

## CPSC/ELEN 689 Topics in Network Security

Spring 2004

### Homework 1

Due: Tuesday, February 24, before class

Please give concise answers, and **type them neatly**.

**Problem 1** Alice and Bob want to check whether they share the same secret key. Alice generates a random bit string  $r$  of the same length as the key, xors it with the key and sends the resulting bit string  $s$  to Bob. Then Bob xors his key to  $s$  and sends the resulting random string back to Alice. Alice checks whether the string that she has received from Bob coincides with the string  $r$  that she had created. Alice announces the result of her comparison. Is there a flaw in this scheme?

Answer this question in 1-2 sentences.

**Problem 2** In the lectures, we have encountered the birthday paradox several times; this exercise allows you to discover some background information.

Suppose we want to find a collision of a good cryptographic hash function  $h$  that can produce  $v$  possible values. So our goal is to find two messages  $m$  and  $m'$  such that  $h(m) = h(m')$ . We randomly choose sufficiently long messages  $m_1, m_2, \dots$  and compute their hash value. A good cryptographic hash function produces uniformly distributed values in such a case. The probability that no collision occurs among the  $n$  values is approximately

$$\Pr[h(m_1), \dots, h(m_n) \text{ take all different values}] \approx e^{-n^2/2v},$$

assuming that  $v \gg n$ .

Let  $n_{\text{med}}$  denote the median of the number of the trial on which the first collision occurs. We can define this number  $n_{\text{med}}$  by the relation

$$\Pr[h(m_1), \dots, h(m_{n_{\text{med}}}) \text{ take all different values}] = 1/2.$$

Your task is to show that  $n_{\text{med}} \approx 1.2\sqrt{v}$

To get a feeling for the power of collision attacks, check out the neat applet at <http://www-stat.stanford.edu/~susan/surprise/Birthday.html>

**Problem 3** Take a graylevel image of 8 bit depth in pgm format (or some other simple image format that directly represents the gray values without complicated encoding). Take DES and encrypt the image (a) using electronic codebook (ECB) mode, and (b) using cipher block chaining (CBC) mode. Include original, ECB and CBC mode images in your document, that is, visualize the result of your experiment. Explain the result of your experiment in technical terms,

and explain the cryptographic relevance. Your answer should not exceed 3-4 sentences.

You can use, for example, the cryptographic library contained in openssl for this experiment, [www.openssl.org](http://www.openssl.org). Incidentally, this library is interesting since it contains implementations of all cryptographic primitives that we have discussed so far.

**Breaking a Feistel Cipher.** The following problems discuss a small single-round Feistel cipher that operates on a block of 64 bits. The plaintext is split into two blocks `left` and `right` of equal size. The left part is replaced by `left = left  $\oplus$  f(K, right)`. The function  $f$  consists of an expansion function that replicates bits of `right`, an xor of the key, followed by nonlinear S-boxes. It is similar to a single step in DES, but the permutation after the S-boxes is omitted.

The source code realizing the cipher is available from the course web page (but the key settings `k[0], \dots, k[7]` are different). And an executable it available as well.

**Problem 4** Draw the expansion function that maps 32 bits into 48 bits. You can omit the middle part, but give enough detail so that input bits 1-6 and 26-32, and all their output bits are covered.

**Problem 5** (a) Determine an input difference of  $f$  that affects just the S-box  $S_2=S[1]$ , and no other S-boxes. (b) Tabulate the XOR profiles for  $S_2$  for this input difference. (c) Derive a characteristic of  $S_2$  for (one of) the most likely output differences, given the input differences chosen earlier. (d) Find a pair of inputs satisfying the characteristics for the posted cipher. (e) Determine the restricted set of potential key settings of  $K[1]=K[2]$  using your characteristics and this input pair.

**Problem 6** Determine the key settings in the cipher using differential cryptanalysis. Give a (very brief!) outline how you have accomplished that (for instance, what difference pairs have you used, and how many key settings remained after that).

Note: *Exhaustive search or other methods* can be used to get the key settings as well, but that would completely miss the point of this exercise.

**Reference:** E. Biham, A. Shamir: Differential Cryptanalysis of DES-like Cryptosystems, J. Cryptology, 4(1), pp. 3-72, 1991

<http://www.cs.technion.ac.il/~biham/publications.html>