Blowfish

A Block Cipher

Team Venture

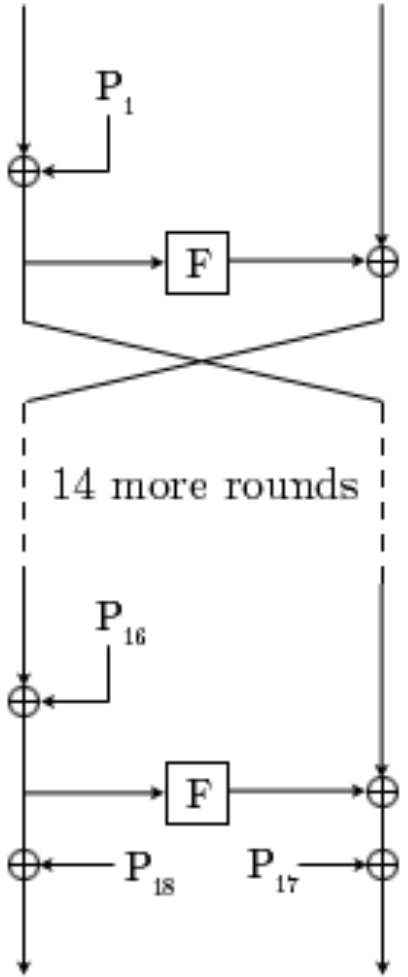
Stephen Yingling

Wesley Wigham

Chad Zawistowski

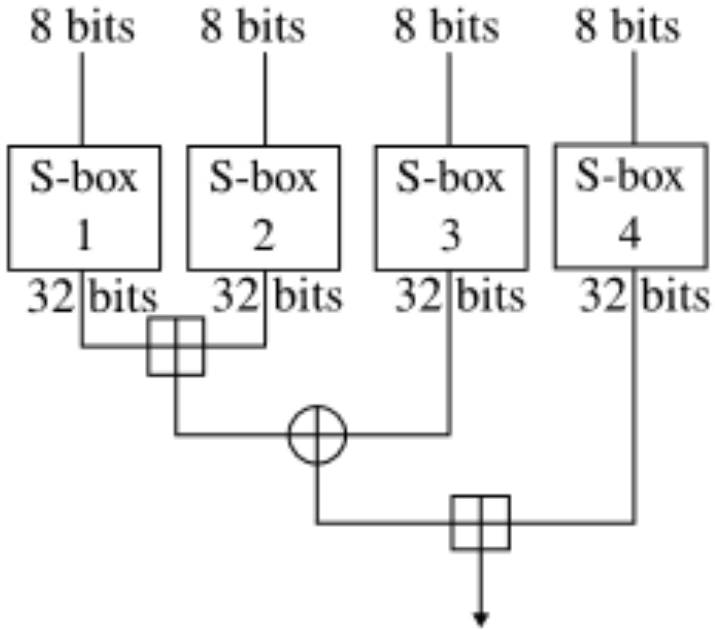
Feistel Structure

- Each block split into two 32-bit halves
- 16 rounds
- P 1-18 are elements in the subkey array



The Function F

- Splits a 32-bit chunk into 4 bytes
- Feeds each byte through an S box
- Added mod 2^{32}, XORed and added mod 2^{32} again



The Function F (Cont)

- Given 4 bytes a, b, c, and d where a is the leftmost byte of the parameter and d the rightmost.
- $F = ((S[0][a] + S[1][b] \bmod 2^{32}) \text{ XOR } S[3][c]) + S[4][d] \bmod 2^{32}$

