Math 314: Discrete Mathematics **Spring 2019**
by Benjamin Schroeter **04/10/2019**

Exercies Sheet 2

Write your name on every sheet that you hand in. Do not use a pencil or a red colored ink. Write down your solution by yourself and do not copy it.

Hand in your solution before **Friday April 22 – 8 am**. **Have fun!**

Exercies 1: Visit the website `https://courses.csail.mit.edu/6.042/spring18/mcs.pdf`. Look at the *SSL Server Certificate* of that page.

a) What is its date of expiration and the used algorithm?

b) How many bits long is the modulus n of the public key?

c) How many digits long is n in the decimal system?

d) Which number is the exponent e in the decimal system?

Remark: How to find the certificate and information depends on your browser. Take a look into the details of the certificate.

Exercies 2: (RSA with small numbers) Assume $p = 11$ and $q = 13$.

a) Find the modulus n. How many different public keys exits with this modulus in the range $0, 1, \ldots, \varphi(n) - 1$?

b) Decide which of the following exponents are valid $e_1 = 0$, $e_2 = 1$, $e_3 = 5$, $e_4 = 17$, $e_5 = 119$ and $e_6 = 123$. Justify your answer.

c) Find the private key d when the exponent e is 103. Include all necessary steps.

d) Decrypt the ciphertext $\hat{m}_1 = 2$ and $\hat{m}_2 = 139$.

e) Encypt the plaintext message $m_1 = 16$ and $m_2 = 17$ with the public key $(n = 943, e = 3)$.

Exercies 3: Assume someone forgot to take the modulus and sent $\widehat{m} = m^e$ instead. Explain how you can use this to get the plain-text message m.