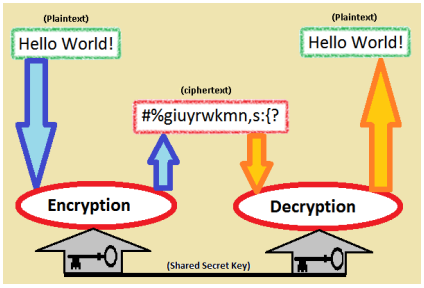
Carnegie Design Systems, Inc.

C3: Correction Code Cryptography

Data Security using Error Correction Codes

What is cryptography?

- "… is the practice and study of techniques for secure communications."



Source: Wikipedia

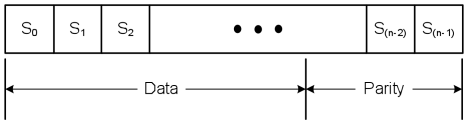
Types of cryptography

- symmetric key
  - block cipher
    - DES / 3DES
    - IDEA
    - AES
  - stream cipher
    - RC4
- asymmetric key
    - Diffie-Hellman
    - RSA
    - Elliptic Curve Cryptography

What are error correction codes?

- techniques to reliably transfer data over unreliable channels
- use supplemental information to detect and correct errors
- developed from information theory and coding theory
- common uses include
  - cell phone communications
  - CD/DVD/Blue-Ray players
  - things with FLASH memory
  - Netflix/You Tube

Reed Solomon Codeword

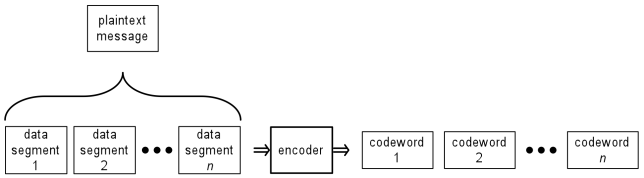


Symbol Size	Codeword Size	# bits	# bytes
4	15	60	7.5
5	31	155	19.4
6	63	378	47.3
7	127	889	111.1
8	255	2040	255
9	511	4599	574.9
10	1023	10230	1278.8

C3 …

- is a family of symmetric key block cipher algorithms
- uses ECC to protect plain-text data
- injects random and deterministic noise to corrupt data
- uses ECC to remove random noise to recover plain-text data

C3 Encryption Process

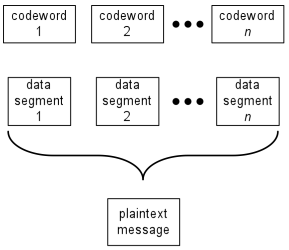


Encoding a plaintext message into plaintext codewords

Encoding a plaintext codeword

C3 Decryption Process

Decoding a ciphertext codeword



Reassembling a plaintext message

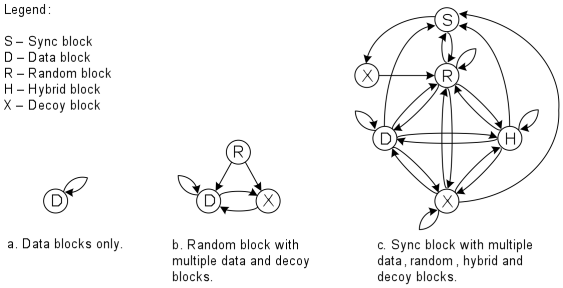
C3++

- state machine control
- heterogeneous blocks
  - Data blocks
  - Random blocks
  - Hybrid blocks
  - Decoy blocks
  - Sync blocks
  - Pad blocks
- varying codeword sizes
- varying noise threshold levels
- varying correction codes

Codeword History Revisited

- a mechanism to represent previous codewords for noise generation
- comparable to cipher block chaining (CBC) and cipher feedback (CFB)
- currently implemented using CRC-32 and CRC-64
- combined 96 bits provide *reproducible* high entropy material for
  - codeword history noise generation
  - state machine transitions
  - block selection
  - codeword size
  - noise threshold level
  - error correction code selection
- encryption: use pristine codeword
- decryption: use recovered codeword

State Machine Control



Examples of possible state transition graphs.

