

Information Security

Project 2

Public-Key Cryptography

Prof. Junbeom Hur

**Department of Computer Science and Engineering
Korea University**

Project 2

- You came to know two encrypted messages sent by terrorists
- You found they were encrypted by RSA and ElGamal encryption algorithms, respectively
- You must decrypt them to prevent any possible incidents as soon as possible with only the public information

Problem 1 – RSA

- Decrypt the ciphertext $C = 21$, which is encrypted using RSA with the following public parameters
 - n : 18444164967047483891 (64 bits)
 - e : 29 (receiver's public key)

* You have to implement the extended Euclidean algorithm

Problem 2 – ElGamal

- Decrypt the ciphertext c : ($c_1 = 187341129$, $c_2 = 881954783$), which is encrypted using ElGamal with the following public parameters
 - q : 1605333871 (GF(1605333871)-32 bits)
 - a : 43 (primitive root of q)
 - Y_A : 22 (receiver's public key)

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

Project 2

- Due date
 - 2017. Dec. 11, 23:59
 - Upload your source programs and result screen(that is, plaintext result) into the Blackboard
 - **Plagiarism will be “F”**
- If you have any question, send an email to T.A
 - Hyunsoo Kwon (khs910504@gmail.com)
 - Youngki Hong (gee308@naver.com)