SECURITY

Assignment 13, Monday, December 22, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Exercise 1

A. n = p * q = 11 * 19 = 209
   $\phi(n)$ = (p-1)(q-1) = 10 * 18 = 180
B. To compute d we should use the extended euclidean algorithm with starting pair (180,7)

Pair	Remainder	Linear combination
(180, 7)	5 = 180 - 25 * 7	1 = 3 * 180 - 77 * 7 1 = 3 * (180 - 25 * 7) - 2 * 7
(7, 5)	2 = 7 - 1 * 5	1 = 3 * 5 - 2 * 7 1 = 1 * 5 - 2 * (7 - 1 * 5)
(5, 2)	1 = 5 - 2 * 2	1 = 1 * 5 - 2 * 2 1 = 2 * 0 + 1 * (5 - 2 * 2)
(2, 1)	0 = 2 - 2 * 1	1 = 2 * 0 + 1 * 1

   We see that the inverse of e = 7 is -77. In order to convert it to a value in the cyclic group we will add 180 to it which gives us 103 as inverse, so d = 103.
C. Alice's signature will be as follows:
   $S = m^d \bmod n$
   $S = 16^{103} \bmod 209 = 81$
D. In order to compute the signature using the public key we should compute the message m' from the signature and check that m = m'.
   m' = $s^e \bmod n$
   = $81^7 \bmod 209$
   = $81 * 81^6 \bmod 209$
   = $81 * (81^3)^2 \bmod 209$
   = $81 * (81)^2 * (81^2)^2 \bmod 209$
   = $81 * 82 * (82)^2 \bmod 209$
   = $81 * 82 * 36 \bmod 209$
   = $163 * 36 \bmod 209$
   = 16

Exercise 2

A. Alice's corresponding public key may be computed as follows:
   A = g^a mod p
   = 3^{21} mod 29
   = 17

B. So m = 15 and r =5
   a. #g = ϕ(p)
   = ϕ(29) = 28

   The prime factorization of 28 = 2 * 2 * 7 which shows that 5 isn't a common factor and gcd(28, 5) = 1. So they are relatively prime.
   b. S_1 = R = g^r mod p = 3^5 mod 29 = 11
   c. We can compute this using extended euclidean:

Pair	Remainder	Linear combination
(28, 5)	3 = 28 - 5 * 5	1= 2 * 28 - 11 * 5 1= 2 * (28 - 5 * 5) - 1 * 5
(5, 3)	2 = 5 - 1 * 3	1= 2 * 3 - 1 * 5 1= 1 * 3 - 1 * (5 - 1 * 3)
(3, 2)	1 = 3 - 1 * 2	1= 1 * 3 + 1 * - 2 1= 0 * 2 + 1 * (3 - 1 * 2)
(2, 1)	0 = 2 - 2* 1	1= 0 * 2 + 1 * 1

   Now we see that r^{-1} = -11. To transfer it to an element in the cyclic group we may add the value of p to it. So r^{-1} mod #g = -11 + 28 = 17
   d. S_2 = (h(m) - a * R) * r^{-1} mod #g
   = (15 - 21 * 11) * 17 mod 28
   = 8 * 17 mod 28
   = 24

C. Now we may verify that the signature is correct
   a. S_1 = 11 and 1 ≤ 11 ≤ 29, so 1 ≤ s_1 ≤ p holds.
   b. v := s_1^{s2} * A^{s1} mod p
   = 11^{24} * 17^{11} mod 29
   = 7 * 12 mod 29
   = 7 * 12 mod 29
   = 26
   c. First, we should compute $g^{h(m)}$
   $g^{h(m)}$ = 3^{15} mod 29
   = 26

   From b we see that v = 26 which shows that $g^{h(m)}$ = v holds.

Exercise 3

A. According to the scheme, Alice chooses an r randomly from {1,...,q-1}. She then computes h := g^r. Say that the randomness was known, the attacker would then be able to find the private key of Alice. According to the scheme: Alice publishes h, along with the description of G, q, g, as her public key. Alice then keeps r as her private key, which must be kept secret. Knowing the randomness would lead to a compromised r.
   Since the attacker now knows r, he can now also compute h := g^r and sign messages as Alice.
B. Almost the same as the previous assignment holds here. Since the attacker knows r, we can use that to compute the signature. Since s1 is known, we can then use r to compute g^r. When we have that number n^r we can then calculate the computed number mod n. After that we follow the steps to hash m with H(m) -a * g^r / r to find the signature (s1,s2). The attacker can then use this to his advantage to impersonate Alice.
C. Since El Gamal is used for encryption and DSA for signing messages with a private key we think that first scenario where the discovered randomness of El Gamal has far more devastating consequences. A message can be signed with DSA, but has to be encrypted anyway to have any importance. The goal of El Gamal however is to encrypt so discovering the randomness would then lead to discovering the decrypted message. This shows that is is very important to keep the randomness very high and private.