C3 Encryption Architecture

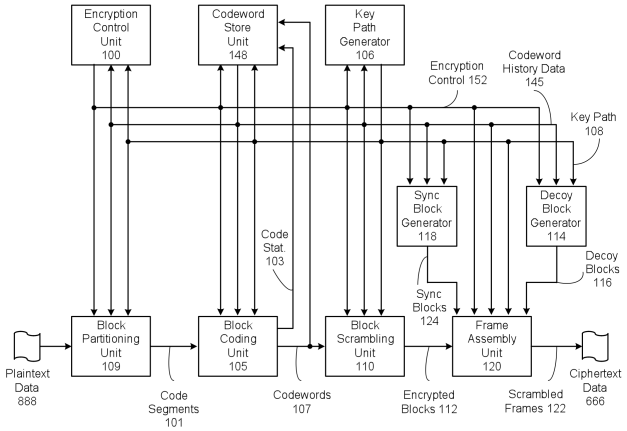


FIG. 1

C3 Encryption Block

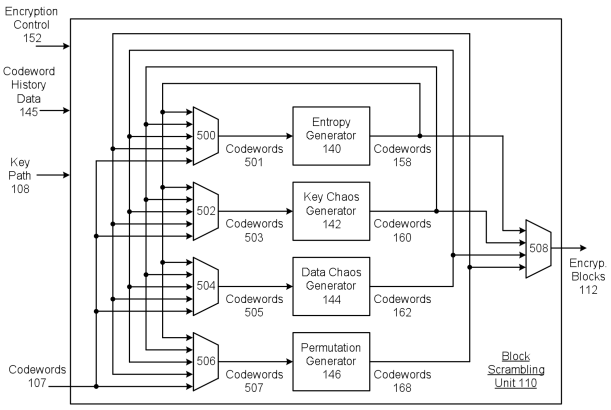


FIG. 5

C3 Decryption Architecture

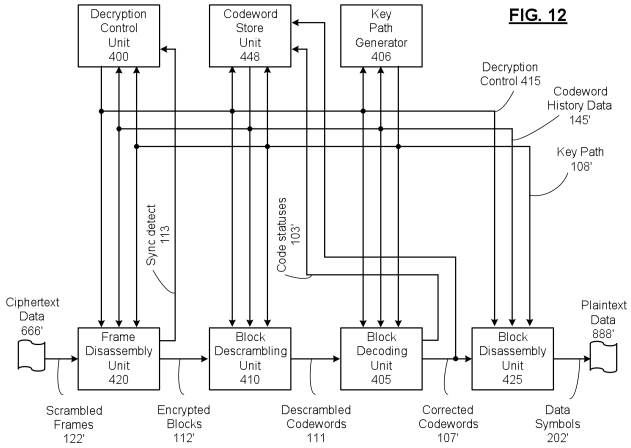


FIG. 12

C3 Decryption Block

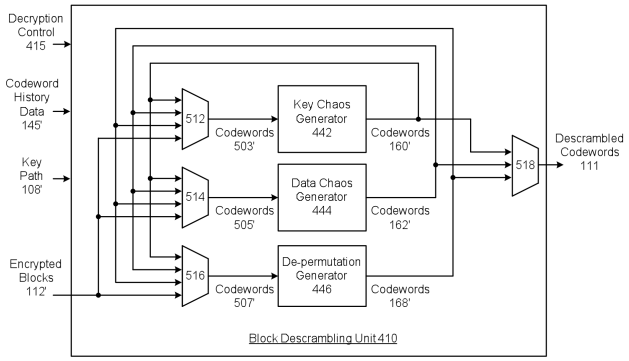


FIG. 14

Test Case 1

UT Tower and Littlefield Fountain

JPG file: 4,861,400 Bytes

Test Case 2

King James Bible (1611 Authorized Version)

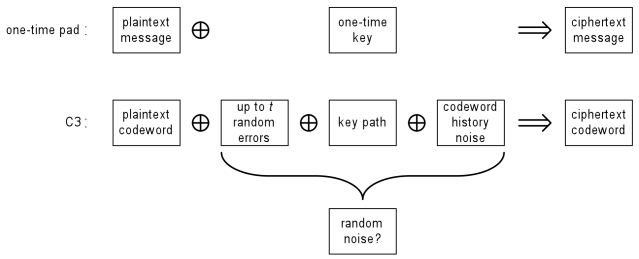
Text file: 4,397,206 Bytes

Source: printkjv.ifbweb.com

Summary

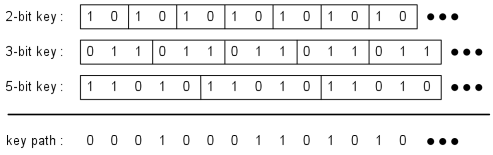
- is a family of symmetric key block cipher algorithms
- uses ECC to protect plain-text data
- injects random and deterministic noise to corrupt data
- uses ECC to remove random noise to recover plain-text data

Food For Thought



Comparing one-time pad and C3 encoding.

A Key Path



A key path generated from a 2-bit, 3-bit and 5-bit key.