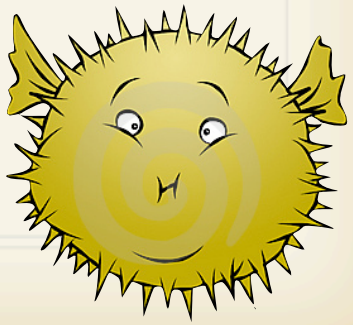
The Phone Phreakers

Achilles Tziazas - apt0048@rit.edu
Ed Wolf - efw6415@rit.edu

www.cs.rit.edu/~efw6415

The Blowfish Cipher

- Written in 1993 by Bruce Schneier
- No cryptanalysis discovered yet
- Designed originally to replace DES because of it's vulnerable 56-bit key
- Takes a 32-448-bit key, which permutes 4 S-boxes and 1 P-box, making key recovery difficult.
- 64-bit block encryption
- A Feistel network consisting of 16 rounds
- Unpatented and in the public domain
- Very Fast, except when changing keys
- Simple implementation



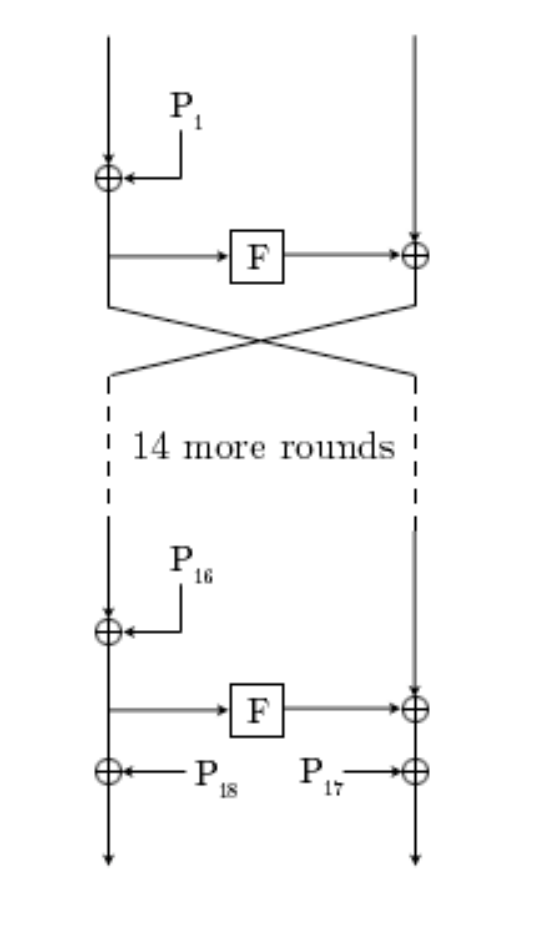
Algorithm Strengths

- A variable key generates strong subkeys from the S-boxes/P-box so that recovery is difficult
- 64 bit block encryption
- Fiestel Network adds to complexity of the algorithm

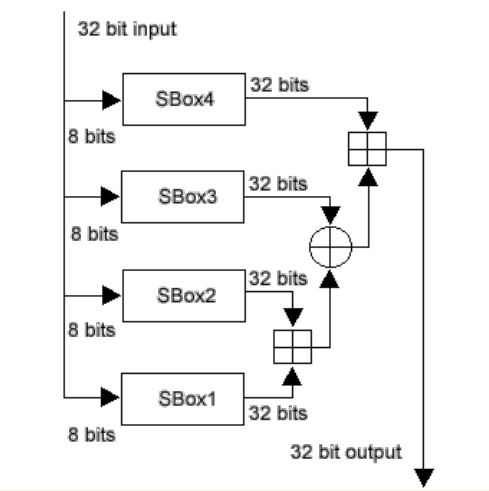
The Software

- Written in Java. Uses the command line for now.
- Takes an input of the following:
  - 0-448 bit key, of 8-bit increments
  - Plaintext (ASCII) or Ciphertext (HEX)
  - Flags [-e] encrypt or [-d] decrypt
- Prints the output round by round so you can see where the algorithm is in its implementation
- Uses Hex strings to convert to integer, then XOR
- Generates subkeys for each key as specified in the design specs of the algorithm

The Software (Continued)



The Algorithm



F-Function

- Software is designed to show what is happening in every step of the algorithm

DEMO

What We Learned

- In the Java language, there is no good support for large Hex operations. You need to convert everything to hex strings, convert those to integers, then perform the XOR. We used the Hex class from the Computer Science Course Library at: http://www.cs.rit.edu/~ark/cscl/doc/edu/rit/util/Hex.html
- The Blowfish cipher to this day is still a good alternative to DES, but Twofish provides 128-bit block encryption and is therefore recommended
- Over 150 different applications

Future Work

- Investigate ways to speed up subkey generation
- Research further possible attacks on the algorithm for key discovery
- Re-write program in a language more suitable for bitwise operations and unsigned integers
- Possible GUI implementation
- Variable input plaintext. As of now we only allow 16 character ASCII input plaintext and 32 chartacter HEX input cyphertext.

Bibliography

- Schneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." Dec. 1993. 22 Mar. 2008 <http://www.schneier.com/paper-blowfish-fse.html>.
- Schneier, Bruce. "The Blowfish Encryption Algorithm -- One Year Later." Schneier. Sept. 1995. 22 Mar. 2008 <http://www.schneier.com/paper-blowfish-oneyear.html>.
- "Blowfish Encryption." BletchleyPark. 4 May 2008 <http://www.bletchleypark.net/cryptology/blowfish.html>.
- "Blowfish (Cipher)." Wikipedia. 3 Mar. 2008. 4 May 2008 <http://en.wikipedia.org/wiki/Blowfish_(cipher)>.