Number Theory

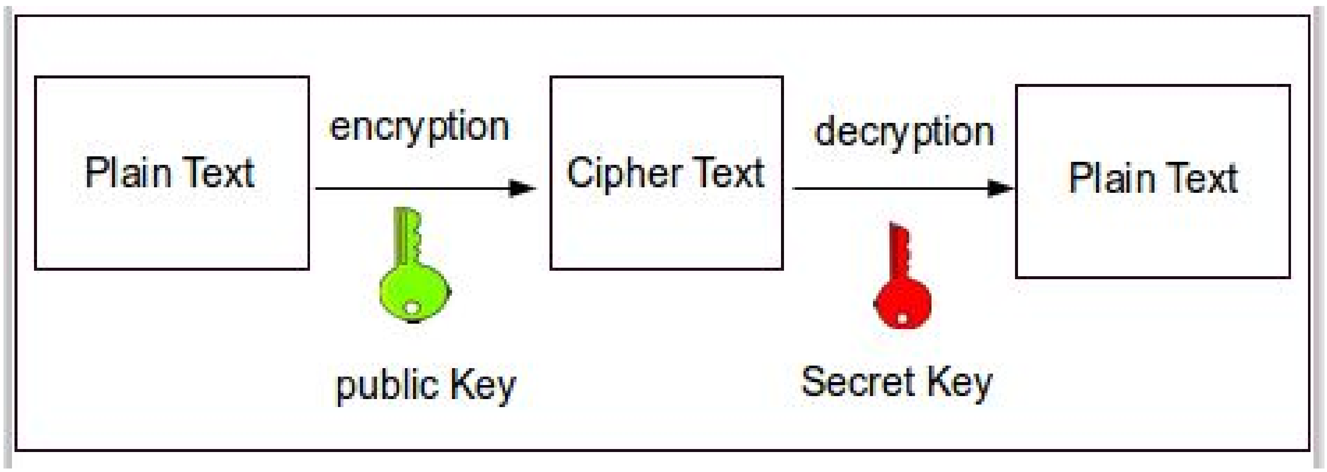
Application to Encryption

Modular inverses of matrices

We'll look at the case of 2 x 2 matrices

Modular inverses of matrices

We'll look at the case of 2 x 2 matrices



Modular inverses of matrices

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

Modular inverses of matrices

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

$$A^{-1} = 4\begin{bmatrix} 2 & -1 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 8 & -4 \\ -8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \bmod 5$$

Modular inverses of matrices

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

$$A^{-1} = 4\begin{bmatrix} 2 & -1 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 8 & -4 \\ -8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \bmod 5$$

$$A * A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix}$$ and taking mod 5 of all elements,

Modular inverses of matrices

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

$$A^{-1} = 4\begin{bmatrix} 2 & -1 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 8 & -4 \\ -8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \bmod 5$$

$$A * A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix}$$ and taking mod 5 of all elements,

We get $\begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \bmod 5 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

Example:

Find the modular inverse of $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ mod 5 and show that $A*A^{-1} \equiv I(\text{mod } 5)$.

Example:

Find the modular inverse of $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ mod 5 and show that $A*A^{-1} \equiv I(\text{mod } 5)$.

$$A^{-1} = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$$

Example:

Find the modular inverse of $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ mod 5 and show that $A*A^{-1} \equiv I \pmod 5$.

$$A^{-1} = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$$

The same idea applies for higher order square matrices, i.e. of size n x n.

Modular Inverses – summary

- The determinant is the term: $a*d - b*c = \mathit{det}$

Modular Inverses – summary

- The determinant is the term: a*d – b*c = *det*
- For modular inverses, we cannot use 1/*det* as it's not usually an integer

Modular Inverses – summary

- The determinant is the term: a*d – b*c = *det*
- For modular inverses, we cannot use 1/*det* as it's not usually an integer
- So we solve:

$$det * x \equiv 1 \bmod n$$

Modular Inverses – summary

- The determinant is the term: a*d – b*c = *det*
- For modular inverses, we cannot use 1/*det* as it's not usually an integer
- So we solve:

$$det * x \equiv 1 \bmod n$$

- Now *x* is the modular inverse of *det*

Modular Inverses – summary

- The determinant is the term: a*d – b*c = *det*
- For modular inverses, we cannot use 1/*det* as it's not usually an integer
- So we solve:

$$det * x \equiv 1 \bmod n$$

- Now *x* is the modular inverse of *det*
- Negative numbers are replaced by positive congruent (mod n) numbers

Modular Inverses – summary

- The determinant is the term: a*d – b*c = *det*
- For modular inverses, we cannot use 1/*det* as it's not usually an integer
- So we solve:

$$det * x \equiv 1 \bmod n$$

- Now *x* is the modular inverse of *det*
- Negative numbers are replaced by positive congruent (mod n) numbers
- From these we get the modular inverse of A

Exam question

Example 1: Show that the modular inverse mod 7 of

$$E = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \text{ is } D = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Hence show how to encrypt the string "ACAB" using E as the encryption matrix, and find the encrypted string. Assume letters A to Z are represented by 1 to 26, and '*' represents 0.

1) Compute the determinant of E. Here it is,

$$3*3-2*2=5$$

So, we need the modular inverse of 5 (mod 7).

Solve $5x = 1 \pmod 7$

So $x = 3$ is the solution.

2) Then the inverse is given by :

$$D = 3\begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 9 & -6 \\ -6 & 9 \end{pmatrix} \bmod 7$$

$$= \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

3) The string "AC" = 13, and "AB" = 12

Then the encrypted string is:

$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 9 \\ 11 \end{pmatrix} \bmod 7 \quad = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \bmod 7 \quad = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

This gives "BD" and "*A" so the full string is

$$"BD * A"$$

Check your answer:

As always, we can check our answer - does the message decode using D to return the original message?

Exam question

Example 2 : Show that the modular inverse mod 7 of

$E = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}$ is $D = \begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$

Hence show how to encrypt the string "ABBA" using E as the encryption matrix, and fnd the encrypted string. Assume letters A to Z are represented by 1 to 26, and '*' represents 0.

Compute the determinant of E.
Here: $ad - bc = 3(2) - 1(2) = 4$

Then find the modular inverse (mod 7):
$\frac{1}{det} = \frac{1}{4} = 4^{-1} = 2$

Then the inverse is given by:

$$D = 2\begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & -2 \\ -4 & 6 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$$

3) The string "AB" = 1 2, and "BA" = 21

Then the encrypted string is :

$$\begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \end{pmatrix} \bmod 7 \quad = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 6 \end{pmatrix} \bmod 7 \quad = \begin{pmatrix} 0 \\ 6 \end{pmatrix}$$

This gives "EF" and "*F" so the full string is

$$"EF\ *F"$$

Check your answer:

As always, we can check our answer - does the message decode using D to return the original message?