

*Assignment 3:*

Cryptography

Information &  
Communications Security  
(WS 2008)

Guest Lecturer Dr. Martin Reichenbach

T-Mobile Chair for  
Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.  
[www.whatismobile.de](http://www.whatismobile.de)



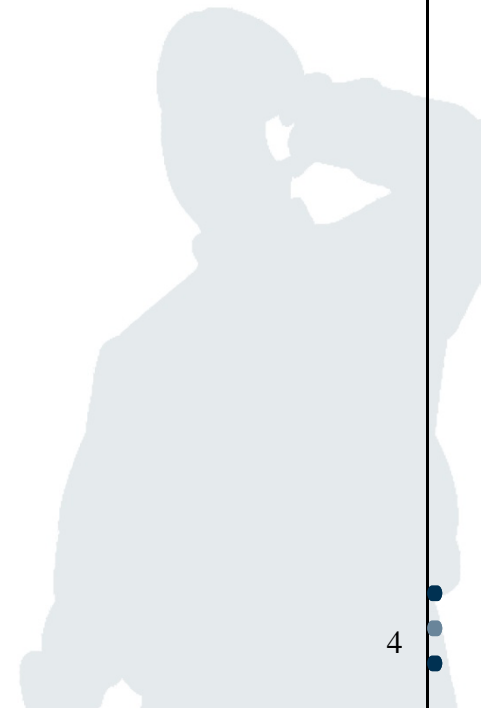
- a)  $n = p \cdot q = 3 \cdot 11 = 33$
- b)  $e \cdot d \bmod (p-1) \cdot (q-1) =$   
 $3 \cdot d \bmod (3-1) \cdot (11-1) =$   
 $3 \cdot d \bmod 20 =$   
 $21 \bmod 20 = 1$   
 $\Rightarrow d = 7$
- c) Example  $M = "E" = "04"$   
Verschlüsselung des Message-Blockes "04"  
 $(4^{**}3) \bmod 33 = 64 \bmod 33 = 31$
- d) Entschlüsselung des Cipher-Blockes "31"  
 $(31^{**}7) \bmod 33 = 27 512 614 111 \bmod 33 = 4$

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

UGEWTKVA

- Caesar: transposition, Caesar used A->C
- A->C works here
- Or try out A->B, A->C (only 26 possible keys [of which A->A doesn't make sense, but is valid])
- You may also use letter frequency tables, but not in this case (each letter appears 1 time only)

- UGEWTKVA (A->A)
  - A->B: TFDVSJUZ
  - A->C: SECURITY
  - A->D...
  
- „Security“ sounds good



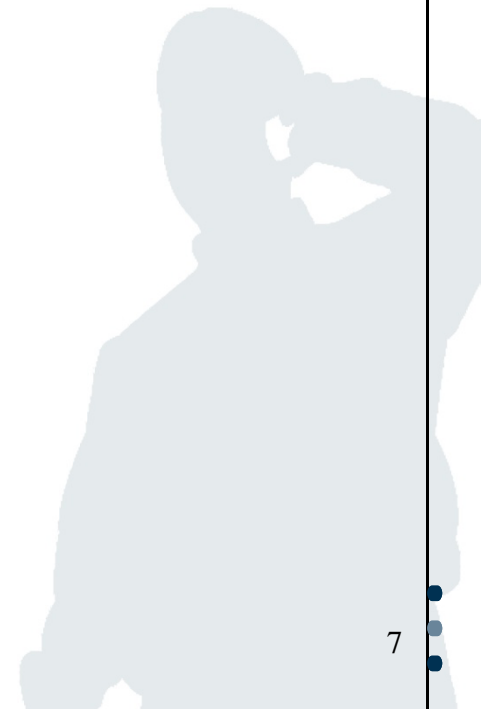
- a) Describe differences between symmetric and asymmetric cryptosystems.
- b) Why is there a need for hybrid crypto systems?
- c) What is the basic assumption making RSA to a valid crypto system and what are the basic vulnerabilities?

a) Describe differences between symmetric and asymmetric cryptosystems.

- Asymmetric cryptosystems
  - Two keys: public and private
  - Key management by publication/certification of public keys
  - Relatively slow performance
- Symmetric cryptosystems
  - One key: has to be kept secret from outsiders
  - Key management: sharing of keys via secure channels
  - Fast performance (-> For encryption of e.g. large files -> hybrid systems)

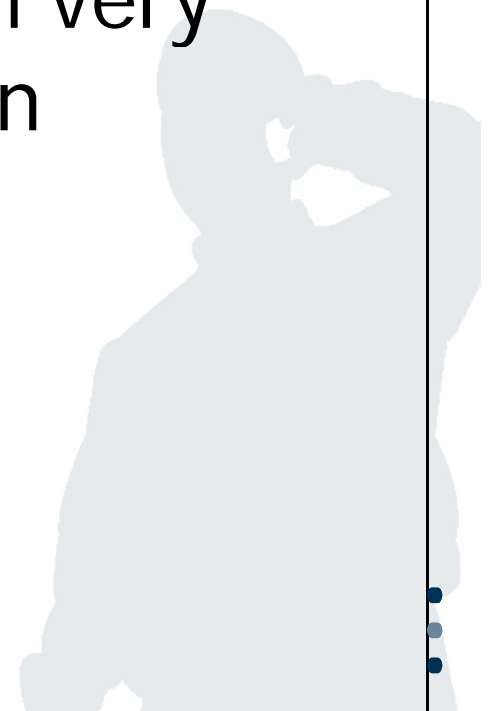
b) Why is there a need for hybrid crypto systems?

- Combine advantages of symmetric and asymmetric crypto
- Performance, efficiency
- Good key management



- What is the basic assumption making RSA to a valid crypto system and what are the basic vulnerabilities?
  - Factorisation Problem
  - Impossible to deduct the private key from the publicly known one.
  - a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key
  - a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with.

- factoring of the public key.
- If this can be achieved, all messages written with the public key can be decrypted. The point is that with very large numbers, factoring takes an unreasonable amount of time



- A popular choice for the public exponents is  $e = 216 + 1 = 65537$ .
- Some applications choose smaller values such as  $e = 3, 5, 17$  or  $257$  instead. This is done to make encryption and signature verification faster on small devices like smart cards but small public exponents can lead to greater security risks