Cryptography and Network Security

BLOWFISH

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	8 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Blowfish
- Summary
- Test your understanding
- References

Introduction

- a symmetric block cipher designed by Bruce Schneier in 1993/94
- Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. *(Wikipedia)*
- Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. *(Bruce Schneier)*
- characteristics
  - fast implementation on 32-bit CPUs, 18 clock cycles per byte
  - compact in use of memory, less than 5KB
  - simple structure for analysis/implementation
  - variable security by varying key size
    - Allows tuning for speed/security tradeoff

Agenda

- Introduction
- Blowfish
- Summary
- Test your understanding
- References

Blowfish Key Schedule

- uses a 32 to 448 bit key
- used to generate
  - 18 32-bit subkeys stored in P-array: P1 to P18
  - S-boxes stored in $S_{i,j}$,
    - i=1..4
    - j=0..255

Blowfish Encryption & Decryption

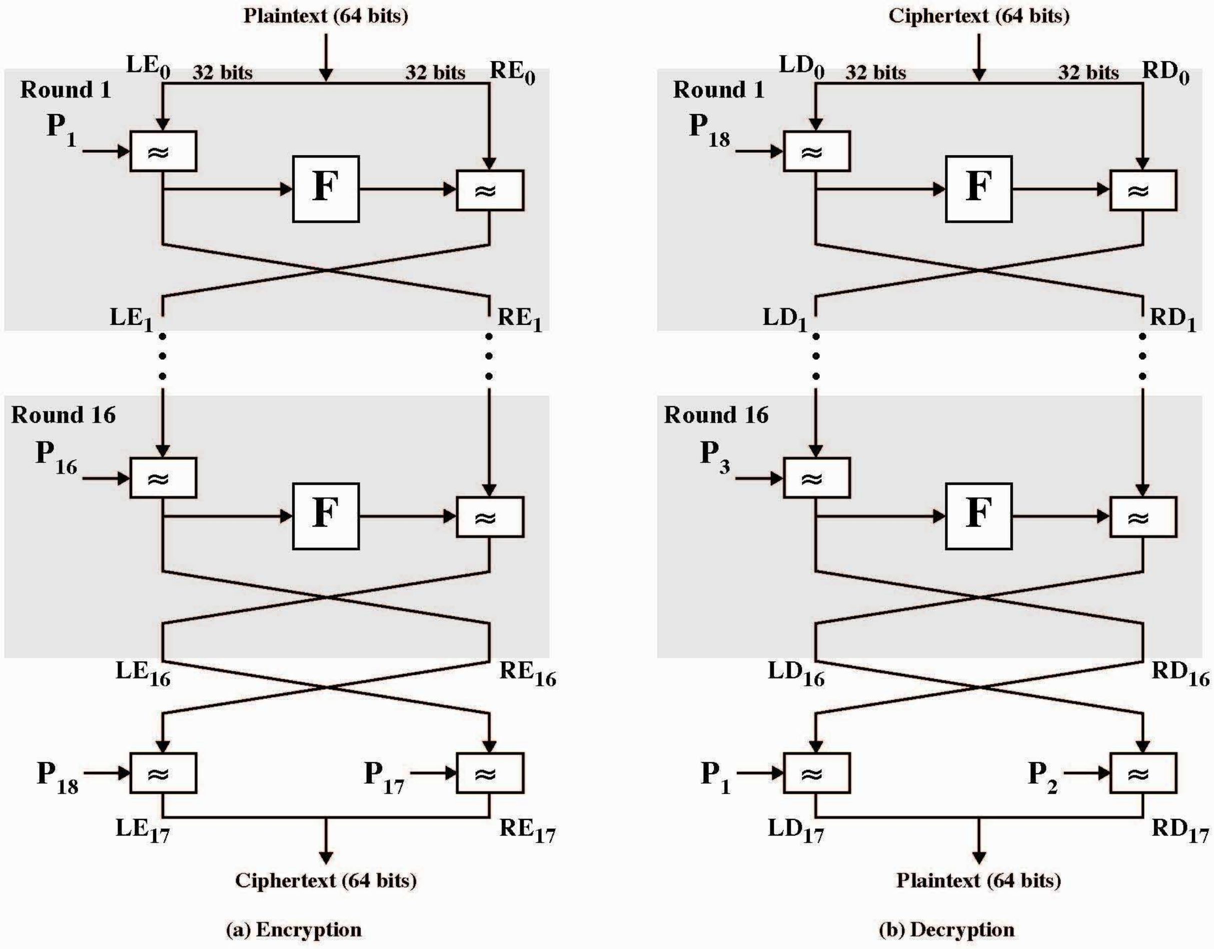

Figure 6.3 Blowfish Encryption and Decryption

Blowfish Encryption

- uses two primitives: addition & XOR
- data is divided into two 32-bit halves L_0 & R_0

```
for $i$ = 1 to 16 do
    $R_i = L_{i-1}$ XOR $P_i$;
    $L_i = F[R_i]$ XOR $R_{i-1}$;
$L_{17} = R_{16}$ XOR $P_{18}$;
$R_{17} = L_{16}$ XOR $i_{17}$;
```

- where

```
F[$a,b,c,d$] = (($S_{1,a}$ + $S_{2,b}$) XOR $S_{3,c}$) + $S_{4,a}$
Break 32-bit $R_i$ into (a,b,c,d)
```

Blowfish Round Structure

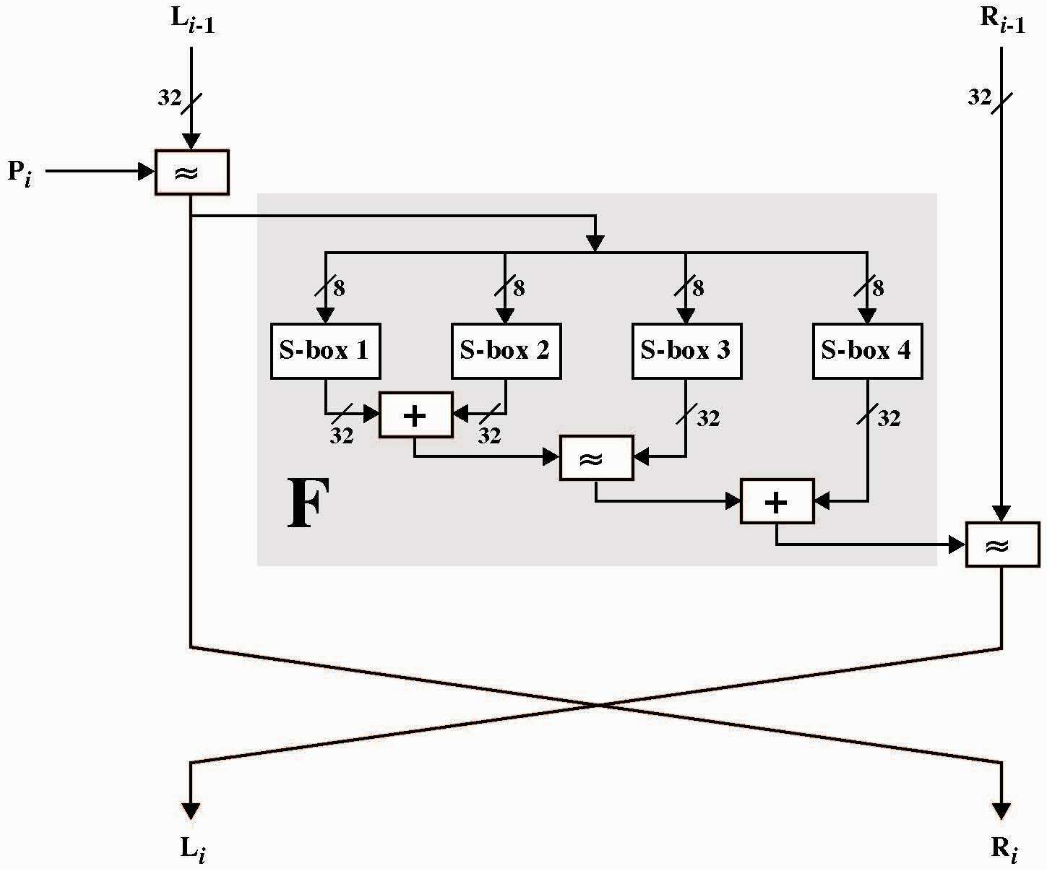

Figure 6.4 Detail of Single Blowfish Round

Agenda

- Introduction
- Blowfish
- Summary
- Test your understanding
- References

Summary

- provided key is large enough, brute-force key search is not practical, especially given the high key schedule cost
- key dependent S-boxes and subkeys make analysis very difficult
  - Very few cryptoanalysis results on blowfish
- changing both halves in each round increases security
  - Some study shows improved avalanche effects

Agenda

- Introduction
- Blowfish
- Summary
- Test your understanding
- References

Test your understanding

1. Explain Blowfish algorithm in detail.

Agenda

- Introduction
- Blowfish
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.