Information Security

2018 Project 2

Prof. Junbeom Hur
TA. Changhee Hahn, Hyeong-seob Kim
Department of Computer Science and Engineering
Korea University

Problem 1

- Alice communicates with Bob
- She chooses the El-Gamal public parameter as
  - $(q, g) = (15383399235709406497,3)$
- She uses a secret key x_A where $1 \leq x_A \leq q - 1$
- She issues her public key as a follow:
  - $(q, g, h = g^{x_A})$ where $h = 12036625823877237123$
- Bob encrypts a message M under Alice's public key
  - $CT = (g^r, M * h^r) = (26955971572751 21,15118850555567 1261)$

Problem 1

- Later, Alice communicates with Charlie
- She chooses another El-Gamal public parameter as
  - $(q', g') = (223,3)$
- She reuses x_A to compute a new secret key $x'_A \equiv x_A \ (mod\ q')$
- She issues her new public key as a follow:
  - $\left(q', g', h' = {g'}^{x'_A}\right)$ where $h' = 118$

- Find M

Problem 2

- Suppose Alice has a secret key x_A
- She issues her public parameter as a follow:
  - $(q, g) = (153833992357094064 97,3)$
- She establishes a session key with Bob (who has a secret key x_B) using DHE as follows:
  - Alice and Bob agrees on the above (q, g)
  - Alice sends g^{x_A} to Bob, where $g^{x_A} = 325592838927301 7819$
  - Bob sends g^{x_B} to Alice, where $g^{x_B} = 116844921525386 08742$
  - They set a session key as $g^{x_A x_B}$
  - Then, they communicate using El-Gamal-like encryption

Problem 2 Cont'd

- You are given a list of six plaintext-ciphertext pairs as follows:
  - $(PT, < CT >) = (m, < g^r, m * g^{x_A x_B r} >)$
  - $(617, <5789380000885006824, 112919120438258672 99>)$
  - $(971, < 67237887994157077 68, 136841591713369768 88 >)$
  - $(593, < 102906542957330388 0, 699774373487079648 9 >)$
  - $(727, < 831289352548622152 5, 100930895313572324 28 >)$
  - $(941, < 908079942892990460 7, 710389074863998323 >)$
  - $(929, < 114411520058105542 93, 340307190580149730 9 >)$
- Note that, for each ciphertext, r is chosen randomly
- Note also that these ciphertexts are not decryptable since descriptions about how to recover r are missing

Problem 2 Cont'd

- After the session ends, Bob encrypts M_2 under Alice's public key a follow:
  - $CT = (g^r, M_2 * g^{x_A r}) =$ $(8312893525486221525, 78258681334322465 71)$

- Find M_2

Problem 3

- Bob encrypts another message M_3 under Alice's public key as a follow:
  - $CT = (g^r, M_3 * g^{x_A r})$
    $=(4232920939787140673,125943636072120863 62)$

- Find $M_2 * M_3$
  - M_2 is the answer to Problem 2

Submission Guideline

1. Source code (e.g., C or Java)
2. Report (e.g., .doc, .hwp, …)
   - Approach to the problems
   - Comment to your source code
     - Explain what functions, variables, etc., you use in your source code do
   - Screen capture of the running program
     - Explain what the captured images mean
   - Answer
     - List the values for each problem
3. Executable file
   - Project_2_1.exe, Project_2_2.exe, Project_2_3.exe, etc.

Grading Criteria

- 0 if at least one is not submitted
- +8 for each problem
- +6 for report
- 30 as the maximum score

Submission

- Due date
  - 21th of Dec. (Fri.) 23:59

- Upload into Blackboard

- **Late submission is not accepted**