S-Boxes

- 4 32-bit S boxes with 256 elements apiece

P Array

- 18-element key-dependent subkey schedule

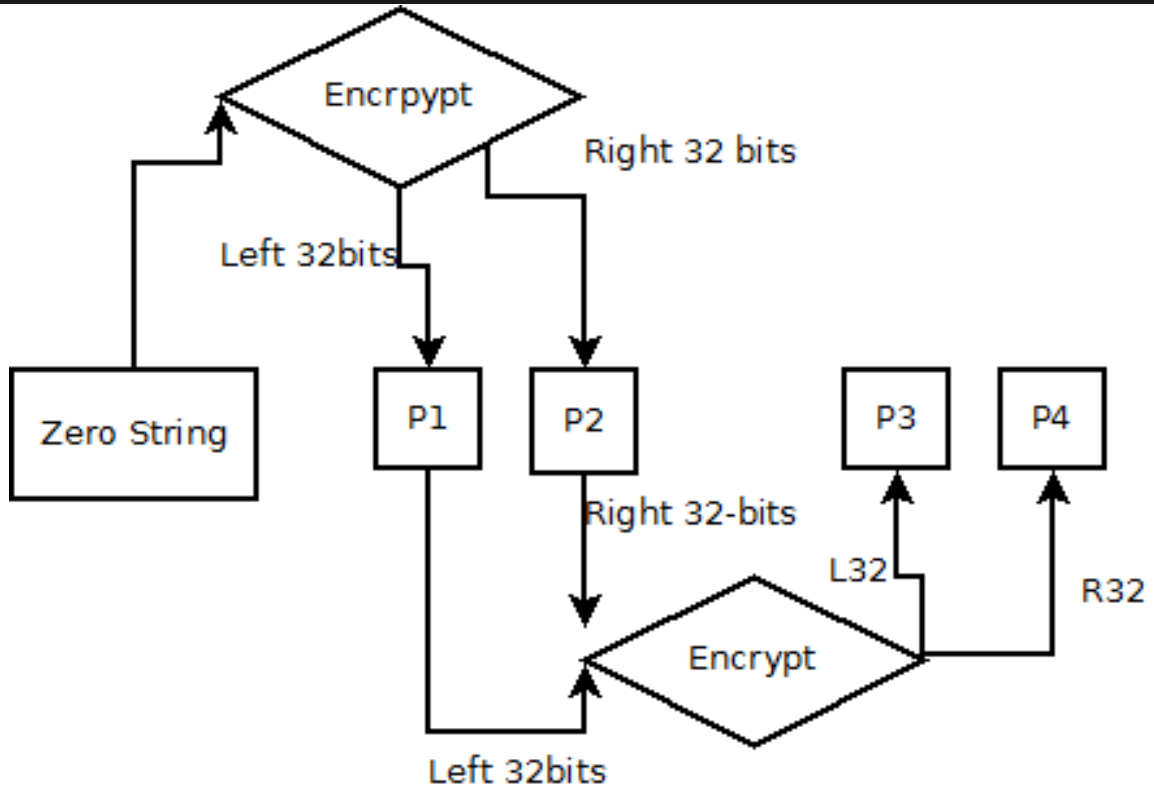
P & S Initialization

- Initialized with the hexadecimal digits of pi
- XOR each element of P with 32 bits of the key, until the entire P array has been permuted by the key
- Encrypt an all 0 bytestring with the algorithm and use the output for the new values of P1 and P2

P & S Initialization Cont.

- Encrypt P1P2 and use output for values of P3 and P4
- Continue this initialization sequence for all entries in P array sequentially, and then all S-boxes

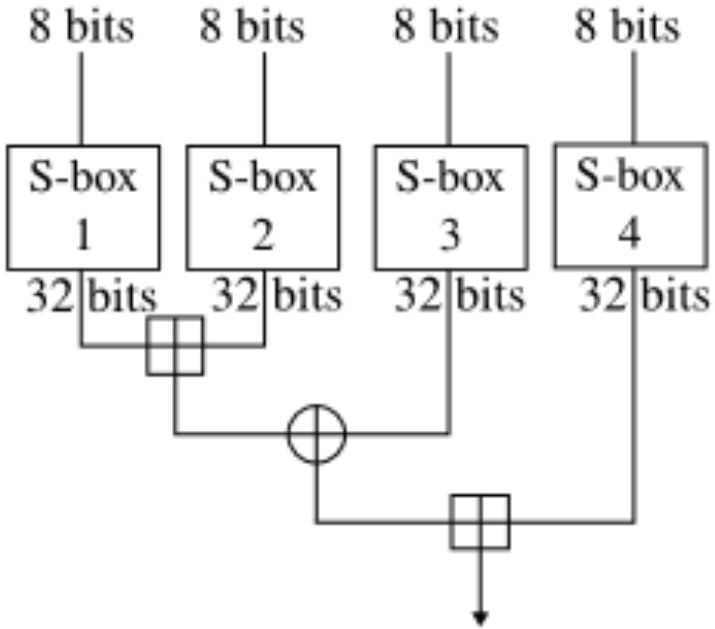
Initialization Diagram

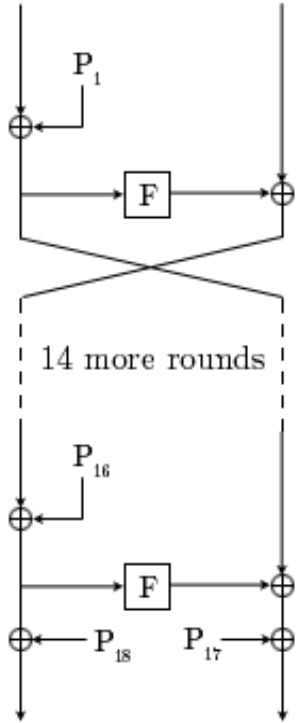


Putting it Together

- Each 64 bit block is divided into a left and right half
- The left half is XORed with P[i] where i is the round number
- The left half is run through the function F
- The output from F is XORed with the right half

Putting it Together (Cont)





Putting it Together (Cont)

- The left and right halves are swapped
- Repeated 15 more times
- The left and right halves are unswapped
- The right half is XORed with P[17]
- The left half is XORed with P[18]
- The halves are recombined.

References

- Main Content from: https://www.schneier.com/paper-blowfish-fse.html
- Feistel Network Diagram and S-box diagram from: http://en.wikipedia.org/wiki/Blowfish_%28cipher%29