render the ciphertext as 10-16, 23-20, 12-20 and we compute

$$\begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} \begin{bmatrix} 10 \\ 16 \end{bmatrix} = \begin{bmatrix} -178 \\ 124 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} \begin{bmatrix} 23 \\ 20 \end{bmatrix} = \begin{bmatrix} -191 \\ 134 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} \begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} -224 \\ 156 \end{bmatrix} \equiv \begin{bmatrix} 10 \\ 0 \end{bmatrix}$$

Thus the plaintext is 04-20 17-04 10-00, which translates to **eureka**.

5. The ciphertext **GEZXDS** was encrypted by a 2×2 Hill cipher. The plaintext is **solved**. Find the encryption key.

Solution: The plaintext is 18-14 11-21 04-03, and the ciphertext is 06-04 25-23 03-18. We need to solve

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 18 & 11 \\ 14 & 21 \end{bmatrix} = \begin{bmatrix} 6 & 25 \\ 4 & 23 \end{bmatrix}$$

but we have $\det \begin{bmatrix} 18 & 11 \\ 14 & 21 \end{bmatrix} = 224 \equiv 16 \pmod{26}$ and $\gcd(16, 26) = 2 \neq 1$, so this matrix isn't invertible. We try again:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 18 & 04 \\ 14 & 03 \end{bmatrix} = \begin{bmatrix} 6 & 03 \\ 4 & 18 \end{bmatrix}$$

but again the determinant is even, so we don't get a unique solution. We try the last option:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 11 & 4 \\ 21 & 3 \end{bmatrix} = \begin{bmatrix} 25 & 3 \\ 23 & 18 \end{bmatrix}$$

We compute $\det \begin{bmatrix} 11 & 4 \\ 21 & 3 \end{bmatrix} = -51 \equiv 1 \pmod{26}$. Thus the inverse is $\begin{bmatrix} 3 & -4 \\ -21 & 11 \end{bmatrix} \equiv \begin{bmatrix} 3 & 22 \\ 5 & 11 \end{bmatrix}$ and we compute

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 25 & 3 \\ 23 & 18 \end{bmatrix} \begin{bmatrix} 3 & -4 \\ -21 & 11 \end{bmatrix} = \begin{bmatrix} 12 & -67 \\ -309 & 106 \end{bmatrix} \equiv \begin{bmatrix} 12 & 11 \\ 3 & 2 \end{bmatrix}.$$

6. Suppose that the matrix $A = \begin{bmatrix} 2 & 3 \\ 4 & 3 \end{bmatrix}$ is used as the encryption key for a Hill cipher. Find two different (two-letter) plaintexts that encrypt to the same ciphertext. Why did this happen, and why is it a problem?

Solution: **aa** and **na** both encrypt to **AA**. (There are many possible solutions).

7. Suppose I encrypt a message with the Hill cipher, and the ciphertext is a sequence of one hundred As:

AA
 AA

What can you tell me about the plaintext and the key?

Does your answer change if the ciphertext is a sequence of one hundred Bs instead?

Solution: If the ciphertext is a sequence of 100 As, this tells us the plaintext was also a sequence of 100 As, but tells us nothing about the key. (Any key will send all-As to all-As).

If the sequence is all Bs instead, the same argument doesn't hold. Clearly every block is the same, but the plaintext could be almost anything.