Modern Cryptography	Dec 18, 2018
Homework 11	
Lecturer: Daniel Slamanig, TA: Karen Klein	*Due: 23.59 CET, Jan 9, 2019*

To get credit for this homework it must be submitted no later than Wednesday, January 9th via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 11" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW11.pdf.

1. Key Exchange

   - **[10.4 in book, 2nd edition]** Consider the following key-exchange protocol:
     - Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s := k \oplus r$ to Bob.
     - Bob chooses uniform $t \in \{0,1\}^n$, and sends $u := s \oplus t$ to Alice.
     - Alice computes $w := u \oplus r$ and sends w to Bob.
     - Alice outputs k and Bob outputs $w \oplus t$.

     Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

2. Textbook RSA encryption

   - Prove the correctness of the textbook RSA encryption algorithm as introduced in the lecture, i.e., show that for all $n \in \mathbb{N}$, $((d, N), (e, N)) \leftarrow \mathsf{KeyGen}(1^n)$ any $m \in \mathbb{Z}_N$ it holds that $(m^e)^d \equiv m \pmod{N}$.
   - Show that factoring an RSA integer $N = pq$ is equivalent to computing the order $\varphi(N)$ of the group $\mathbb{Z}_N^*$. Use this result to show that an efficient algotithm for factoring yields an efficient algorithm for solving RSA.

3. IND-CPA secure encryption in the ROM

   - **[11.19 in book, 2nd edition]** Say three users have RSA public keys $(3, N_1)$, $(3, N_2)$, and $(3, N_3)$ (i.e., they all use $e = 3$), with $N_1 < N_2 < N_3$. Consider the following method for sending the same message $m \in \{0,1\}^\ell$ to each of these parties: choose a uniform $r \leftarrow \mathbb{Z}_{N_1}^*$, and send to everyone the same ciphertext

     $$(c_1, c_2, c_3, c_4) := (r^3 \bmod N_1, r^3 \bmod N_2, r^3 \bmod N_3, H(r) \oplus m)$$

     where $H : \mathbb{Z}_{N_1}^* \to \{0,1\}^\ell$. Assume $\ell \gg n$.
     - Show that this is not IND-CPA-secure, and an adversary can recover m from the ciphertext even when H is modeled as a random oracle (Hint: Chinese remainder theorem).

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`

- Show a simple way to fix this and get a IND-CPA-secure method that transmits a ciphertext of length $3\ell + \mathcal{O}(n)$ (you do not need to provide a formal proof of IND-CPA security).
- Show a better approach that is still IND-CPA-secure but with a ciphertext of length $\ell + \mathcal{O}(n)$ (you do not need to provide a formal proof of IND-CPA security).