Project #1

This project is about developing and implementing a 1R differential attack on the 8-round DES variant you were given. You will work in groups of two, and implement your attack in C. The project consists of two phases:

Phase 1: Design of the attack

1. Study the attack of Biham and Shamir on DES with an iterative characteristic (Section 6 and 6.3, [1]).

2. Find a new 2-round iterative characteristic to attack your DES variant. (Use the difference tables on p.91–98 in [1].)

3. Develop an attack using this characteristic. Study the signal-to-noise ratio and the plaintext requirement of your attack.

Phase 2: Implementation of the attack

1. Implement your attack to find the 8th round key on your active s-boxes.

2. Bonus: Find the whole 8th round key using more characteristics, and find the remaining eight bits of the main key by exhaustive search.

Deadlines:

23 October 2012: Phase 1 complete, progress report due

6 November 2012: Phase 2 complete, final program due

Bibliography

[1] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Technical report CS90-16, Weizmann Institute of Science, July 19, 1990.