

Mobile Business 2 SS 2017 Homework 2 Cryptography

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
Ahmed Seid Yesuf, MSc.
Iulia Bastys, MSc.

Telefon +49 (0)69-798 34701
Telefax +49 (0)69-798 35004
E-Mail mob2@m-chair.de

Exercise 1:

Decrypt the following word, encrypted with the Caesar cipher:
JYFWAVNYHWOF

Exercise 2:

Imagine the following situation: Alice wants to share a secret with Bob and therefore sends an encrypted message to Bob.

- a) Sketch the process by using symmetric encryption/decryption.
 - i. Complete the illustration by highlighting each step and adding all the missing elements – such as keys, involved 3rd parties,...



- ii. What are the pre-conditions for this approach?
- iii. What are the advantages and disadvantages of symmetric encryption/decryption?

- b) Sketch the process by using asymmetric encryption/decryption.
- i. Complete the illustration by highlighting each step and adding all the missing elements – such as keys, involved 3rd parties,...



- ii. What are the pre-conditions for this approach?
- iii. What are the advantages and disadvantages of asymmetric encryption/decryption?

- c) Sketch the process by using PGP.
- i. Complete the illustration by highlighting each step and adding all the missing elements – such as keys, involved 3rd parties,...



- ii. What are the pre-conditions for this approach?
- iii. What are the advantages and disadvantages of PGP?

Exercise 3:

Describe the possible ways for distributing keys and discuss their pros and cons.