Assignment 4 – Cryptography II

Information & Communication Security
(WS 2018/19)

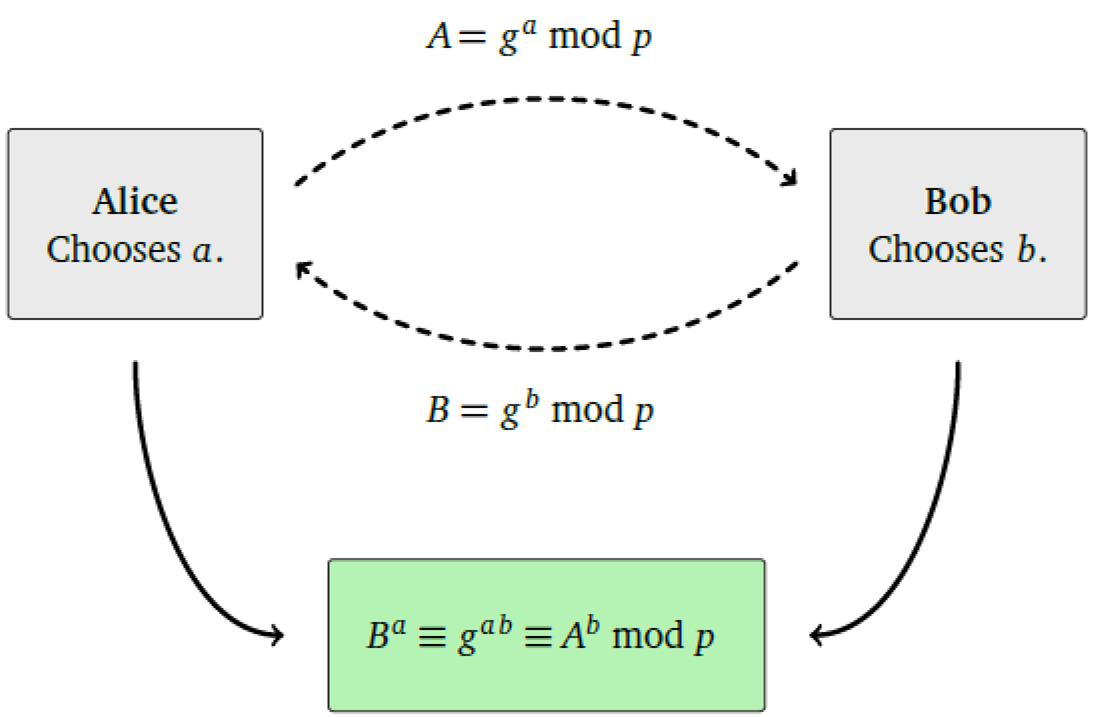
Abtin Shahkarami(M.Sc.)

Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

Exercise 1

Describe Diffie-Hellman key exchange method in detail.

Exercise 1 - Solution



Diffie-Hellman Key Exchange

Exercise 1 – Solution (Cont.)

a) Alice and Bob agree publicly on a cyclic group, e.g. $G = \langle g \rangle$, $G = \mathbb{F}^*$.

b) Alice chooses randomly some $0 \leq a < |G|$ and computes $A := g^a$. Bob chooses randomly some $0 \leq b < |G|$ and computes $B := g^b$.

c) Alice sends Bob A. Bob sends Alice B.

d) Alice computes $S := B^a = (g^b)^a = g^{ab}$. Bob computes $S := A^a = (g^a)^b = g^{ab}$.

e) Now Alice and Bob can use S as their secret key to encrypt and decrypt messages.

Exercise 1 – Solution (Cont.)

Outside of this process Eve only knows $G = \langle g \rangle$, A and B, but she does not know a, b, S. Thus Eve either needs to compute $a = \log_g A$ and $b = \log_g B$ (this is known as *discrete logarithm problem* and is assumed to be "hard"); or she has some other magical function f such that $S = f(A, B, G)$. Clearly, security of this system highly relies on the choice of the group, i.e. g. For example, taking $G = (\mathbb{Z}/n\mathbb{Z}, +) = \langle 1 \rangle$, thus exponentiation g^a boils down to $g \cdot a = a$ in this setting.

