

Cryptology homework sheet 1

Due: 10 September 2015, 10:45

Please hand in your homework in groups of two or three. To submit your homework, place it on the table of the lecturer *before* the lecture.

Please write the names and student numbers on the homework sheet. Please indicate your home university and study direction.

You can use a calculator or some computer algebra system for these exercises, but make sure to document all intermediate computations.

1. Compute $\varphi(37800)$.
2. Execute the RSA key generation where $p = 239$, $q = 433$, and $e = 23441$.
3. RSA-encrypt the message 23 to a user with public key $(e, n) = (17, 11584115749)$. Document how you compute the exponentiation if you only have a pocket calculator.
4. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

$$x \equiv 0 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{8}$$

5. Security proofs in crypto are usually allowing the attacker access to a decryption oracle, i.e. an algorithm that returns the decryption of any valid ciphertext. In the schoolbook version of RSA presented in class, any ciphertext is valid. The attacker wins if he finds the plaintext m belonging to ciphertext c without ever asking the oracle for a decryption of c itself.

Show how the attacker can recover m from $c \equiv m^e \pmod{n}$ with *one* oracle query and some (easy) computation.

This exercise shows you that schoolbook RSA should not be used in practice. A much better way is to use https://en.wikipedia.org/wiki/Optimal_asymmetric_encryption_padding RSA-OAEP, which means that modified ciphertexts are likely invalid.