Blowfish Encryption Algorithm

Main point

- Introduction
- Structure
- Cryptanalysis
- Comparison
- References

Introduction

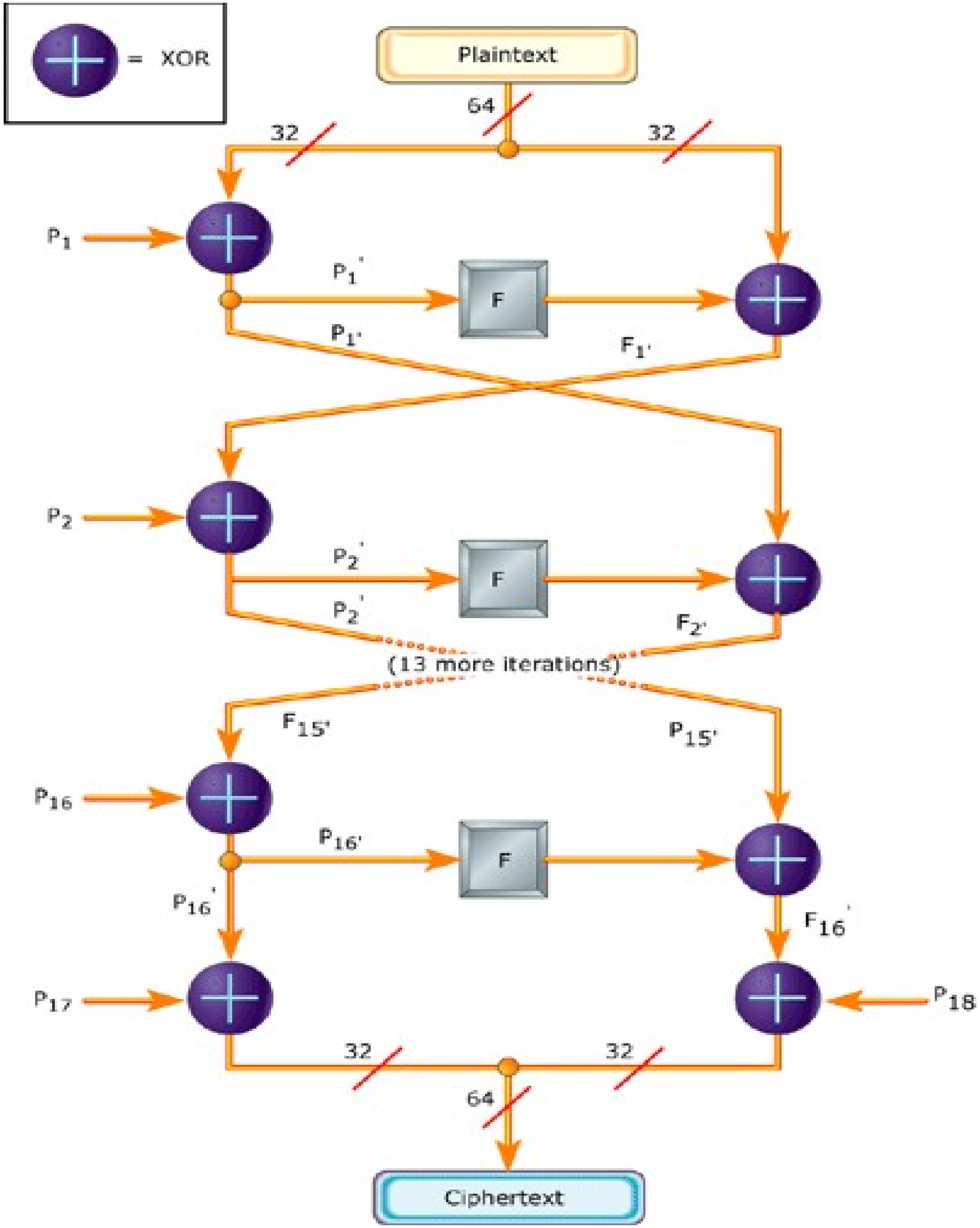
- designed in 1993 by Bruce Blowfish
- 64-bit block cipher with variable length key
- Large key-dependent S-boxes
  - More resistant to cryptanalysis
- Key-dependent permutations
- Diverse Mathematical Operations
  - Combine XOR and addition

Continue

- **Fast**
- **Compact** It can run in less than 5K of memory.
- **Simple to code**
- Easily modifiable for different security levels
- **Secure:** The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length.
- Unpatented and royality-free.

