Information Security (COSE354)

2019 2nd Project – Public Key Cryptography

Prof. Junbeom Hur
TA. Hyundo Yoon
Department of Computer Science and Engineering
Korea University

Problem 1 - RSA

- Decrypt the ciphertext C = 1220703125, which is encrypted using RSA with the following public parameters
  - n: 994323785284587765 1 (64 bits)
  - e: 13 (receiver's public key)

* You have to implement the extended Euclidean algorithm and square-and-multiply algorithm

Problem 1 - RSA

- Use following plaintext & ciphertext to check if you have solved correctly
  - Plaintext : 8835383948117812667
  - Ciphertext : 52856736590059552 9

  - Plaintext : 852845877651
  - Ciphertext : 879221550388509811 7

Problem 2 - ElGamal

- Decrypt the ciphertext c:($c1$= 2909170161,$c2$= 2565161545), which is encrypted using ElGamal with the following public parameters
  - q: 2934201397 (GF(2934201397)-32 bits)
  - a: 37 (primitive root of q)
  - YA: 2174919958 (receiver's public key)

* You have to implement the extended Euclidean algorithm and square-and-multiply algorithm

Problem 2 - ElGamal

- Use following plaintext & ciphertext to check if you have solved correctly
  - Plaintext : 189465461
  - Ciphertext : c1 = 2909170161, c2 = 1004005362

  - Plaintext : 848963461
  - Ciphertext : c1 = 2909170161, c2 = 2081016632

Term Project

- For the submission, please upload on Blackboard

    1. Upload your source programs and result screen(that is, plaintext result) into the Blackboard
    2. Plagiarism will be “F”
    3. No Late Submission (0 points, no exceptions)

- DUE DATE
  December 11th (Wed.), 23:59