PUBLIC KEY CRYPTOGRAPHY - Computer Science

Lab 5 (Weeks 9-10)

All programs will be written in versions of C or Python with commented code.

Topic: public key cryptosystems.

- Each team of two students will be assigned one of the following ciphers during the labs:

  1. Knapsack cryptosystem.

  2. Paillier cryptosystem.

  3. Cramer–Shoup cryptosystem.

  4. McEliece cryptosystem.

  5. Goldwasser–Micali cryptosystem.

- Prepare a short documentation describing the cryptosystem and create a project with the following features:

  (i) Setting. The alphabet will have 27 characters: the blank and the 26 letters of the English alphabet.

  (ii) Generates a public key and a private key. The public key will be randomly generated in the required interval.

  (iii) Using the public key, encrypts a given plaintext. There will be a plaintext validation.

  (iv) Using the private key, decrypts a given ciphertext. There will be a ciphertext validation.

Points

- **1 point** for each member of the team if handed in by Week 13 (odd week groups) or Week 14 (even week groups).

Note: *Each student will keep her/his semigroup for the lab throughout the semester! Taking and presenting labs in weeks with a changed parity may only be done in exceptional cases, if the teaching assistant agrees with it and if time allows.*