CSEEC: CRYPTO-SYSTEM WITH EMBEDDED ERROR CONTROL

Basics:
- Encryption: data secrecy
- Encoding: data reliability

Challenges:
- Secrecy and reliability are competing concerns

Advantages:
- Achieve data secrecy and reliability, either individually or jointly
- Easy to switch between the two services
- Scale the level of each service

Applications:
- Multi-path routing in WSN
- Multi-cast video streaming

Algorithm

Encryption

Decryption

Parameters:
- Error correction code (C)
- Pseudo Random Number Generator (PRNG)
- Number of rows (r)
- Number of columns (c)
- Number of parity or check columns (P)
- Number of parity used toward reliability (R)

Security:
- Present unreliable PRNG output to an attacker
  - Increase the complexity of PRNG attacks
  - Known plaintext attacks
    \[
    \left(\frac{r x P}{(P - R)}\right)^2 + \left(\frac{r x (c + R)}{(c + R) / 2}\right)^2
    \]
  - Chosen plaintext attacks
  \[
  \left(\frac{r x P}{(P - R)}\right)^2 + \left(\frac{r x (c + R)}{(c + R) / 2}\right)^2 + \left(\frac{r x (c + R)}{(c + R) / 2}\right)^2
  \]

Randomness Tests:
- NIST statistical test suite for random number generator
  - 15 core tests
  - 7 data sets
  - All tests were passed