**Description for: CS 492 Homework 5**

Advanced crytoanalysis

**You may work in groups of 2**

Complete the problems below and submit this word document with the solution to the questions here.

Name(s):

Question 1 (25 pts): Differential Cryptoanalysis:

What is differential cryptoanalysis and how is it applied to a problem in general (ie. Not mathematic formulas, but how you would apply the approach to some new crypto problem.)

Differential cryptoanalysis was developed to attack DES by focusing on the non-linear part (S-Box). Idea is to compare input & output differences. If you know the inputs then you can determine the input difference without knowing the key. The input difference is used in conjunction with the output difference to be (almost) the input difference to the next round. Ultimately, the goal is to chain differences through rounds. Plain text is chosen to turn off the rest of the S-boxes except the one attacked.

Question 2: Linear Cryptoanalysis:

1. [25 pts] What is linear cryptoanalysis and how is it applied to a problem in general (ie. Not mathematic formulas, but how you would apply the approach to some new crypto problem.)

Goal is to attack non-linear portion of Feistel Cipher by using mathematical approximation of biases in S-Boxes. Use mathematical approximation of S-boxes to determine bits of key with greater than 50% probability. To do this - take S-boxes in non-linear portion and approximate them as mathematical functions even if they aren’t truly mathematical functions. (ie. If we know what “comes out of” 01 75% of the time then that provides us with information that we can use to find out what the keybits are rather than brute force). We are trying to approximate the outcome of the s-boxes by linear equations of what the input bits happen to be. Determine bits of key with probability greater than 50%. With DES, everything is linear except for S-boxes (if we know where a bit is – it is deterministic. Trace where bits go until they get to S-boxes. Select the portions of S-box that have the largest biased, then trace the bits every single round to get approximation.

1. [50 pts]Complete the linear analysis table of the following S-box indicating the best approximation of y0 and y1

S-Box

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 00 | 01 | 10 | 11 |
| 0 | 10 | 11 | 00 | 11 |
| 1 | 01 | 01 | 01 | 10 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Y0 | Y1 | Y0 ⊕ Y1 |
| 0 | 4/8 | ***5/8*** | ***5/8*** |
| X0 | ***1/4*** | ***3/4*** | ***4/4*** |
| X1 | 2/4 | 2/4 | 2/4 |
| X2 | ***3/4*** | ***3/4*** | 2/4 |
| X0 ⊕ X1 | ***1/4*** | ***3/4*** | 2/4 |
| X0 ⊕ Y2 | 2/4 | ***4/4*** | 2/4 |
| X1 ⊕ X2 | ***1/4*** | ***3/4*** | 2/4 |
| X0 ⊕ X1 ⊕ X2 | 2/4 | 2/4 | 2/4 |