Hill Cipher

Josephine Lee, Shuprovo Sikder

Hill Cipher: Encoding

- the Hill cipher is a polygraphic substitution cipher based on linear algebra
- To encrypt a message:
  - each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26.
- To decrypt the message:
  - each block is multiplied by the inverse of the matrix used for encryption.
- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Hill Cipher: Decoding

<What it is>

Hill Cipher: Weakness/How to Break it

<What it is>

Hill Cipher: Challenges

1.

2.

3.

4.

5.