

Information and Communications Security

SS 08

Assignment 3

Cryptography

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
Dipl. Kfm. André Deuker
Dipl. Inf. Jan Zibuschka

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306
E-Mail kai.rannenberg@m-lehrstuhl.de

2008-04-30

Exercise 1: (PGP)

Install GNUPG or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to sec@m-chair.net containing your newly created public key and a short summary of your experiences.

GNUPG can be downloaded from <http://www.gnupg.de/>

Exercise 2: (Hash functions and signature systems)

Scenario: A cryptographer has published an algorithm that allows him to find pairs of values v_1, v_2 such that $h(v_1)=h(v_2)$, for a hash function h .

- Which security properties of the function has he broken, which are not directly affected?
- Describe an attack on a signature system using h resulting from the attack on the hash function (h).

Exercise 3: (Caesar)

Decrypt the following word, encrypted with the Caesar cipher:

UGEWTKVA

Exercise 4: (Misc)

- Describe differences between symmetric and asymmetric cryptosystems.
- Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.
- Describe different approaches towards the certification of keys.