SECURITY

Assignment 12, Monday, December 15, 2017
S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Exercise 1

A. Since we know the Alice's private key we may compute the private key as follows:
K_{AB} = B^a where B is Bob's public key which is g^b
This means that K_{AB} can be computed as follows:
K_{AB} = $(g^b)^a$ mod p
= $(491)^{317}$ mod 1021
= 1,18 × 10^{853} mod 1021
= 71

B. Bob's secret key may be derived using the value of g^b. We know that g = 10 and that g^b = 491, so we should find the value for b for which 10^b mod 1021 = 491. The mod 1021 we can derive from the p that have been sent. Using Wolfram Alpha we find that b = 12.

C. In Bob's case the shared will equal A^b. Using b = 12 from the computation in the previous exercise we came to the following computation:
K_{AB} = A^b mod p
= $(g^a)^b$ mod p
= 93^{12} mod 1021
= 71
Wee see that this indeed equals the computed shared key from Alice.

D. i). The messages are as follows:
A → E(B): p = 1021, g = 10, g^a = 93
E(A) → B: p = 1021, g = 10, g^{404} = ...
B → E(A): g^b = 491
E(B) → A: g^{37}
ii). First, we will compute the key between Alice and Eve:
K_{AE} = $(g^{rB})^a$ mod p
= $(10^{404})^{317}$ mod 1021
= $(1 * 10^{404})^{317}$ mod 1021
= 622

We may compute the shared key between Eve and Bob using Bob's computed private key.

K_{BE} $= (g^{rA})^b \bmod p$
$= (10^{37})^{12} \bmod 1021$
$= (1 * 10^{37})^{12} \bmod 1021$
$= 73$

Exercise 2

A. A $= g^a \bmod p$
$= 3^{17} \bmod 31$
$= 129.140.163 \bmod 31$
$= 22$

B.

Encryption	**r**	**e**	**m**	**e**	**m**	**b**	**e**	**r**
Mapping m	18	5	13	5	13	2	5	18
r	3	6	9	12	15	18	21	24
A^r	15	8	27	2	30	16	23	4
$c_1 = g^r$	27	16	29	8	30	4	15	2
$c_2 = m * A^r$	270	40	351	10	390	32	115	72

C. The decryption table of the encrypted message in B is as follows:

Decryption of ciphertext (c_1, c_2)								
$(A^r)^{-1} = c_1^{-a}$	29	4	23	16	30	2	27	8
$m = c_2 * A^{-r}$	18	5	13	5	13	2	5	18

Exercise 3

The first number 5955819876511066883652848427785158583996665478598703733005 67
can be factored by the following two integers since the first factor is a common factor with the last number:

- 521192137187180935658403029827
- 114273018558069570996461461 4621

The second number has no GCD higher than 1 with any of the other numbers.

The third number 697998237255232517803133139640937207091669333334886072165381 can be factored in the following two numbers:

- 701397335649456892851007539749
- 995153819067366445814664502369

The fourth number has no GCD higher than 1 with any of the other numbers.

The fifth number 176294427788887166758409622538881387638478405478915857712513 can be factored in the following numbers:

- 701397335649456892851007539749
- 251347444349282901859447208237

The last number 592339248856319601455928821705423109007342115448431777433343 can be factored in the following numbers:

- 521192137187180935658403029827
- 113650841329478248301310121870 9

Common factors

1. GCD with all is 1 except for the last one it's: 521192137187180935658403029827
2. All GCD are 1
3. GCD with 5th: 701397335649456892851007539749 and all others are 1
4. All gcd are 1
5. All gcd are 1 except with third
6. All gcd are 1 except with the first