Serpent

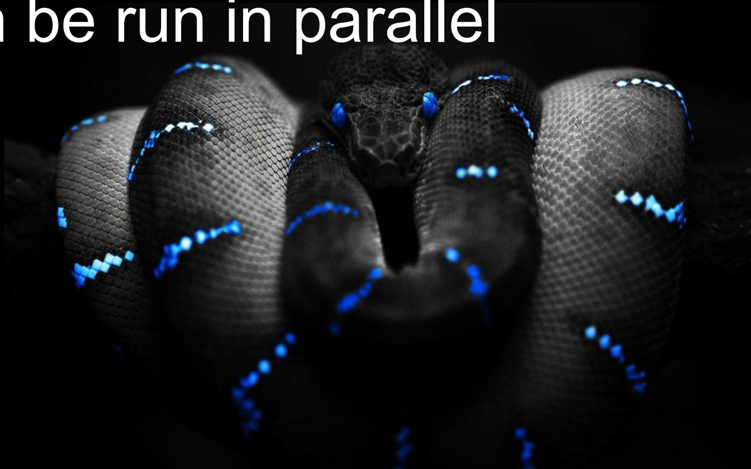
Team Rikki Tikki Tavi:
Nicholas Sereni, Dan Grau, Karl Berger

Background

- Designed by Ross Anderson, Eli Biham, and Lars Knudsen
- A Finalist in the Advanced Encryption Standard(AES) contest, lost to Rijndael
- Serpent 0 was a preliminary design that was changed to Serpent 1 for the AES competition
    - Serpent 1 includes new, stronger S-boxes and a slightly different key scheduling algorithm
- In the public domain, free to use

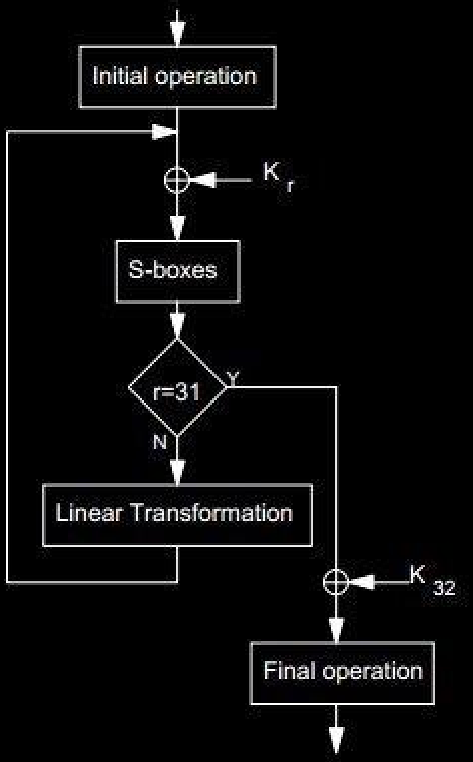
Description

- Symmetric-key Algorithm
  - Same key is used for encryption and decryption
- 32 round block cipher
  - Works on fixed-length group of bits
- 128, 192, 256 bit key lengths supported
- 128 bit block length
  - Broken into 4 32-bit words
  - Designed so all operations can be run in parallel using 32 1-bit slices



