

Lecture 5

Cryptography



Mobile Business II (SS 2010)

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe-Universität Frankfurt a. M.



- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography

- Intention
 - Confidentiality (secrecy of messages):
encryption systems
 - Integrity (protection from undetected manipulation) and accountability:
authentication systems and **digital signature systems**
- Key distribution
 - **Symmetric:**
Both partners have the same key.
 - **Asymmetric:**
Different (but related) keys for encryption and decryption
- In practice mostly hybrid systems

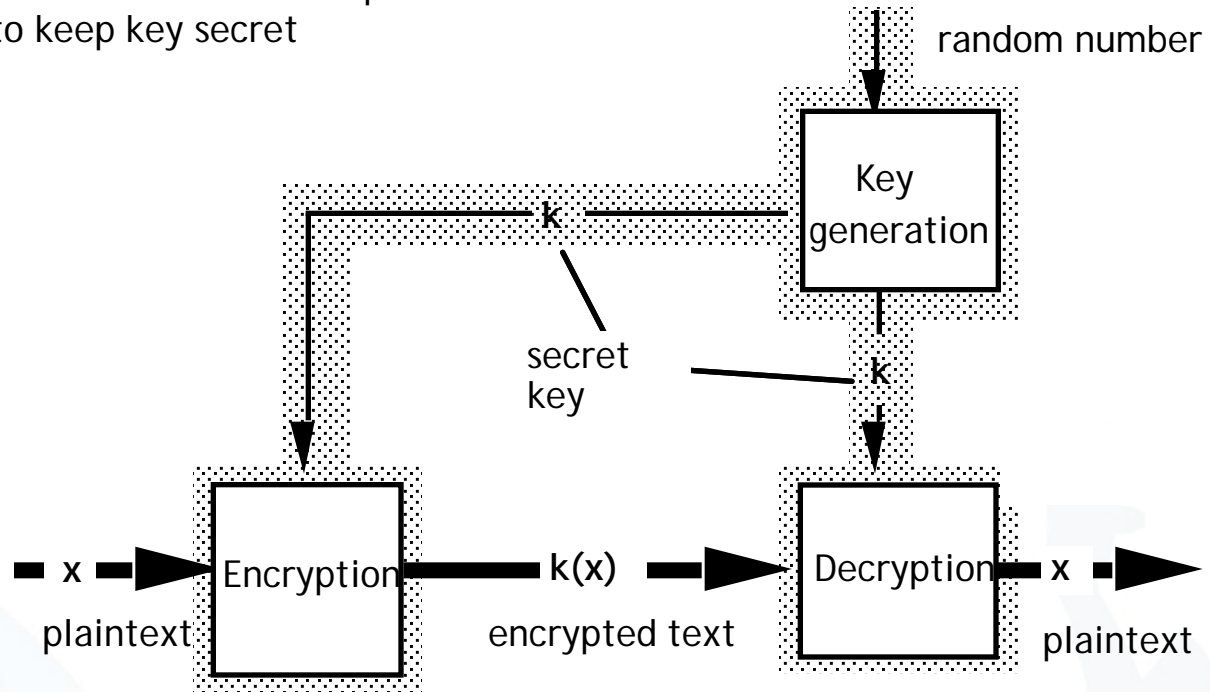
- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography

- Typical applications
 - confidential storage of user data
 - transfer of data between 2 users who negotiate a key via a secure channel
 - end-to-end channel decryption
- Examples
 - Vernam-Code (one-time pad, Gilbert Vernam)
 - key length = length of the plaintext (information theoretically secure)
 - DES: Data Encryption Standard
 - key length 56 bit, so 2^{56} different keys
 - AES: Advanced Encryption Standard (Rijndael, [NIST])
 - three possible key lengths: 128, 192 and 256 bit

- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography

Symmetric Encryption Systems

Area that needs to be protected to keep key secret

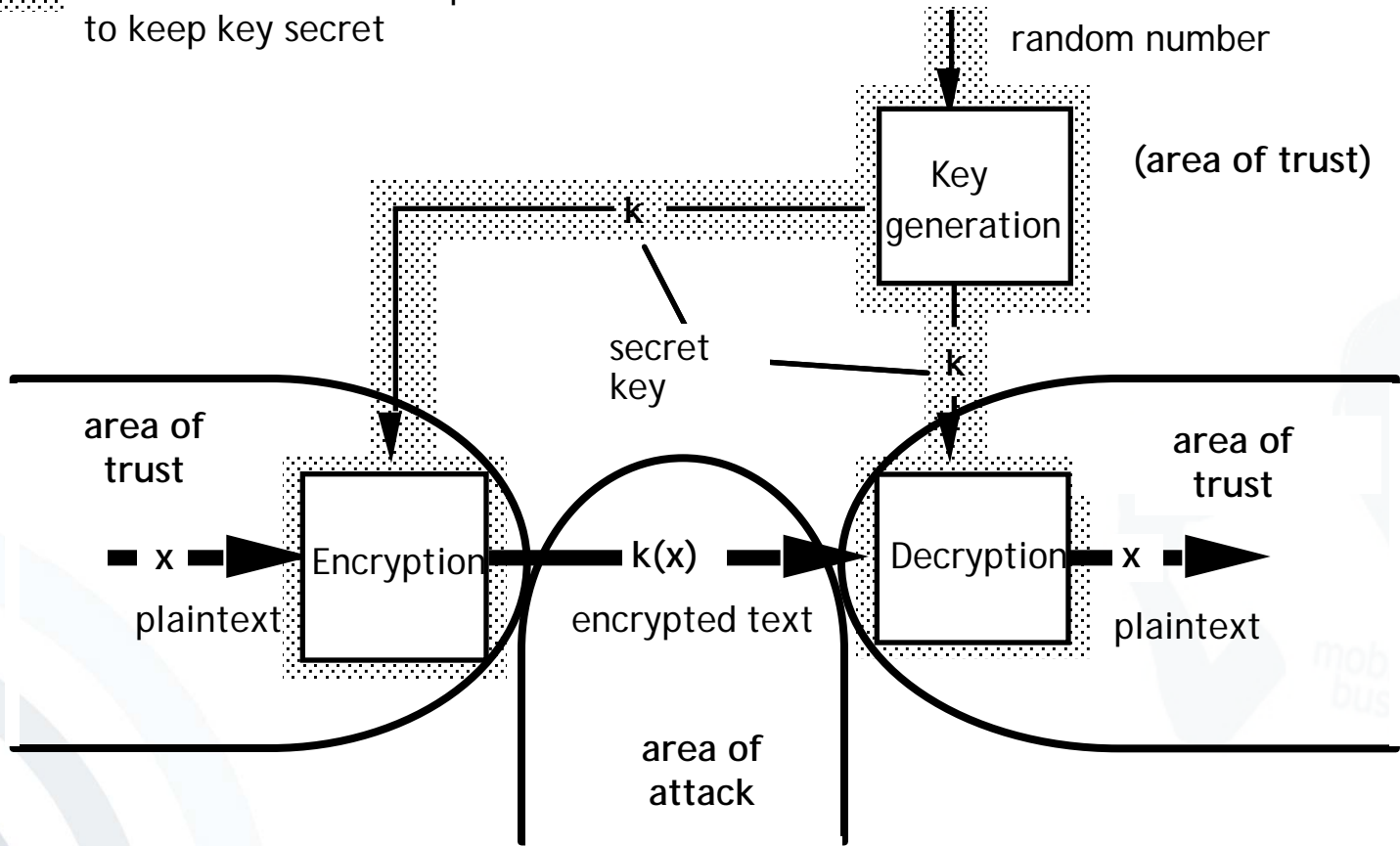


black box with lock, two equal keys

[based on Federrath and Pfitzmann 1997]

Symmetric Encryption Systems

Area that needs to be protected to keep key secret



[based on Federrath and Pfitzmann 1997]

- Keys have to be kept secret
→ *secret key crypto system*
- It must not be possible to infer on the plaintext or the keys used from the encrypted text (ideally encrypted text is not distinguishable from a numerical random sequence).
- Keys should be uniformly distributed.
- In principle each system with limited key length is breakable by testing all possible keys.
- Publication of encoding and decoding functions (algorithms) is considered as good style and is trust-building. Security of cryptosystems should base on the strength of chosen key lengths.

