Cryptography and Linear Algebra

David McClelland
Diego Perilla
Alissa Clark
Daniel Lopez

Introduction to Cryptography

- Cryptography is the study of the techniques of writing and decoding messages in code.

- Cipher - A procedure that will render a message unintelligible to the recipient. Used to also recreate the original message.
- Plaintext - The message or information that is being encrypted.
- Ciphertext - The message or information that is created after the cipher has been used.

- Examples of encryption:
  - Shift Cipher, Substitution, Transformation

Summary of Application in Linear Algebra

- A matrix can be used as a cipher to encrypt a message.
  - The matrix must be invertible for use in decrypting.

- Cipher matrix can be as simple as a 3x3 matrix composed of random integers.
- In order to encrypt plaintext, each character in the plaintext must be denoted with a numerical value and placed into a matrix.
  - These numbers can range in value, but an example is using 1-26 to represent A to Z and 27 to represent a space.
- This matrix is then multiplied with the cipher matrix to form a new matrix containing the ciphertext message.

Encrypting a Message

- Each character of the plaintext is given a numerical value as stated before.
- These values are then separated into vectors, S.T. the number of rows of each vector is equivalent to the number of rows of the cipher matrix.
  - Values are placed into each vector one at a time, going down a row for each value. Once a vector is filled the next vector is created. If the last vector does not get filled by the plaintext then the remaining entries will hold the value for a space.
- The vectors are then augmented to form a matrix that contains the plaintext.
- The plaintext matrix is then multiplied with the cipher matrix to create the ciphertext matrix.

Decrypting a Message

- To decrypt a ciphertext matrix the original cipher matrix must be used. The cipher matrix must be inverted in order to decrypt the ciphertext.

- This inverted cipher matrix is then multiplied with the ciphertext matrix.
  - The product produces the original plaintext matrix.

- The plaintext can be found again by taking this product and splitting it back up into its separate vectors, and then converting the numbers back into their letter forms.

An Example

- First obtain a cipher matrix -

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

- For this example we will use the following plaintext -
    - PENGUINS ARE ONE TO ONE
- Now we will replace each letter with its numerical representation, using 1-26 for A-Z and 27 for a space.
    - 16, 5, 14, 7, 21, 9, 14, 19, 27, 1, 18, 5, 27, 15, 14, 5, 27, 20, 15, 27, 15, 14, 5

Example Continued

- Now separate the plaintext into 3x1 vectors until the whole plaintext is used.

$$\begin{bmatrix}16\\5\\14\end{bmatrix}\begin{bmatrix}7\\21\\9\end{bmatrix}\begin{bmatrix}14\\19\\27\end{bmatrix}\begin{bmatrix}1\\18\\5\end{bmatrix}\begin{bmatrix}27\\15\\14\end{bmatrix}\begin{bmatrix}5\\27\\20\end{bmatrix}\begin{bmatrix}15\\27\\15\end{bmatrix}\begin{bmatrix}14\\5\\27\end{bmatrix}$$

- Augment these vectors into a plaintext matrix -

$$\begin{bmatrix}16 & 7 & 14 & 1 & 27 & 5 & 15 & 14\\5 & 21 & 19 & 18 & 15 & 27 & 27 & 5\\14 & 9 & 27 & 5 & 14 & 20 & 15 & 27\end{bmatrix}$$

- Multiply the plaintext matrix with the cipher matrix to form the encrypted matrix -

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix} X \begin{bmatrix}16 & 7 & 14 & 1 & 27 & 5 & 15 & 14\\5 & 21 & 19 & 18 & 15 & 27 & 27 & 5\\14 & 9 & 27 & 5 & 14 & 20 & 15 & 27\end{bmatrix}$$

Example Continued

- The newly formed matrix contains the ciphertext -

  [-119 -120 -207 -77 -182 -176 -186 -165]
  | 19 30 46 23 29 47 42 32 |
  [135 127 221 78 209 181 201 179]

- To decrypt the matrix back into plaintext, multiply it by the inverse of the cipher -

  [1 0 1] [-119 -120 -207 -77 -182 -176 -186 -165]
  | 4 4 3 | X | 19 30 46 23 29 47 42 32 |
  [−4 −3 −3] [135 127 221 78 209 181 201 179]

  [16 7 14 1 27 5 15 14] [P G N A _ E O N]
  | 5 21 19 18 15 27 27 5 | --> | E U S R O _ _ E |
  [14 9 27 5 14 20 15 27] [N I _ E N T O _]

  Which contains the plaintext -

  PENGUINS ARE ONE TO ONE

THE END

QUESTIONS?