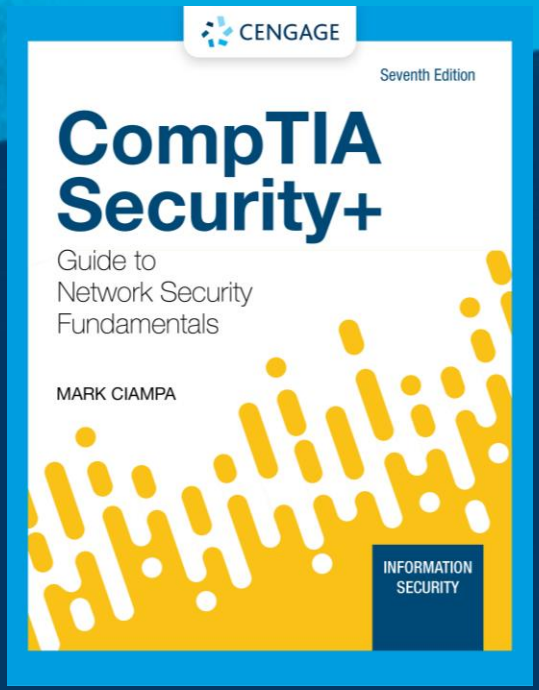


Principles of Cyber Security

Lecture 10: Traditional Ciphers_V

CENGAGE

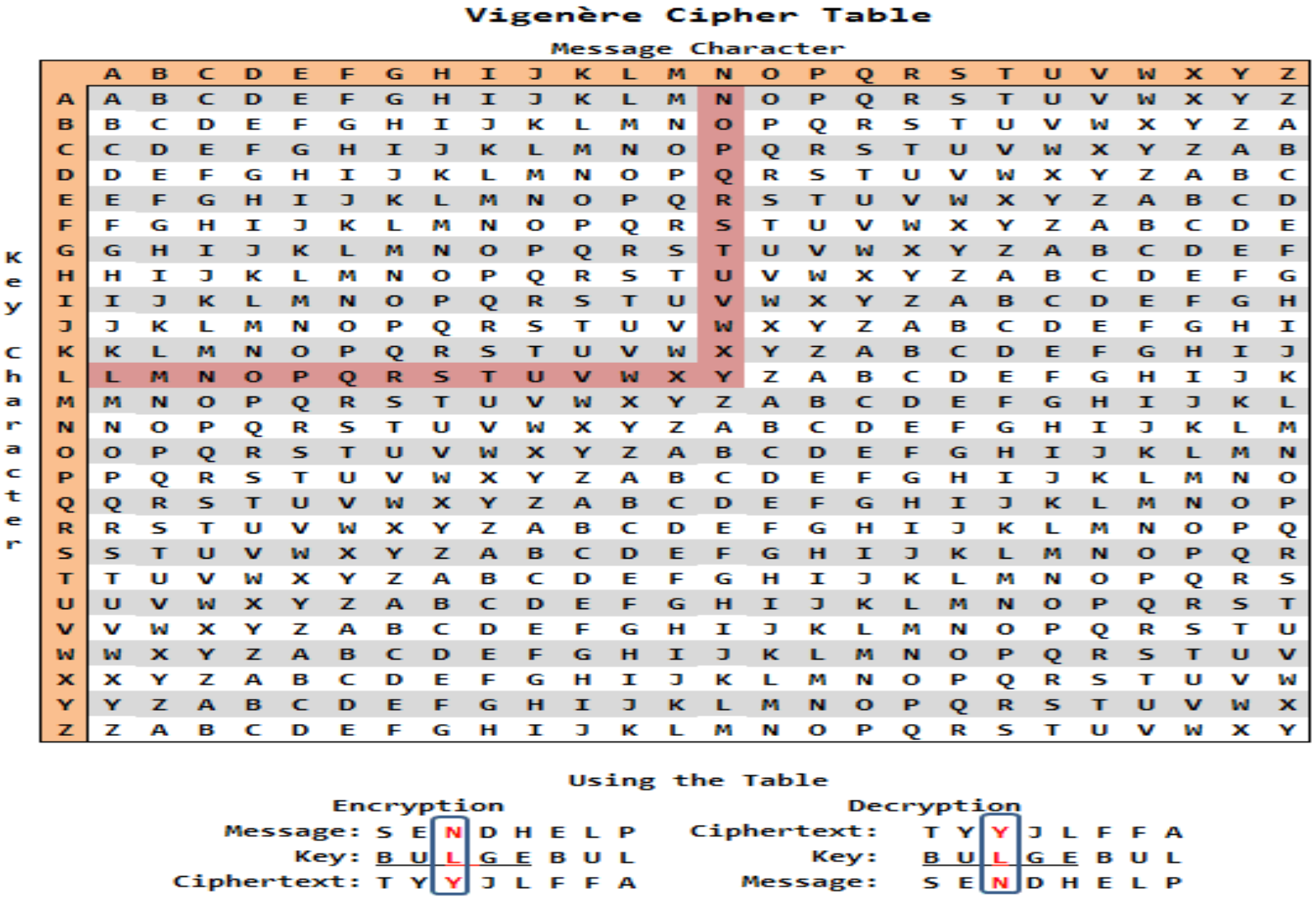
Objectives

11.1 Describe Substitution Ciphers algorithms (Vigenère Cipher).

Vigenère Cipher

- The Vigenère Cipher is an example of a polyalphabetic cipher, sometimes called a running key cipher because the key is another text.
- Start with a key string: “monitors to go to the bathroom” and a plaintext to encrypt: “four score and seven years ago.” Align the two texts, possibly removing spaces:
  - **plaintext:** fours corea ndsev enyea rsago
  - **key:** monit orsto gotot hebat hroom
  - **ciphertext:** rcizl qfkxo trlso lrzet yjoua
    - Then use the letter pairs to look up an encryption in a table
    - (called a Vigenère Tableau or tabula recta).
    - What is the corresponding decryption algorithm?

Vigenère Cipher Table



Using the Table

Encryption

Message: S E N D H E L P
Key: B U L G E B U L
Ciphertext: T Y Y J L F F A

Decryption

Ciphertext: T Y Y J L F F A
Key: B U L G E B U L
Message: S E N D H E L P

CENGAGE

Cryptanalysis on Vigenère Cipher

- The Vigenère Cipher selects one of twenty-six different Caesar Ciphers, depending upon the corresponding letter in the key.
- Running key ciphers are susceptible to statistical analysis. Both key and plaintext are English language strings and so have the entropy characteristics of English. In particular, the letters A, E, O, T, N, I make up approximately 50% of English text. Thus, at approximately 25% of indices, these can be expected to coincide.
- This is an example of a *regularity* in the ciphertext that would not be expected merely from chance.

Thank you

CENGAGE