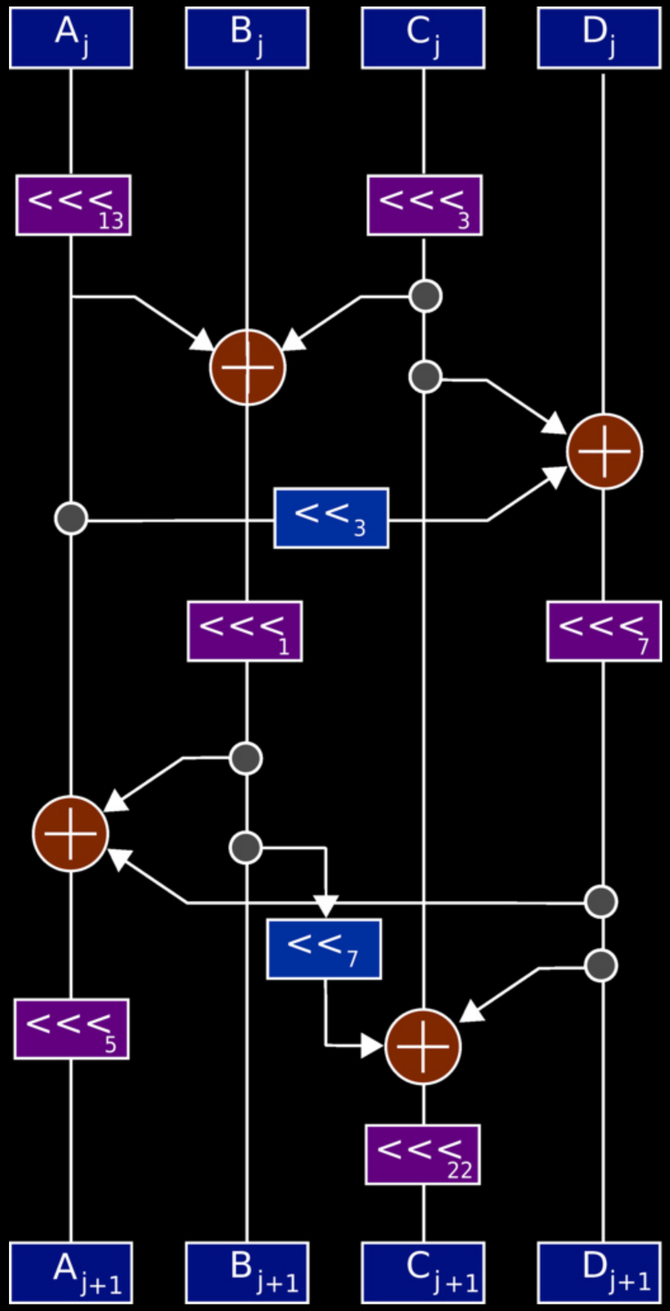
Encryption

- S-boxes in each round are identical
    - Set of 8 unique S-boxes, each used 4 times
- Linear Transformation on 4 32-bit words in parallel
- Within 3 rounds, any change to input has affected every data bit



Linear Transformation

- Rotations
- XORs
- Shifts
    - Always in combination with an XOR



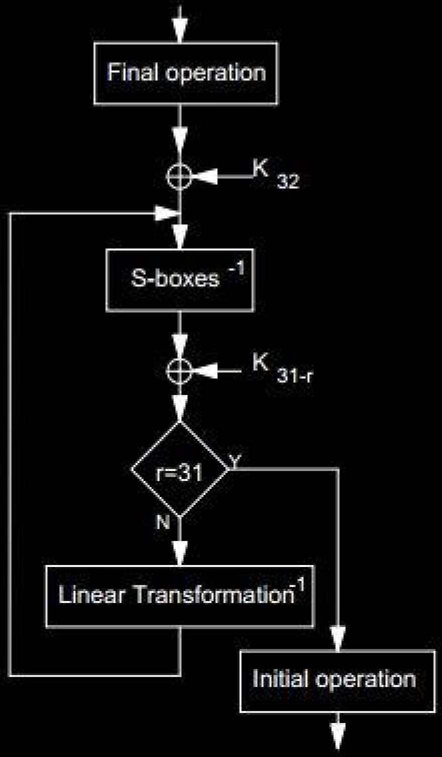
Key Schedule

- Keys shorter than 256 are padded on the right.
- Round keys are then generated by:
  - recurrence operation with previous round keys (and the initial key at start)
  - a pass through one of the 8 S-boxes (starting with S_3 and working down)

$$w_i := (w_{i-8} \oplus w_{i-5} \oplus w_{i-3} \oplus w_{i-1} \oplus \phi \oplus i) <<< 11$$

Decryption

- Inverse the encryption process
  - Invert the linear transformation
  - Apply inverse S-boxes in reverse order



Questions?