Use of Linear Algebra in Cryptography

Hong-Jian Lai

Department of Mathematics
West Virginia University
Morgantown, WV
Problem: To create a matrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$.
Creating a Matrix

- **Problem:** To create a matrix \( A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix} \).

- **Matlab:**

---

---
Creating a Matrix

**Problem:** To create a matrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$.

**Matlab:**

$A = [1 \ 2 \ 3; \ 4 \ 5 \ 6; \ 7 \ 8 \ 10]$
Compute the inverse of $A \mod m$

- **Output setting:** Need to set the output as "rational" using a matlab comment `format rat;`
Compute the inverse of $A \mod m$

- **Output setting:** Need to set the output as "rational" using a matlab comment `format rat;`

- **Problem:** Given $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$, find $A^{-1} \mod 26$. 

Step 1: Compute inverse over the reals

- Matlab commends:
Step 1: Compute inverse over the reals

- Matlab commands:
  - format rat;
Step 1: Compute inverse over the reals

- Matlab commends:
  - `format rat;`
  - `Ainv = inv(A)`
Step 1: Compute inverse over the reals

- Matlab commands:
  - format rat;
  - Ainv = inv(A)

\[
Ainv = \begin{pmatrix}
-2/3 & -4/3 & 1 \\
-2/3 & 11/3 & -2 \\
1 & -2 & 1
\end{pmatrix}
\]
Step 1: Compute inverse over the reals

- Matlab commands:
  - `format rat;`
  - `Ainv = inv(A)`

\[
A_{inv} = \begin{pmatrix}
-2/3 & -4/3 & 1 \\
-2/3 & 11/3 & -2 \\
1 & -2 & 1
\end{pmatrix}
\]

- **Observation:** 3 is a common denominator.
Step 2: Making it all integral

- **Problem:** Need to rationalize this matrix before we take modulo $m$. As every entry of $A_{inv}$ has a common denominator 3, multiply by 3 to make it an integer valued matrix.
Step 2: Making it all integral

- **Problem:** Need to rationalize this matrix before we take modulo $m$. As every entry of $A_{inv}$ has a common denominator 3, multiply by 3 to make it an integer valued matrix.

- $A_1 = (A_{inv} \times 3)$
Step 2: Making it all integral

- **Problem:** Need to rationalize this matrix before we take modulo $m$. As every entry of $A_{inv}$ has a common denominator 3, multiply by 3 to make it an integer valued matrix.

- $A_1 = (A_{inv} \times 3)$

$$
A_1 = \begin{pmatrix}
-2 & -4 & 3 \\
-2 & 11 & -6 \\
3 & -6 & 3
\end{pmatrix}
$$
Step 3: Find the inverse of $A$ (mod 26)

- **Problem:** In Step 2, we computed $A_1 = 3A^{-1}$ (mod 26). We need to multiply $A_1$ by $3^{-1}$ to get $A^{-1}$.
Step 3: Find the inverse of $A \ (\text{mod} \ 26)$

- **Problem:** In Step 2, we computed $A_1 = 3A^{-1} \ (\text{mod} \ 26)$. We need to multiply $A_1$ by $3^{-1}$ to get $A^{-1}$.

- Compute $3^{-1} \equiv 9 \ (\text{mod} \ 26)$. 
Step 3: Find the inverse of $A \pmod{26}$

- **Problem**: In Step 2, we computed $A_1 = 3A^{-1} \pmod{26}$. We need to multiply $A_1$ by $3^{-1}$ to get $A^{-1}$.

- Compute $3^{-1} \equiv 9 \pmod{26}$.

- Use matlab commend: $M_2 = \text{round}(\text{mod}(M_1 \times 9, 26))$ to find $A^{-1} = A_2$
Step 3: Find the inverse of $A$ (mod 26)

- **Problem:** In Step 2, we computed $A_1 = 3A^{-1}$ (mod 26). We need to multiply $A_1$ by $3^{-1}$ to get $A^{-1}$.

- Compute $3^{-1} \equiv 9$ (mod 26).

- Use matlab commend: $M2 = round(mod(M1 * 9, 26))$ to find $A^{-1} = A_2$

- $A^{-1} := A_2 = \begin{pmatrix} 8 & 16 & 1 \\ 8 & 21 & 24 \\ 1 & 24 & 1 \end{pmatrix}$
Example 1: The problem

Problem Suppose that we have intercepted a cipher text HVSCSCBKRYMIUA, and intelligent agents informed us that this is encrypted by a block cipher using digraphs (size 2 blocks) with a mod 26 alphabet, and that the plain text of THRY has been encrypted as HVRY. Break this code by finding the plain text.
Example 1: Compute deciphering matrix,

Step 1

Solution strategy: Compute the decoding matrix

\[ A^{-1} = P_1 C_1^{-1} \], where \( P_1 \) is given by plain text THRY and \( C_1 \) is by cipher text HVRY.
Example 1: Compute deciphering matrix,
Step 1

- Solution strategy: Compute the decoding matrix
  \[ A^{-1} = P_1 C_1^{-1} \], where \( P_1 \) is given by plain text THRY and
  \( C_1 \) is by cipher text HVRY.

