KTH Computer Science and Communication

Homework I, Foundations of Cryptography 2016

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-2016-krypto16/page/deadlines-16`.
2. Read the detailed homework rules at `https://www.kth.se/social/files/5686fcd8f276542387729c18/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/5692df7bf2765405aca1825f/course_description.pdf`.
4. You may only submit solutions for a nominal value of 50 points in total (summing I and T points). The total number of points below may be larger and this should be interpreted as giving you a way to choose problems you like.

The problems are given in no particular order. If something seems wrong, then visit `https://www.kth.se/social/course/DD2448/subgroup/vt-2016-krypto16/page/handouts-10` to see if any errata was posted. If this does not help, then email `dog@kth.se`. Don't forget to prefix your email subject with `Krypto16`.

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

1 (12T) All students should have received an email with subject `Krypto16 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 $12T$ in total. 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 (up to one page).

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 tar-bombs please.) The simplest way to do this on a Linux/Unix machine at the school is, e.g., `tar cvfz wikstrom_douglas`.

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, but they are equally hard to solve.

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

2 (2T) Describe the structure of a proof by reduction in cryptography as explained in class, 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!

3 Motivate the definition of negligible functions.

3a (3T) 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 $\epsilon(n)$ and $\epsilon'(n)$ respectively, where $\epsilon(n)$ and $\epsilon'(n)$ are 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. Review your solution when you are done and make sure that it is rigorous.

3b (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.

4 (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".

$$f_1(n) = n^{-\log n} \quad f_2(n) = 2^{-256} \quad f_3(n) = (\sqrt{2})^{-n} \quad f_4(n) = n^{-128n} \quad f_5(n) = n^{-2} + 2^{-n}$$

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.

5 (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.

6 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.)

6a (1T) Let $Y = (X_1, \ldots, X_n)$ be a random variable over $\{0,1\}^n$ such that $\Pr[X_i = 1] = 2^{-i}$ for $i = 1, \ldots, n$.

6b (1T) Let S be a uniformly distributed random variable over $\{0,1\}^{128}$ and define $Y = \mathsf{AES}_k(S)$, where AES_k denotes the AES function for a fixed key k.

6c (1T) Let S be a uniformly distributed random variable over $\{0,1\}^{128}$ and define $Y = \mathcal{RO}(S)$, where $\mathcal{RO} : \{0,1\}^{256} \to \{0,1\}^{256}$ is a random oracle.

6d (1T) Let X and S be independent random variables over $\mathbb{Z}_q$, where q is an odd prime, and define $Y = (X, S, X^2 + S^3 + XS \bmod q)$.

6e (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 $i = 1, \ldots, n$.

6f (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.

6g (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.

7 Denote by X a random variable with probability function $\mathsf{P}_X : \mathbb{Z}_{12} \to [0,1]$ defined by the following table.

x	0	1	2	3	4	5	6	7	8	9	10	11
$\mathsf{P}_X(x)$	0.12	0.07	0.02	0.05	0.10	0.13	0.14	0.11	0.08	0.04	0.09	0.05

7a (2T) Compute the binary Hoffman code for P_X and derive how far it is from theoretical lower bound on any binary code for P_X.

7b (2T) Compute the ternary Hoffman code for P_X and derive how far it is from theoretical lower bound on any ternary code for P_X.

7c (1T) Is there a difference? If so, then explain informally why this is so.

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

8a (1T) Describe the difference in your own words.

8b (2T) Does it matter which view we take on efficient adversaries? (both in theory and practice) Are they equivalent?

9 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.

9a (2T) Show that if $t = 1$, then the Feistel network is not a pseudorandom permutation.

9b (4T) Show that if $t = 2$, then the Feistel network is not a pseudorandom permutation.

9c (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.)