JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.de

Prof. Dr. Kai Rannenberg
Abtin Shahkarami, MSc.

Telefon +49 (0)69-798 34706
Telefax +49 (0)69-798 35004
E-Mail security@m-chair.de

Information and Communications Security
WS 18/19
Assignment 4
Cryptography II

Study the following questions and prepare your answers before the **5th of December 2018.**

Exercise 1:

Describe Diffie-Hellman key exchange method in detail.

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 m.
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.
c) Determine Alice's private key (or decryption key) d.
d) Suppose that Bob has also sent Alice the ciphertext y = 625. Determine the base twenty-six representation of the plaintext message.

Exercise 3: (PGP)
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.