DD2448 Foundations of cryptography

Homework II krypto18

Persnr	Name	Email
941212-T437	**Étienne Houzé**	**houze@kth.se**
123456-7890	Mohammad Al-Khwarizmi	mohammad@alkhwarizmi.hi
123456-7890	Ada Lovelace	ada@lovelace.hi

1 (2T) SOLVED

A proof by reduction is a means of proving that a cryptographic system is secrue. This proof is vastly inspired by the problem reduction often used in complexity theory. It conssists of finding a problem $\mathcal{P}$ which is proved to be hard to solve, and reduce the breaking of the cryptosystem to the resolution of $\mathcal{P}$. Reducing the cryptosystem to $\mathbb{P}$ means that solving the cryptosystem implies solving an instance of $\mathcal{P}$. Thus, if the cryptosystem is easy to solve, then $\mathcal{P}$ should also be easy to solve. Since we know that $\mathcal{P}$ is hard, then we have proved that the cryptosytem is at least as hard to solve.

2

2a (2T) SOLVED

The definition of a negligible fucntion is : "a function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ is negligible if and only if for every integer c there exists a rank n_c such that $\forall n > n_c, \epsilon(n) < \frac{1}{n^c}$ ". This implies that any negligble function tends to zero as n tends to infinity.

Moreover, let l be a polynomial function and let us call d its degree (d is finite). Let us prove that $l \times \epsilon$ is negligible.

Let c be an integer. Since ϵ is negligible, we know that there exists a rank n_0 such that for all $n > n_0$ we have $\epsilon(n) < n^{-c-d}$. Then we have for all $n > n_0$: $l(n) \times \epsilon(n) = Kn^{-c}$, where K is greater than the sum of all coefficients of l. Then there exists a rank n_1 such that, for all $n > n_1$ we finally have $l(n)\ times\epsilon n < n^{-c}$. So by definition, $l \times \epsilon$ is negligible.

2b (1T) NOT SOLVED

2c (2T) NOT SOLVED

3

3a (1T) NOT SOLVED

3b (1T) NOT SOLVED

3c (1T) NOT SOLVED

3d (1T) NOT SOLVED

3e (2T) NOT SOLVED

3f (2T) NOT SOLVED

4

4a (2T) NOT SOLVED

4b (1T) NOT SOLVED

4c (3T) NOT SOLVED

5

5a (7T) NOT SOLVED

5b (3T) NOT SOLVED

6

6a (4T) NOT SOLVED

6b (2T) NOT SOLVED

7 (4I) NOT SOLVED

8 (3I) NOT SOLVED

9 (4I) NOT SOLVED

10 (2I) NOT SOLVED