

# Information and Communications Security WS 08 Assignment 3 Cryptography

18. November 2008

**Exercise 1:** RSA-Example:  $p=3$ ,  $q=11$ ,  $e=3$

- Compute  $n$
- Compute  $d$
- Encrypt the Message „SECURITY IS COOL“  
with A(00), B(01) ... Z(25), Blank (26)
- Show, that decrypting the Cipher results in the original Message again.

**Exercise 2:** (Caesar)

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

**Exercise 3:** (Misc)

- Describe differences between symmetric and asymmetric cryptosystems.
- Why is there a need for hybrid crypto systems?
- What is the basic assumption making RSA to a valid crypto system and what are the basic vulnerabilities?