Lab Simon Razniewski

24. Cryptography and RSA

In the first two exercises, do not use calculators. In the others, the use of calculators is permitted (recommendation: Wolframalpha).

1. Diffie-Hellman Key Exchange

Perform a Diffie-Hellman key exchange with your neighbor (instructions are in the slides). Check whether you arrive at the same shared secret.

2. Decoding in RSA

Decode the three ciphertext symbols 5, 9 and 3 using the private RSA key (7,11). What are the corresponding plaintext symbols?

3. Matching RSA Keys

Which of the following private RSA keys matches the public RSA key (5,91)?

- (19,91)
- (24,91)
- (29,91)
- (19,81)
- (24,81)
- (29,81)

4. Generate Your Own RSA Key Pair

Use the procedure as described in the lecture to generate a RSA key pair, using primes in the range from 20 to 100. Test the correctness of your key pair by encoding and decoding a number. If your key pair is correct, after decoding an encoded number, you should arrive at the number you started from.

5. Message Signing With Private-Public Key Pairs

In this exercise we use the key pair generated above for checking the integrity of messages.

1. Choose two messages (short strings) and write them on the blackboard
2. If your birthday is on an **even** day (2, 4, 6, …), compute the Java hashcode (with the "string".hashCode() function) of the **first** string, sign it with your private key, and write the signature on the blackboard. Put a random number as signature for the **second** key on the blackboard.
   If your birthday is on an **odd** day (1, 3, 5, …), compute the Java hashcode (with the "string".hashCode() function) of the **second** string, sign it with your private key, and write the signature on the blackboard. Put a random number as signature for the **first** key on the blackboard.
3. Verify for the 3 classmates after you on the blackboard, which of the two strings is correctly signed by them. Does your assessment match that of others?