**Team Members:** Achilleas Tziazas - apt0084@rit.edu
Ed Wolf -efw6415@rit.edu
**Team Name:** The Phone Phreakers
**Team Website:** http://www.cs.rit.edu/~efw6415/

**Topic Description:**

Our team project will focus our presentation on the Blowfish Cipher. This Cipher, which was developed in 1993 by Bruce Schneier is a public domain symmetric block cipher that is structured after a Feistel network. From the developer's website, the Blowfish Cipher was developed to act as a replacement for DES and has the following specifications:

- **Block Size:** 64 bits
- **Key Size:** 32 - 448 bits
- **Rounds:** 16

Our intention for this topic is to give an overview of the structure of the algorithm that is use to encrypt data, the weaknesses associated with this algorithm, and how this cipher had real world applications.

**Topic Citations:**

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. "Blowfish." Schneier.Com. 22 Mar. 2008 <http://www.schneier.com/blowfish.html>.

Schneier, Bruce. "The Blowfish Encryption Algorithm -- One Year Later." Schneier.Com. Sept. 1995. 22 Mar. 2008 <http://www.schneier.com/paper-blowfish-oneyear.html>.

"Standard Cryptographic Algorithm Naming." ZetNet User Pages. 22 Mar. 2008 <http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html>.

**Software Description:**

The software demonstration that we plan to deliver will show how a plaintext message can be encrypted with the Blowfish cipher. The software will have the following demonstrations:

Demo 1:
The software will show the message in its plaintext, encrypted and decrypted state.

Demo 2:
The software will show on a round by round basis the current state of a plaintext message, as well as the keys and inputs used to generate the next output. Overall this will demonstrate the encryption of the message.

Demo 3:

The software will show on a round by round basis what the current state of an encrypted, as well as the keys and inputs used to generate the next output.  Overall this will demonstrate the decryption of the message.