JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

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

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
Shuzhe Yang, M.Sc.
David Harborth, M.Sc.

Telefon +49 (0)69-798 34701
Telefax +49 (0)69-798 35004
E-Mail mb2@m-chair.de

Mobile Business 2
SS 2016
Homework 1
Cryptography

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.

Exercise 4:
Download the following three research articles about the "Privacy Paradox" and the use behavior regarding passwords (accessible via UB Uni-Frankfurt Portal):

1. Florencio, D. & Herley, C., 2007. A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web - WWW '07*, p.657. Available at: http://portal.acm.org/citation.cfm?doid=1242572.1242661.

2. Florêncio, D., Herley, C. & Coskun, B., 2007. Do strong web passwords accomplish anything? *Proceedings of the 2nd USENIX workshop on Hot topics in security (HOTSEC'07)*, p.10. Available at: http://portal.acm.org/citation.cfm?id=1361419.1361429.

3. Norberg, P.A., Horne, D.R. & Horne, D.A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), pp.100–126.

Read the articles thoroughly and answer the following questions for each of the research contributions:

1. What is the research problem?
2. Why is this paper relevant? How does it contribute to science?
3. What is the methodology used and what are the results?
4. Can you identify weaknesses in any part of the research?