Week 4
Apply to Computers

School of Information Studies
SYRACUSE UNIVERSITY

Apply the Idea to Computers

- Computers represent data using bits (sequence of 0s and 1s)
- The key is a random sequence of bits as long as the plaintext message
- The encryption method is the exclusive OR (XOR) operation between plaintext bit and the key bit in the same order
  - Cryptographic algorithms can be efficiently implemented by XOR
  - Output is 1 if the two bits differ

Example: Binary Ciphers

Plaintext (English): "WE " (Note: There is a space.)

==> Binary Number bits of "WE " in ASCII (American Standard Code for Information Interchange): "01010111 01000101 00100000"

Plaintext (ASCII): "01010111 01000101 00100000"

$\oplus$ XOR

Key bits: "11001010 01010011 10101101"

Ciphertext: "10011101 00010110 10001101"