Structure of BF

- Feistel iterated block cipher
- Scalable Key (32 to 448 bits)
- Simple operation that are efficient on microprocessors
  - XOR, Addition, Table lookup, etc
- Employ Precomputable Subkeys
- Variable number of iterations


= XOR
Plaintext
64
32
32
P1
P1'
F
P1'
F1'
P2
P2'
F
P2'
F2'
(13 more iterations)
F15'
P15'
P16
P16'
F
P16'
F16'
P17
P18
32
32
64
Ciphertext

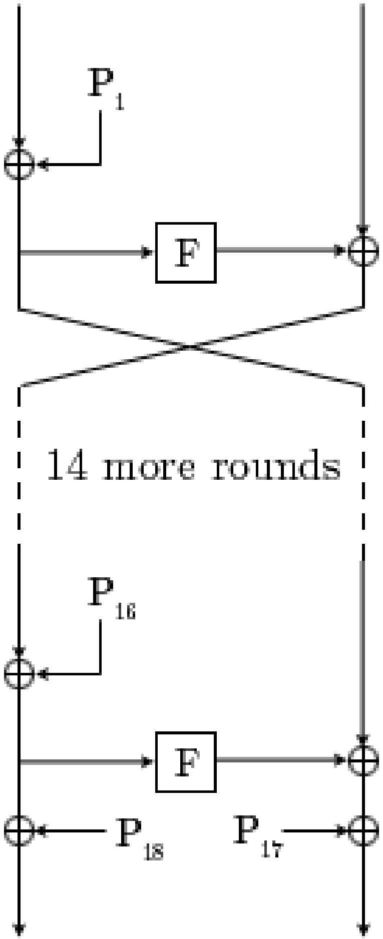
Implementation: Encryption

Arrays:

P – Number of rounds + 2 elements

4 S-boxes – 256 elements

$$L_i = F\left(L_{i-1} \oplus P_{i-1}\right) \oplus R_{i-1}$$
$$R_i = L_{i-1} \oplus P_{i-1}$$
$$L_{17} = L_{16} \oplus P_{18}$$
$$R_{17} = R_{16} \oplus P_{17}$$

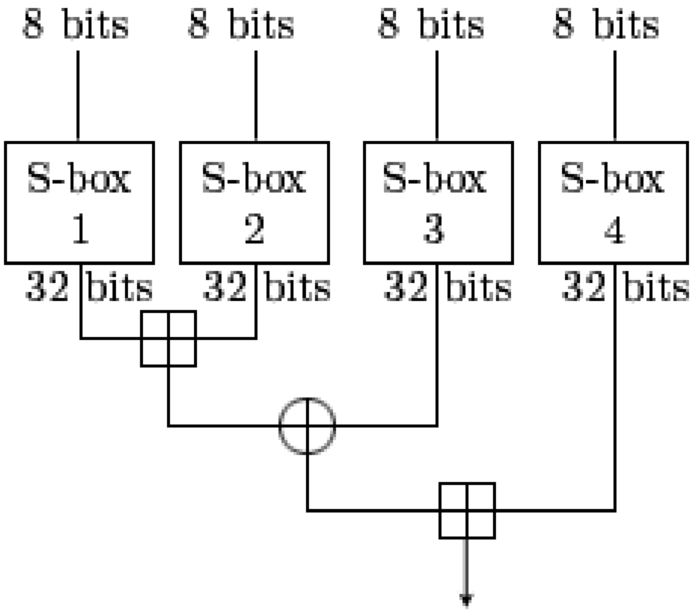


Wikipedia,
http://en.wikipedia.org/wiki/Image:BlowfishDiagram.png

)Implementation: Function F(x

$$F\left(X_{31-0}\right) = \left(\left(S1\left[X_{31-24}\right] + S2\left[X_{23-16}\right]\right) \oplus S3\left[X_{15-8}\right]\right) + S4\left[X_{7-0}\right]$$

Addition is mod 2^{32}



Wikipedia, http://upload.wikimedia.org/wikipedia/en/8/81/BlowfishFFunction.png

Data Encryption

- Divide 64-bits into two 32-bit halves: XL, XR
- For i = 1 to 16
    - XL = XL XOR Pi
    - XR=F(XL) XOR XR
    - Swap XL and XR
- Swap XL and XR (Undo the last swap)
- XR=XR XOR P17
- XL = XL XOR P18
- Concatenate XL and XR

Cryptanalysis

- Differential Attack
  - After 4 rounds a differential attack is no better than a brute force attack
- Weak Keys
  - S-box collisions
  - blowfish algorithm has yet to be cracked as the key size is high, requires 2^{448} combinations

