Cryptography
ECE 5632
Sheet 7

Spring 2023

Problem 1

Consider El-Gamal public key encryption scheme, with public parameters $p = 23$ and $\alpha = 4$. Let the private key $d = 9$.

(a) Verify that α is indeed a generator of order 11, modulo 23.

(b) Compute the public key β.

(c) For a message $x = 15$ and a picked random integer $i = 8$, Compute the El-Gamal encryption of x.

(d) Repeat (c) for $i = 10$ and give a comment on the security of the system.

(e) Decrypt the El-Gamal observed ciphertext $y = (13, 10)$ (i.e., extract x).

Problem 2

Encrypt the following messages with the El-Gamal scheme ($p = 467, \alpha = 2$):

(a) $d = 105, i = 213, x = 33$

(b) $d = 105, i = 123, x = 33$

(c) $d = 300, i = 45, x = 248$

(d) $d = 300, i = 47, x = 248$

Now decrypt every ciphertext and show all steps.

Problem 3

Considering the four examples from Problem 2, we see that the El-Gamal scheme is nondeterministic: A given plaintext x has many valid ciphertexts.

(a) Why is the El-Gamal signature scheme nondeterministic?

(b) How many valid ciphertexts exist for each message x (general expression)?

(c) Is the RSA crypto system nondeterministic once the public key has been chosen?

Problem 4

Assume Bob sends an El-Gamal encrypted message to Alice. Wrongly, Bob uses the same parameter i for all messages. Moreover, we know that each of Bob's cleartexts start with the number $x_1 = 21$ (Bob's ID). We now obtain the following ciphertexts ($k_{E,1} = 6, y_1 = 17$), ($k_{E,2} = 6, y_2 = 25$). The El-Gamal parameters are $p = 31$, $\alpha = 3$, $\beta = 18$. Determine the second plaintext x_2.

Problem 5

Given an RSA signature scheme with the parameters $p = 101, q = 97, e = 131$. Verify the validity of the following: $(x, s) = (123, 6292)$

Problem 6

Given an RSA signature scheme with the parameters p$= 17, q = 23, e = 237$. What's the signature of the message $x = 321$?

Problem 7

Consider the ElGamal signature scheme. Given Bob's private key $d = 67$ and the corresponding public key $(p, \alpha, \beta) = (97, 23, 15)$.

(a) Calculate the ElGamal signature (r, s) and the corresponding verification for a message from Bob to Alice with the following messages x and ephemeral keys k_E:

(i) $x = 17$ and $k_E = 31$

(ii) $x = 17$ and $k_E = 49$

(b) You receive two alleged messages x_1, x_2 with their corresponding signatures (r_i, s_i) from Bob. Verify whether the messages $(x_1, r_1, s_1) = (22, 37, 33)$ and $(x_2, r_2, s_2) = (82, 13, 65)$ both originate from Bob.

(c) Compare the RSA signature scheme with the ElGamal signature scheme. Where are their relative advantages and drawbacks?