

HW # 6

Due Date: Wednesday, October 17th, 2007, 7:20 PM
at the beginning of class

Reading Assignment:

- W. Stallings, *Cryptography and Network Security*, Sections 3.1-3.3, 3.5, 6.1
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapter 7.4

Problems:

Please use very legible handwriting or type the answers. In either case you can draw diagrams and write formulae by hand but they have to be legible and the diagrams have to be labeled clearly. Answers that neither the TA nor the instructor can read receive 0 points. You are allowed to work in groups on these problems but you have to **write your own solution** in your own words. Copying the solution from someone else (in class or otherwise e.g. Internet) is a serious honor code violation and will be treated as such.

1. (20 points) A popular approach for determining the security of a private-key cipher against a brute force attack is estimating the cost of a key search machine. We will study this approach in this problem.

Assume a DES chip with pipelined hardware so that one encryption (or key test) can be done in one clock cycle and the chip can be clocked at 200 MHz. The production of this chip (ASIC) has a one-time cost of \$50,000 for making the masks and then each chip costs \$9.

- (a) How many chips must run in parallel for an **average search** time of 6 hours.
- (b) What is the cost for such a machine. Assume that for each chip we have to calculate 100% overhead on the chip price (not the one-time cost) for glue logic and building the machine?
- (c) We try now to take the advances in computer technology into account. Predicting the future tends to be tricky, but the estimate usually applied is Moore's law, according to which computer power doubles every 18 months. How many years do we have to wait until a key search machine can be build for DES with an average search time of 1 hour? We assume that 2,000 DES chips are used in parallel in our machine.

2. (8 points) As shown in the lecture, one important property which makes DES secure is that the S-boxes are non-linear. In this problem we are going to verify this property by computing the output of S1 for several pairs of inputs. Show that $S1(x_1) \oplus S1(x_2) \neq S1(x_1 \oplus x_2)$, where “ \oplus ” denotes bitwise XOR, for:
- (a) $x_1 = 000000, x_2 = 100010$
 - (b) $x_1 = 010011, x_2 = 101111$
3. (10 points) What is the output of the first iteration of the DES algorithm when the plaintext is all zero and the key is all zero?
4. (22 points) Remember that it is desirable for good block ciphers that a change in one input bit effects many output bits (diffusion or avalanche effect). We try now to get a feeling for the diffusion property of DES. We apply now a plaintext input that has a “1” at bit position 57 and all other bits are zero and the key are all zero. (Note that the input word has to run through the initial permutation.)
- (a) How many S-boxes get different inputs compared to the case considered in the previous problem?
 - (b) What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?
 - (c) Which output bits change here? Does this fulfill the S-box design criteria?
 - (d) What is the output after the first round? Hint: only follow the changed bits, the others have the same value as in the previous problem.
 - (e) How many output bits have actually changed compared to the case when the plaintext was all zero. (Observe that we only consider a single round here. There will be more and more output differences after every new round. Hence the term *avalanche effect*).