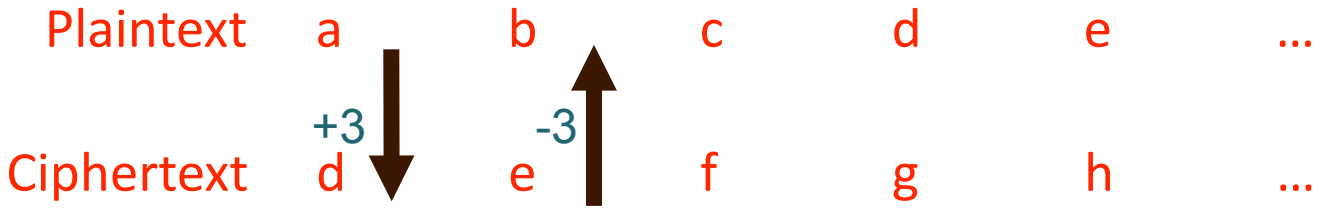
Week 4
Basic Transformations

Basic Types of Transformations

- Transpositions (permutations)
  - Rearrange bits or characters
- Substitution
  - Replace bits or characters
- Transformations are “keyed”
  - A single method can be used with different keys to produce different results
  - To decrypt, one must know the method (algorithm) and the key
  - In general, algorithms are public

An Example of Substitution

- Caesar cipher
  - Rule (algorithm)
    - Shifts the plaintext alphabet by *X* letters to form a cipher alphabet
    - Mono-alphabetic substitution
  - Key (X) = 3



- Example
  - dog ➔ grj

An Example of Transposition

- Rule (algorithm)
  - A cipher transposes a message in blocks of five characters each
  - The key specifies the new order of the characters in the block
- If the key is [45132]
  - Plaintext: “WE ARE HAPPY”
  - Blocked text: “[WE AR][E HAP] [PY]”
  - Ciphertext: “ARW EAPEH PY”
- Decryption is a reverse process

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT