

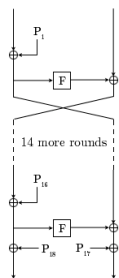
Blowfish

A widely used block cipher

Blowfish

- Designed by Bruce Schneier (1993)
- A variant of it (Twofish) was an AES finalist candidate
- 64-bit block size, 16-round Feistel network structure.
- Variable key size: 32-448 bits
- Key-dependent S-Boxes

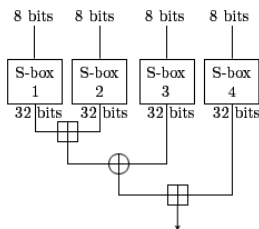
Blowfish Feistel Structure



- Unlike a regular Feistel network, both sides are modified in each round:
- On 1st round,
 - $R_1 = L_0 \oplus P_1$;
 - $L_1 = R_0 \oplus F(L_0 \oplus P_1)$

[http://en.wikipedia.org/wiki/Blowfish_\(cipher\)](http://en.wikipedia.org/wiki/Blowfish_(cipher))

Blowfish round function



- Four 8-to-32 bits S-Boxes are used.
- \oplus indicates XOR
- \boxplus indicates addition mod 2^{32}
- Mixing XOR and addition mod 2^{32} complicates cryptanalysis

[http://en.wikipedia.org/wiki/Blowfish_\(cipher\)](http://en.wikipedia.org/wiki/Blowfish_(cipher))

Key schedule

- In Blowfish, the key schedule has two components
 - Initialization of the S-boxes
 - Initialization of the P-array (proper key schedule of a Feistel network)
- The entries of the P-array and S-boxes are first filled with the fractional part of the expansion of π in hexadecimal.

Key schedule (2)

- $P_1 = 243F6A88$, $P_2 = 85A308D3$, ..., $S_{(4:254)} = 578FD3E3$, $S_{(4:255)} = 3AC372E6$
- The key K is XORED with the P-array, cycling over the key as needed.
- A 64-bit block of 0's is encrypted with the Blowfish algorithm and P_1 , P_2 are replaced with the result, which is then encrypted again and substitutes P_3 , P_4 . This continues until all P-array and all S-Boxes entries are replaced.

Key schedule algorithm

- Initialize P, S With $(\text{frac}(\pi))_{16}$.
- XOR P, S with cyclically extended key.
- For $(P, S) = (P_1, P_2, \dots, S_{(4:254)}, S_{(4:255)})$ Do
 - Replace P_1, P_2 by $\text{Enc}(P; S; \mathbf{0})$
 - Replace P_3, P_4 by $\text{Enc}(P; S; P_1 || P_2)$
 - ...
 - Replace P_{17}, P_{18} by $\text{Enc}(P; S; P_{15} || P_{16})$
 - Replace $S_{(1:0)}, S_{(1:1)}$ by $\text{Enc}(P; S; P_{17} || P_{18})$
 - ...
 - Replace $S_{(4:254)}, S_{(4:255)}$ by $\text{Enc}(P; S; S_{(4:252)} || S_{(4:253)})$

Notes

- The S-boxes are read as simple lookup tables.
 - For instance, if S_2 is given the 8-bit input which is the binary expansion of the integer 127, then $S_{(2:127)}$ is returned.
- 521 applications of Blowfish are required to install a new key:
 - There are 18 P-array entries and 4x256 S-Box entries = total of 1042 entries. Each application of Blowfish replaces two of these entries.

Blowfish facts

- Low key-agility and/or high memory demands makes Blowfish impractical in constrained environments.
- Small (64-bit) blocksize makes it insecure for applications that encrypt large amounts of data with the same key (such as data archival, file system encryption, etc.)
- Implemented in SSL and other security suites.
- Blowfish's speed makes it an good choice for applications that encrypt intermediate amounts of data, such as typical of network communications (e-mail, file transfers).
- No attacks on Blowfish are known that work on the full 16-round official version (certain attacks recover some information from versions with up to 14-rounds).
