

Mobile Business 2

SS 2011

Exercise Sheet 1

Cryptography

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
Dipl.-Inf. Gökhan Bal
Dipl.-Wirt.-Inf. Markus Tschersich

Telefon +49 (0)69-798 34701
Telefax +49 (0)69-798 35004
E-Mail kai.rannenberg@m-chair.net

Exercise 1: Caesar-Cipher

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

Exercise 2: Cryptosystems

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 missing elements – such as keys, involved 3rd parties,...



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

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



- What are pre-conditions for this approach?
 - What are advantages and disadvantages of asymmetric encryption/decryption?
- c) Sketch the process by using PGP.
- Complete the illustration by highlighting each step and adding all missing elements – such as keys, involved 3rd parties,...



- What are pre-conditions for this approach?
- What are advantages and disadvantages of PGP?

2. Mention possible ways for distributing keys and discuss advantages as well as disadvantages.