Cryptography, winter term 16/17: Assignment 10

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due January 25th, 2017

Exercise 10.1 (Be nice to your tutors and TAs, 1 Bonus Point)
Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 10.2 (Key-Exchange, 1 + 3 Points) Consider the following key-exchange protocol:

(1) Alice chooses $k, r \in \{0,1\}^n$ uniformly at random and sends $c := k \oplus r$ to Bob.

(2) Bob recieves c, chooses $s \in \{0,1\}^n$ uniformly at random and sends $d := c \oplus s$ to Alice.

(3) Alice recieves d and sends $e := r \oplus d$ to Bob.

(4) Finally, Alice outputs k and Bob outputs $e \oplus s$.

Now it is your task to analyse correctness and security of this protocol:

(a) Show that Alice and Bob output the same key.

(b) Decide whether the protocol is secure and prove your answer.

Exercise 10.3 (Public-Key Encryption, 3 + (2 + 3) Points) Let $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a public-key encryption scheme for single-bit messages.

(a) Assuming Π has no decryption error, show that there is an *unbounded* adversary $\mathcal{A}$[1] that, on input pk and $c \leftarrow \mathrm{Enc}_{\mathrm{pk}}(m)$ outputs m with probability 1.

(b) Assuming the length of every ciphertext obtained by Enc is bounded logarithmically[2] in the security parameter, show that Π is *not* CPA-secure. Proceed as follows:

(i) Prove that there exists a polynomial p such that for every $n \in \mathbb{N}$:

$$|\{x \in \{0,1\}^* \mid |x| \leq \log n\}| \leq p(n)$$

(ii) Consider the following ppt adversary $\mathcal{A}$:

[1] *Unbounded* means that $\mathcal{A}$ has no time constraints. In particular, the running time of $\mathcal{A}$ may be exponential or even worse.
[2] That is, the length of every ciphertext is $\leq \log n$.

(1) Given pk, $\mathcal{A}$ computes $c_0 = \mathrm{Enc}_{\mathrm{pk}}(0)$ and $c_1 = \mathrm{Enc}_{\mathrm{pk}}(1)$.

(2) Then $\mathcal{A}$ outputs $m_0 = 0$ and $m_1 = 1$.

(3) When $\mathcal{A}$ recieves c it checks whether $c = c_0$ or $c = c_1$. If this is the case, $\mathcal{A}$ outputs 0 or 1, respectively. Otherwise $\mathcal{A}$ outputs a random bit.

Use (i) to prove that $\mathcal{A}$ wins the PubK-experiment with probability non-negligible greater than $\frac{1}{2}$, that is, show that there is a polynomial q such that

$$\Pr[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{q(n)}\,.$$

Exercise 10.4 (Number theory, 4 Points + 4 Bonus Points)

(a) Recall the definition of the Euler totient function $\phi(N) := |\mathbb{Z}_N^*|$, i.e. the number of integers between 1 and N that are coprime to N. In this exercise, you will prove an explicit formula: If N has the prime decomposition $p_1^{e_1} \dots p_t^{e_t}$, then

$$\phi(N) = N \cdot \prod_{i=1}^{t} (1 - \frac{1}{p_i})\,.$$

You can do this as follows: First, prove the formula for ϕ on prime powers, i.e., if p is a prime and $k \geq 1$, show that $\phi(p^k) = p^k(1 - \frac{1}{p})$. Then, use the Chinese Remainder Theorem to argue about the value of $\phi(N)$ for arbitrary N (recall that you can decompose N into powers of distinct primes).

We state the exact version of the theorem you can use to solve this exercise:

Chinese Remainer Theorem. *Let $m_1, \dots, m_t$ be pairwise coprime (i.e., not necessarily prime) integers, and let $m = m_1 \cdots m_t$ be their product. Then, there is an isomorphism between the (multiplicative) groups*

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_t}^*\,.$$

In particular, they have the same number of elements.

(b) **Bonus:** Consider the elliptic curve

$$E \;:\; y^2 = x^3 + 3x + 3$$

over $\mathbb{Z}_{11}$. How many points does $E(\mathbb{Z}_{11})$ have? Also, compute $(0,5) + (7,2)$ and $(0,5) + (0,6)$ in the group defined by E.