Cryptography and Networked Systems Security

Prof. Dr.-Ing. Volker Roth
Freie Universität Berlin

Homework 2

Academic Integrity

Hereby I certify that I have neither received nor given help in answering the questions in this homework assignment.

_____

Date, signature, name in block letters

Question 1 (10 pts.)

When using the one-time pad (Vernam's cipher) with the key $k = 0^\ell$, it follows that $\mathrm{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^\ell$ (i.e., to have Gen choose k uniformly at random from the set of non-zero keys of length ℓ. Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this with the fact that encrypting with 0^ℓ doesn't change the plaintext.

Question 2 (10 pts.)

In this exercise, we study the conditions under which the shift, mono-alphabetic substitution, and Vigenére ciphers are perfectly secret:

1. Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.
2. What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)
3. Show how to use the Vigenére cipher to encrypt any word of length t so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

Reconcile this with the attacks that were shown in the previous chapter.

Question 3 (10 pts.)

Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

Question 4 (10 pts.)

Prove that we may assume that the key-generation algorithm Gen always chooses a key uniformly from the key space $\mathcal{K}$.

Note: the probabilities with which keys are chosen are obviously in $\mathbb{Q}$.

Hint: write a new Gen procedure which generates keys uniformly from the key space but "simulates" the old distribution.

Question 5 (10 pts.)

Let negl_1 and negl_2 be negligible functions. Prove that:

1. The function negl_3 defined by $\mathsf{negl}_3(n) = \mathsf{negl}_1(n) + \mathsf{negl}_2(n)$ is negligible.
2. For any (positive) polynomial p, the function negl_4 defined by $\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1(n)$ is negligible.
3. Prove that for all negligible functions negl with $\forall n \in \mathbb{N} : \mathsf{negl}(n) \geq 0$ it holds that $\lim_{n\to\infty}(\mathsf{negl}(n)) = 0$.
4. Prove or refute whether the following functions are negligible:
   (a) $n^{-\log n}$
   (b) n^{-c} for fixed $c \in \mathbb{N}$
   (c) c^{-n} for $c \in \mathbb{R}$
   (d) $f(n) = c$ for fixed $c \in \mathbb{R}$