Exercise 2

In order to prepare to receive encrypted messages with the RSA cryptosystem, Alice has chosen primes $p = 23$ and $q = 37$. She has also chosen $e = 13$ as her public key (also called her public exponent).

a) Determine Alice's public modulus n.

Links to read & watch

- https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/intro-to-rsa-encryption
- http://mathworld.wolfram.com/RSAEncryption.html
- https://simple.wikipedia.org/wiki/RSA_algorithm

Exercise 2 – Solution (a)

Alice's public modulus is $n = p \cdot q = 23 \cdot 37 = 851$.

b) Suppose that Bob wants to send Alice the message BAT. Determine the base twenty-six representation of the ciphertext that he will send to Alice.

Exercise 2 – Solution (b)

Converting the message BAT to base twenty-six gives BAT = $1 \cdot 26^2 + 0 \cdot 26 + 19 = 695$.

Therefore, since the RSA encryption function is c = m^e MODn, Bob's ciphertext is given by c= 695^{13} MOD851. In order to compute the modular exponential, we repeatedly square:

$$695^2 \equiv 508 \pmod{851}$$
$$695^4 \equiv 508^2 \equiv 211 \pmod{851}$$
$$695^8 \equiv 211^2 \equiv 269 \pmod{851}.$$

We then conclude that

$$695^{13} \equiv 695^8 . 695^4 . 695 \equiv 269 . 211 . 695 \equiv 593 . 695 \equiv 251 \pmod{851}.$$

Thus, the ciphertext is c = 251 which converted to base twenty-six reads

$$251 = 9 \cdot 26 + 17 = \text{JR}.$$

c) Determine Alice’s private key (or decryption key) d.

Exercise 2 – Solution (c)

Alice's decryption key is given by d = e^{-1}MODφ(n) where $\varphi(n) = (p - 1) \cdot (q - 1)$. We find $\varphi(n) = 22 \cdot 36 = 792$, so that d = 13^{-1} MOD792. In order to calculate this modular inverse, we use the extended Euclidean algorithm
so that:

$$792 = 60 \cdot 13 + 12$$
$$13 = 12 + 1.$$

Back substitution therefore gives:

$$-792 + 61 \cdot 13 = 1$$

from which we conclude that

$$d = 13^{-1} \text{ MOD} 792 = 61.$$

d) Suppose that Bob has also sent Alice the ciphertext $y = 625$. Determine the base twenty-six representation of the plaintext message.

Exercise 2 – Solution (d)

The RSA decryption function for Alice is given by m = c^d MODn so that Bob's plaintext message is m = 625^{61} MOD851. In order to compute the modular exponential, we repeatedly square:

$625^2 \equiv 16 \pmod{851}$

$625^4 \equiv 16^2 \equiv 256 \pmod{851}$

$625^8 \equiv 256^2 \equiv 9 \pmod{851}$

$625^{16} \equiv 9^2 \equiv 81 \pmod{851}$

$625^{32} \equiv 81^2 \equiv 604 \pmod{851}$.

We then conclude that

$$625^{61} \equiv 625^{32} \cdot 625^{16} \cdot 625^{8} \cdot 625^{4} \cdot 625 \equiv 604 \cdot 81 \cdot 9 \cdot 256 \cdot 625$$
$$\equiv 784 \pmod{851}.$$

Thus, the plaintext is x = 784 which converted to base twenty-six reads

$$784 = 1 \cdot 26^2 + 4 \cdot 26 + 4 = \text{BEE}.$$

Exercise 3

Install PGP Email Desktop (trial version) or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to abtin.shahkarami@m-chair.de containing your newly created public key and a short summary of your experiences.

PGP can be downloaded from http://www.symantec.com/business/desktop-email.

Looking forward to your Emails ☺

Thank you!

- Questions: security@m-chair.de