Secure and Dependable Systems Module: CO-566
Constructor University Date: 2024-04-08
Dr. Jürgen Schönwälder **Due: 2024-04-15**

Problem Sheet #8

Problem 8.1: *eavesdropping on rsa* (4+1 = 5 points)

Alice is sending Bob a secret RSA-encrypted message. Bob has published his public RSA key $k = (e, n) = (5163359, 7189579)$. Eve managed to obtain a copy of the secret message. Eve recorded the following sequence of decimal numbers:

```
1311615,3205173,475476,7177361,533234,475476,7177361,533234,
6660386,1438457,6389756,533234,6212161,3043363,1956017,6800648,
6800648,1492801,533234,1956017,533234,7177361,3043363,3092893,
6212161,3043363,6389756,2271115
```

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 8.2: *diffie hellman key exchange* (1+2 = 3 points)

Alice and Bob agree on using the prime number $p = 181$ and the primitive root $g = 24$. Alice randomly chooses the value $a = 112$.

a) Which value does Alice send to Bob?

b) After the key exchange, Alice has the key $k = 27$. Which value did Bob choose and which value did Bob send to Alice?

Problem 8.3: *proof of work* (1+1 = 2 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 hash value to have a certain format, e.g., N leading bits of 0.

a) Find a random sequence of 64 hexadecimal digits (different from the one on this sheet) such that the SHA-256 checksum begins with 12 bits or 1s (or the three digits 0xfff). (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`. More precisely, we will use:

   ```
   m=6c93de688a92a15244d482d239ea6014081e0ffd37da210ec6ddee8bc638c91d
   /bin/echo -n $m | openssl sha256 -r
   ```

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.