3. Assignment: Security of RSA

(Hand in solutions on Tuesday, December 4th during the lecture)

Exercise 3.1 (Polynomial-time reductions). (6 points)

If you recall from a previous lecture, we had found four problems related to the breaking of RSA. Given a public key $(N, e)$, these four problems were:

- $B_1$: factor $N$ as the product of two primes $p$ and $q$.
- $B_2$: compute $d$, the multiplicative inverse of $e$ modulo $\varphi(N)$.
- $B_3$: compute $\varphi(N)$.
- $B_4$: compute the plaintext $x$ for a given encrypted message $y = x^e$.

We had then proved that we had several polynomial-time reductions between those different problems. Namely:

$$B_4 \leq_P B_2 \equiv_P B_3 \leq_P B_1.$$ 

We also said that we had $B_1 \leq_P B_3$, but left the proof as an exercise. Well, here we are now!

(i) Given a “black-box” algorithm $A_{\varphi}(N, e)$ that computes $\varphi(N)$, give a polynomial-time algorithm which, given the public key $(N, e)$ of an instance of RSA, factors $N$.

*Hint:* Recall that $N$ is an RSA modulus, i.e. the product of two distinct prime numbers $p$ and $q$. Hence $\varphi(N)$ has a particular form which you may use to retrieve $p$ and $q$. 

---

**Cryptography**

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY
Exercise 3.2 (Multiplicativity attack). (6 points)

We consider an instance of RSA given by its modulus $N$, and its respectively public and secret exponents $e$ and $d$.

Let’s take two messages $x_1$ and $x_2$ in the message space $\mathbb{Z}_N$ and encrypt them as $y_1 = x_1^e \mod N$ and $y_2 = x_2^e \mod N$.

(i) What is the encryption $y_3$ of a third message $x_3$ satisfying $x_3 = x_1 \cdot x_2 \mod N$?

Now let’s suppose that we are the attacker and that we want to decrypt a particular message $y$ that Alice has sent to Bob. We know that there exists an $x$ such that $y = x^e \mod N$, but we don’t know this $x$.

1. (i) What is the decryption of the ciphertext $y' = y \cdot z^e \mod N$, for any $z \in \mathbb{Z}_N$?

2. (ii) Suppose we manage to find a particular $z$ so that $y' = y \cdot z^e \mod N$ is not “suspicious-looking”, in the sense that Bob (the owner of the secret key) accepts to decrypt it for us\(^1\). Explain the details of the attack then used to retrieve $x$.

2. (iii) The existence of such attacks comes from the multiplicative property of RSA encryption. Find a simple way to prevent these attacks (for example using hash functions).

---

\(^1\)This is what we call a chosen-ciphertext attack.