

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

# 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.-Wirt.Inf. Christian Kahl**  
**Dipl. Medien-Inf. Katja Liesebach**

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

8. Mai 2008

## 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 Katja Liesebach ([katja.liesebach@m-chair.net](mailto:katja.liesebach@m-chair.net)) and Christian Kahl ([christian.kahl@m-chair.net](mailto:christian.kahl@m-chair.net)) containing your newly created **public** key and a short summary of your experiences (in German or English – as you please).

### Hints:

- GNUPG can be downloaded from <http://www.gnupg.de/>
- A key ring containing the staff's public keys can be found on the website <http://m-chair.net/>

## Exercise 2: Caesar-Cipher

Decrypt the following word, encrypted with the Caesar cipher:

JYFWAVNYHWOF

---

---

---

---

---

---

---

---

---

---







