KTH Computer Science and Communication

Homework I, Foundations of Cryptography 2014

Before you start:

1. The deadlines in this course are strict. This homework set is due as specified at `http://www.csc.kth.se/DD2448/krypto14/deadlines`.
2. Read the detailed homework rules at `http://www.csc.kth.se/DD2448/krypto14/handouts/solution_rules.pdf`.
3. Read about I and T-points, and how these translate into grades, in the course description at `http://www.csc.kth.se/DD2448/krypto14/handouts/course_description.pdf`.
4. You may only submit solutions for a nominal value of 50 points in total (summing I and T points).

The problems are given in no particular order. If something seems wrong, then visit `http://www.csc.kth.se/DD2448/krypto14/handouts` to see if any errata was posted. If this does not help, then email `dog@csc.kth.se`. Don't forget to prefix your email subject with `Krypto14`. We may publish hints on the homepage as well.

1 (12T) All students should have received an email with subject `Krypto14 HW1 Problem 1` containing three ciphertexts, with some hints on the language of the plaintexts and alphabets used.[1] Find the plaintext of each ciphertext.

One successful attack gives $2T$, two successful attacks give $6T$, and three successful attacks gives $12T$. It does not matter which of the ciphertexts are attacked, only the number of successful attacks is considered. An attack is considered successful if you report your solution as explained below. Report partial success or interesting findings for partial credit.

You must report your solution in two ways:

1. A reasonably large prefix of the plaintext as part of your written solution, where you also give a brief description of how you proceeded in your attacks.

2. You must reply to the challenge email with the source of all the programs you wrote to find the plaintexts. Please put your files in a directory named `<lastname>_<firstname>` (with small letters and turn åääö into aao) and turn it into a single `.tar.gz`-file. (No tarbombs please.)

In addition to the general rules on cooperation, the following rules apply for this problem: (1) do not show your ciphertexts to others, (2) do not use or copy parts of any program found on the Internet for analyzing ciphertexts. You may, however, discuss within your study group. Please note that each student receives unique ciphertexts encrypted with unique keys and that the same cryptosystems are not used for all students.

[1] If this is not the case, then I don't have your personal data. Please email me at dog@csc.kth.se.

2 (10I) Implement the AES cipher. A detailed description is found on Kattis. `https://kth.kattis.scrool.se/problems/oldkattis:aes`. Feel free to consult different sources on how to make an efficient implementation, but any borrowed ideas should be explained briefly in the solutions submitted on paper. You must also be prepared to explain in detail what you did and why at the oral exam. Make sure that your code is commented and well structured. Up to 10I points may be subtracted if this is not the case.

3 (2T) List the indices of the functions below that are negligible functions. For example, if you think $f_1(n)$ and $f_2(n)$ are negligible and no other, then your answer should be "1, 2".

$$f_1(n) = n^{-2} \quad f_2(n) = 1/\sqrt{n} \quad f_3(n) = 3^{-n} \quad f_4(n) = 2^{-(\log(n))^2} \quad f_5(n) = n^{-\frac{1}{n+1}}$$

To get any points your answer must be completely correct, i.e., this is an all-or-nothing problem. You do not need to motivate your answer for this problem.

4 In each case below, say as much as you can about the entropy of Y and motivate your answers. Make sure that you do not assume anything about the distribution of Y that is not stated explicitly. More precisely, for each description of the random variable Y given below, explain if, why, and how, the information given about Y:

1. is sufficient/insufficient to compute the entropy of Y,
2. allows you to give a closed expression of the entropy of Y, or
3. only allows you to bound the entropy of Y from above and/or below.

(Possibly in terms of the entropy of X, Z, and W.)

4a (1T) Let $Y = (X_1, \ldots, X_n)$ be a random variable over $\{0,1\}^n$ such that $\Pr[X_i = 1] = 1/i$ for $i = 1, \ldots, n$.

4b (1T) Let Y be a random variable over $\{1, 2, \ldots, 7\}$ such that $\Pr[Y = y] = y^3/784$.

4c (1T) Let X, W, and Z be independent random variables over $[0, 2^{50} - 1]$ and define $Y = (X, XZ \bmod 2^{47}, Z, W)$.

4d (2T) Let $Y = (X_0, \ldots, X_n)$ be a random variable over $\{0,1\}^n$ such that $X_0 = 1$ and for every $(x_1, \ldots, x_{i-1}) \in \{0,1\}^{i-1}$ we have $\Pr[X_i = X_{i-1} | (X_1, \ldots, X_{i-1}) = (x_1, \ldots, x_{i-1})] = 1/i$ for $i = 1, \ldots, n$.

4e (2T) Let f be a function, let X be a random variable over a set $\mathcal{X}$, and define $Y = f(X)$. Only the probability function $p_X(x)$ of X is given, not the one for Y.

4f (2T) Let f be a function, let Y be a random variable over a set $\mathcal{Y}$, and define $X = f(Y)$. Only the probability function $p_X(x)$ of X is given, not the one for Y.

5 (5T) Motivate the definition of negligible functions. Let $f_0(x) = 0$ be the constant function and let $f_1 : \{0,1\}^n \to \{0,1\}$ be a randomly chosen function such that $2^{-n}\big|\{x \in \{0,1\}^n : f_1(x) = 1\}\big|$ is negligible in n. Then let $g_b(x_0, x_1) = \big(f_b(x_0), f_{1-b}(x_1)\big)$, where $b \in \{0,1\}$ is randomly chosen. Prove that $|\Pr[A^{g_0(\cdot,\cdot)} = 1] - \Pr[A^{g_1(\cdot,\cdot)} = 1]|$ is negligible in n for every polynomial time algorithm A.

6 (2T) The standard definition of an efficient algorithm in complexity theory is an algorithm with polynomial running time (if it is uniform or not does not matter in this problem). Why is this notion not satisfactory when constructing algorithms for optimization problems, but it is rarely unsatisfactory when modeling adversaries in cryptography?

7 (2T) Describe the structure of a proof by reduction in cryptography, i.e., describe the roles of definitions, assumptions, reductions, parties, adversaries, and conclusions. A fellow student that does not follow the course should be able to understand your description. You may show your description to somebody that does not follow the course to check this!

8 Let $E_t : \{0,1\}^n \times \{0,1\}^{tn} \leftarrow \{0,1\}^n$ be an n-bit block cipher with tn-bit keys, consisting of a t-round Feistel network. Let "$\|$" denote concatenation and let f_i be the ith Feistel function. Then denote the key by $k = k_1\|k_2\|..\|k_t$, the plaintext by $L_0\|R_0 \in \{0,1\}^n$, and the output in round $s \geq 1$ by $L_s\|R_s$, i.e., the output ciphertext is $L_t\|R_t$. Assume that $f_i(k_i, \cdot)$ is pseudo-random function for a random k_i.

8a (1T) Draw the Feistel network for $t = 1, 2, 3$.

8b (1T) Show that if $t = 1$, then the Feistel network is not a pseudorandom permutation.

8c (2T) Show that if $t = 2$, then the Feistel network is not a pseudorandom permutation.

8d (10T) Show that if $t = 3$, then the Feistel network is not a pseudorandom permutation. (Hint: Look at several related inputs and outputs. Evaluate the permutation as well as its inverse on these.)