Future Concerns

- Simplifications
  - Fewer and Smaller S-boxes
  - Fewer Iterations
  - On-the-fly subkey calculation
- Twofish
  - AES Finalist
  - 128-bit Block Size
  - More Operations

Comparison

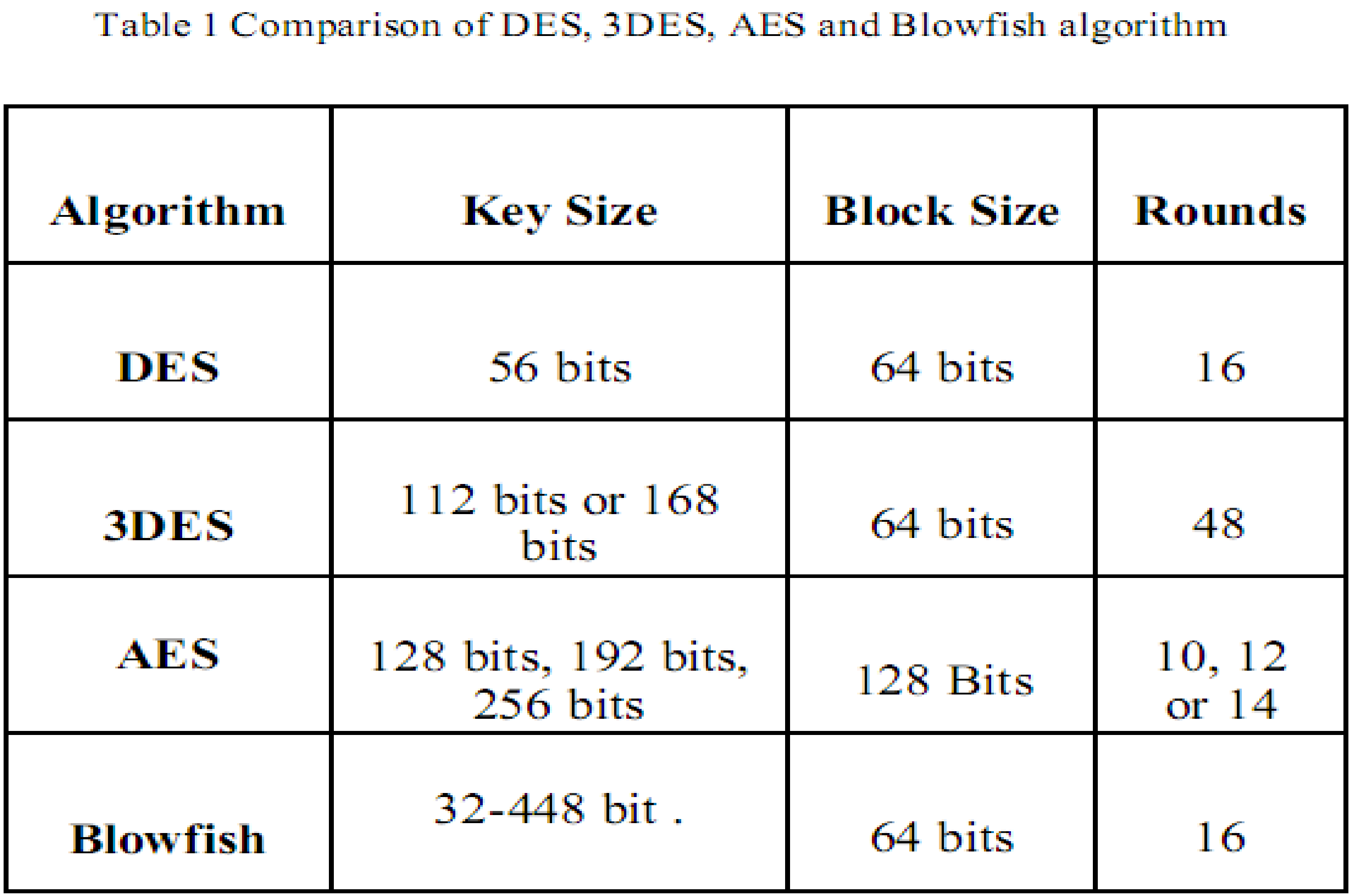


Table 1 Comparison of DES, 3DES, AES and Blowfish algorithm

Algorithm	Key Size	Block Size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 Bits	10, 12 or 14
Blowfish	32-448 bit .	64 bits	16

References

- Wikipedia (for illustrations)
  - http://en.wikipedia.org/wiki/Blowfish_cipher
- Applied Cryptography
  - Bruce Schneier
  - John Wiley and Sons, Inc. 1996
- The Blowfish Paper
  - http://www.schneier.com/paper-blowfish-fse.html