- format rat; \( C_1 = \begin{bmatrix} 7 & 17 \\ 21 & 24 \end{bmatrix}, \ C_3 = inv(C1) \)
Example 1: Compute deciphering matrix,
Step 1

- Solution strategy: Compute the decoding matrix
  \[ A^{-1} = P_1 C_1^{-1} \], where \( P_1 \) is given by plain text THRY and
  \( C_1 \) is by cipher text HVRY.

- Format rat; \( C_1 = [7 
 17; 21 24], C_3 = \text{inv}(C_1) \)

- \( C_3 = \begin{pmatrix} -8/63 & 17/189 \\ 1/9 & -1/27 \end{pmatrix} \)
Example 1: Compute deciphering matrix, Step 1

- Solution strategy: Compute the decoding matrix
  \( A^{-1} = P_1 C_1^{-1} \), where \( P_1 \) is given by plain text THRY and \( C_1 \) is by cipher text HVRY.

- format rat; \( C1 = [7 \ 17; \ 21 \ 24] \), \( C3 = \text{inv}(C1) \)

- \( C3 = \begin{pmatrix} -8/63 & 17/189 \\ 1/9 & -1/27 \end{pmatrix} \)

- Observation: 189 is a common denominator.
Example 1: Compute deciphering matrix, Step 2

- Compute $189^{-1} \equiv 15 \pmod{26}$ (using powermod or gcd).
Example 1: Compute deciphering matrix, Step 2

- Compute $189^{-1} \equiv 15 \pmod{26}$ (using powermod or gcd).
- $C_4 = C_3 \times 189; C_5 = \text{round}(\text{mod}(C_4 \times 15, 26))$
Example 1: Compute deciphering matrix, Step 2

- Compute $189^{-1} \equiv 15 \pmod{26}$ (using powermod or gcd).

- $C_4 = C_3 \times 189; C_5 = \text{round}(\text{mod}(C_4 \times 15, 26))$

- $C_5 = \begin{pmatrix} 4 & 21 \\ 3 & 25 \end{pmatrix}$
Example 1: Compute deciphering matrix $Ainv$, Step 3

Strategy review: $A^{-1} = P_1 C_1^{-1}$, and $C_5 = C_1^{-1}$. 
Example 1: Compute deciphering matrix

$Ainv$, Step 3

- Strategy review: $A^{-1} = P_1 C_1^{-1}$, and $C_5 = C_1^{-1}$.
- $P_1 = [19 \ 17; 7 \ 24]$; $Ainv = mod(P1 * C5, 26)$
Example 1: Compute deciphering matrix $A_{inv}$, Step 3

- **Strategy review:** $A^{-1} = P_1C_1^{-1}$, and $C_5 = C_1^{-1}$.
- $P_1 = [19 \ 17; \ 7 \ 24]$; $A_{inv} = \text{mod}(P_1 \ast C_5, 26)$
- $A_{inv} = \begin{pmatrix} 23 & 18 \\ 22 & 19 \end{pmatrix}$
Example 1: Compute deciphering matrix

$Ainv$, Step 3

- Strategy review: $A^{-1} = P_1 C_1^{-1}$, and $C5 = C_1^{-1}$.
- $P1 = [19\ 17;\ 7\ 24]$; $Ainv = mod(P1 \ast C5, 26)$
- $Ainv = \begin{pmatrix} 23 & 18 \\ 22 & 19 \end{pmatrix}$
Example 1: Decoding

Decoding computation: \[ P = A^{-1}C \]
Example 1: Decoding

- Decoding computation: \( P = A^{-1}C \)
- \( C = [7 \ 18 \ 18 \ 1 \ 17 \ 12 \ 20; \ 21 \ 2 \ 2 \ 10 \ 24 \ 8 \ 0]; \quad P = mod(Ainv \ast C, 26) \)
Example 1: Decoding

Decoding computation:  \( P = A^{-1}C \)

\( C = [7 \ 18 \ 18 \ 1 \ 17 \ 12 \ 20; \ 21 \ 2 \ 2 \ 10 \ 24 \ 8 \ 0] ; \ P = \mod(A^{\text{inv}} * C, \ 26) \)

\[
P = \begin{pmatrix}
19 & 8 & 8 & 21 & 17 & 4 & 18 \\
7 & 18 & 18 & 4 & 24 & 0 & 24
\end{pmatrix}
\]
Example 1: Decoding

- Decoding computation: $P = A^{-1}C$
- $C = \begin{bmatrix} 7 & 18 & 18 & 1 & 17 & 12 & 20 \\ 21 & 2 & 2 & 10 & 24 & 8 & 0 \end{bmatrix}$; $P = \text{mod}(A^{-1} \cdot C, 26)$

$$P = \begin{pmatrix} 19 & 8 & 8 & 21 & 17 & 4 & 18 \\ 7 & 18 & 18 & 4 & 24 & 0 & 24 \end{pmatrix}$$

- Back to English: the message is THISISVERYEASY.