KTH Computer Science
and Communication

Homework I, Foundations of Cryptography 2015

Before you start:

1. The deadlines in this course are strict. This homework set is due as specified at `https://www.kth.se/social/course/DD2448/subgroup/vt-2015-60028/page/deadlines-9`.
2. Read the detailed homework rules at `https://www.kth.se/social/files/54b92449f276547e23765898/solution_rules.pdf`.
3. Read about I and T-points, and how these translate into grades, in the course description at `https://www.kth.se/social/files/54baa2cbf276547f11c5e721/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 `https://www.kth.se/social/course/DD2448/subgroup/vt-2015-60028/page/handouts-8` 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 `Krypto15`.

We may publish hints on the homepage as well if a problem appears to be harder than expected.

1 Motivate the definition of negligible functions.

1a (5T) Prove that for every probabilistic polynomial time algorithm A, if R and R' are functions $\{0,1\}^n \to \{0,1\}$ such that for all inputs the outputs are chosen independently with output equal to one with probability $\epsilon(n)$, where $\epsilon(n)$ is negligible, then the functions are indistinguishable when available as oracles, i.e.,

$$|\Pr_R[A^{R(\cdot)}(1^n) = 1] - \Pr_{R'}[A^{R'(\cdot)}(1^n) = 1]|$$

is negligible, where 1^n denotes the unary encoding of n. Reconsider your solution when you are done and make sure that it is rigorous.

1b (1T) Explain the purpose of the unary representation of n and explain in your own words why the definition of negligible functions makes sense as a definition of "functions that are small enough to be ignored" in the context of efficient algorithms.

2 (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 simply be ”$1, 2$”.

$$f_1(n) = 1/\sqrt[0.9]{n} \quad f_2(n) = 2^{-(\log(n))^2} \quad f_3(n) = n^{-\pi} \quad f_4(n) = n^{-\frac{n}{n+1024}} \quad f_5(n) = 5^{-\sqrt{n}}$$

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.

3 (10I) Implement the AES cipher. A detailed description is found on Kattis `https://kth.kattis.com/problems/oldkattis%3Aaes`. 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.

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 entropies of X and S.)

4a (1T) Let $Y = (X_1, \ldots, X_n)$ be a random variable over $\{0,1\}^n$ such that $\Pr[X_i = 1] = 1/2$ for $i = 1, \ldots, n$.

4b (1T) Let S be a uniformly distributed random variable over $\{0,1\}^{64}$ and denote by Y the Hamming weight of S.

4c (1T) Let X and S be independent random variables over $[0, 2^{32} - 1]$ and define $Y = (X, S, XS \bmod 2^{31})$.

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 $\Pr[X_i = X_{i-1} | (X_1, \ldots, X_{i-1}) = (x_1, \ldots, x_{i-1})] = 1/4$ 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 (2T) Describe in detail what kinds of attacks you can mount on the Hill cipher. Is it a known-plaintext, chosen-plaintext, etc attack? How many ciphertexts do you need? What is the approximate time complexity of your attack?

6 (5T) Your friend is a high school teacher and you are asked to visit her class and talk about cryptography. As preparation for your visit, the students are given as homework to construct their own ciphers. You may assume that the students have no knowledge of cryptography and that none of them is a genius. Your job is to write a program that can break their ciphers. Please describe what assumptions you make and how your program works in plain English (not using pseudo-code). Your solution is graded based on completeness, clarity, and conciseness.

7 Search for information about uniform and non-uniform adversaries.

7a (1T) Describe the difference in your own words.

7b (2T) Does it matter which view we take on efficient adversaries? (both in theory and practice) Are they equivalent?

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 $t = 1, 2, 3$. (You can do this by hand and hand it in as a separate piece of paper.)

8b (2T) Show that if $t = 1$, then the Feistel network is not a pseudorandom permutation.

8c (4T) 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.)