Spring 2018 **CS 513: # 6 RSA** Ghashami, Kleindessner

Due by March 2, 23:59 pm.

Exercise 1 (8 + 6 + 6 points)

Consider an RSA public key $(e, N) = (3, 391)$, where $N = p \cdot q = 17 \cdot 23$.

a) What is the corresponding secret key?

b) What is the encryption of the message $x = 41$?

c) Provide the decryption of the message $y = 7$.

Exercise 2 (30 points)

In the RSA scheme, Bob uses the public key (e, N) and the secret key (d, N), where $N = p \cdot q$ for primes $2 < p < q$ and $0 < e, d < (p-1)(q-1)$ such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$. Bob's public key is known to everyone. Assume that for Bob $e = 3$. Suppose that Eve also obtains his secret key. Show that Eve can compute p and q in time polynomial in the number of bits of N.

Exercise 3 (20 points)

For $n \in \mathbb{N}$, by p_n we denote the n-th prime number (e.g. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$). Use the prime number theorem to show that

$$p_n \in \Theta(n \cdot \ln n).$$

Hint: You might want to use that $\ln x \leq \sqrt{x}$ *for all* $x > 0$.

Exercise 4 (8 points)

The Miller-Rabin test uses the following claim:

Let $N \in \mathbb{N}$. If there exists $x \in \mathbb{Z}$ such that $x \not\equiv 1 \pmod{N}$ and $x \not\equiv -1 \pmod{N}$, but $x^2 \equiv 1 \pmod{N}$, then N is composite.

Prove this claim to be true.

Exercise 5 (1 + 2 + 8 + 8 + 3 points)

Let $N \in \mathbb{N}$. We want to prove that the following holds:

$$N \text{ is prime} \quad \Leftrightarrow \quad (N-1)! \equiv -1 \pmod{N} \tag{1}$$

a) Show that (1) is true for $N = 2$.

b) If N is prime, then we know that every number $1 \leq x < N$ has a multiplicative inverse modulo N. Which of these numbers are their own inverse?

c) By pairing up multiplicative inverses, show that if $N > 2$ is prime, the right-hand side of (1) is true.

d) Show that if N is composite, then the right-hand side of (1) is false.

e) Why can't we immediately base a primality test on (1)?