Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2020-03-26
Due: 2020-04-02

# SADS 2020 Problem Sheet #6

**Problem 6.1:** *eavesdropping on rsa* ((1+2+2)+1 = 6 points)

Alice is sending Bob a secret RSA-encrypted message. Bob has published his public RSA key $(e = 15852553, n = 44331583)$. Eve managed to obtain a copy of the secret message. Eve recorded the following sequence of decimal numbers:

```
21556870,12228498,25056229,38800351,19503311,12228498,38800351,
24444405,35051831,24444405,30059578,38800351,5811028,12228498,
27948437,12228498,1365184,24444405,38800351,18162318,14922283,
27948437,23749280,12351750,42881586
```

a) Help Eve to decrypt the numbers. Explain the steps you are doing.

b) Assuming the decrypted numbers are character code points, what was Alice's message to Bob?

**Problem 6.2:** *proof of work* (2+2 = 4 points)

Cryptographic hash functions can be used for a proof of work, also known as a cryptographic puzzle. The challenge is to find a random value that appended to a given message causes the the hash value to have a certain format, e.g., N leading bits of 0.

a) Find a random sequence of 64 hexadecimal digits such that the SHA-256 checksum begins with 12 bits (three digits in hexadecimal notation) of 0s. (Since your result is a random solution, we expect it to be different from the results produced by other students.) We will test your solution using `openssl sha256`.

b) Provide a script (python, shell, haskell, . . . ) that searches for a solution of the puzzle. Make sure your script can be run by us and that it is understandable.