Distributed Systems

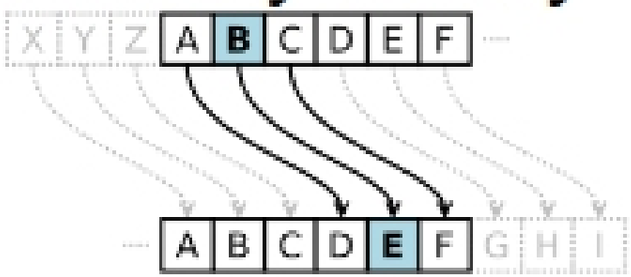
Security and Cryptography Concepts

Assumptions and Guidelines

- Interfaces are exposed
  - How?
- Networks are insecure
  - How?
- Algorithms are available to attackers.
  - We assume they understand RSA, DES, etc.
  - Why not keep them secret?
- Attackers may have have large resources.
  - Why?
- Limit the lifetime and scope of secrets.
- Minimize the trusted base.

Julius Caesar (shift) cipher

- Pick a *key* (a number)
- Shift the letters of the *plaintext* by the key to create the *ciphertext.*
- E.g.
  - Plaintext: Yellow cake
  - Key: 3
  - Ciphertext: Bhoorz fdnh



Source: http://en.wikipedia.org/wiki/File:Caesar3.svg