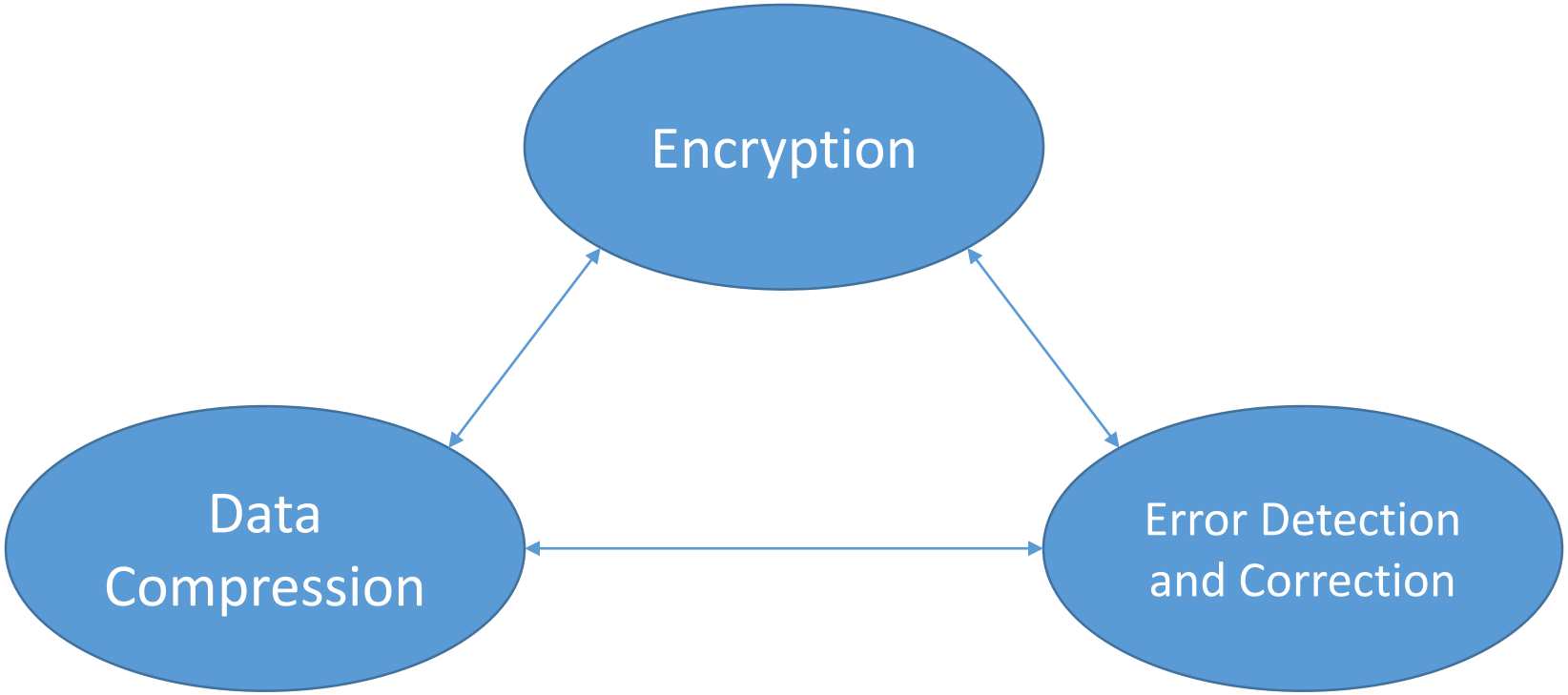
The Three Gnomes

CIS-4040

Peter Chapin

The Three Gnomes



The Three Gnomes

- Encryption…
  - Breaks up patterns and structure in the input
  - Produces output that resembles random data (very high information content)
- Data Compression…
  - Attempts to use patterns and structure to find more compact representation
  - Produces output that resembles random data (very high information content)
- Error Detection and Correction…
  - Adds patterns and structure to help detect and correct errors
  - Produces redundant and non-random output

Rules

- When using multiple gnomes together…
  - Always compress before encrypting
    - Encrypted data is totally uncompressible
    - Compressed plain text is harder to crack… the encryption is hardened
  - Encrypt before applying error detection/correction
    - Encrypting error corrected data may weaken the encryption
    - … but applying error correction to cipher text means the plain text won't have it
  - Remember: *Encryption does not provide data integrity protection!*
  - Error corrected data is more compressible
  - ... but compressed data is more fragile
  - Encrypted data is more fragile