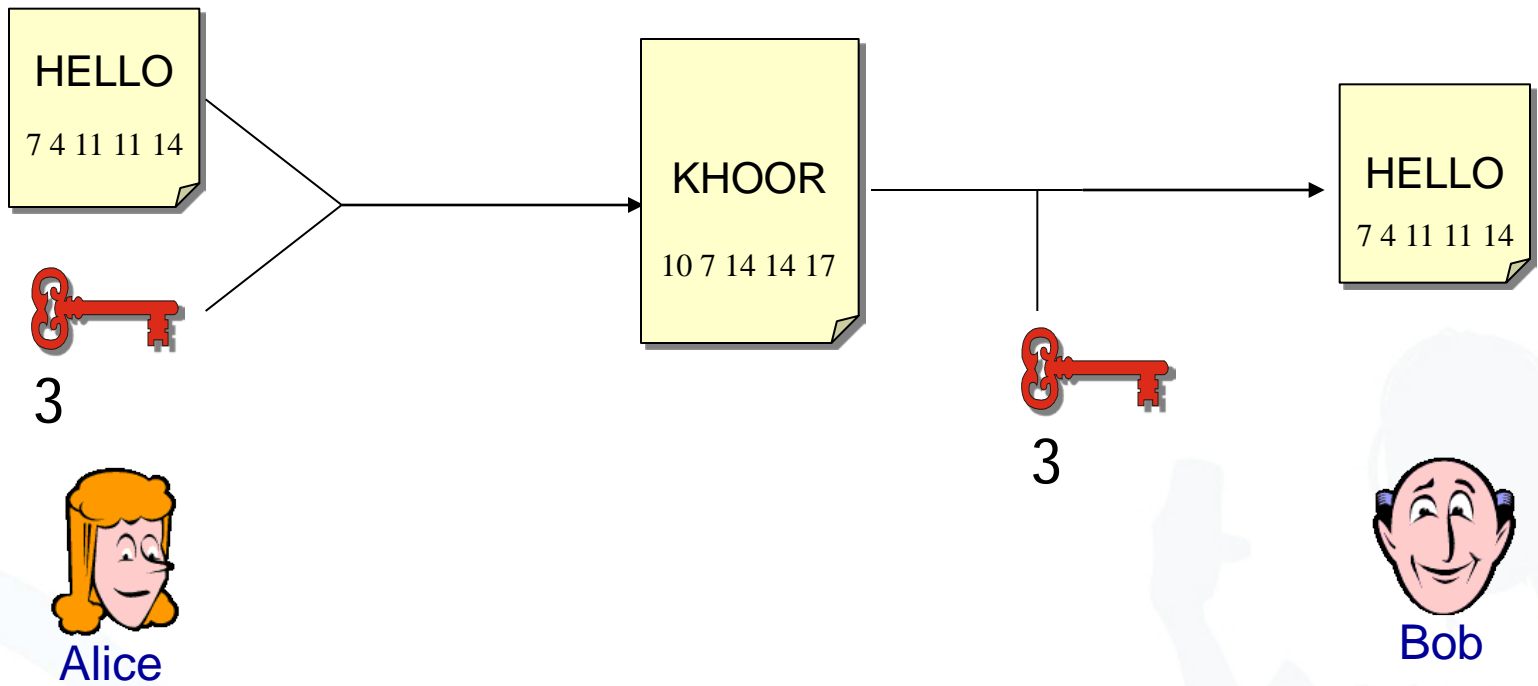
- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|----|----|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

- We assign a number for every character.
- This enables us to calculate with letters as if they were numbers.

Caesar Cipher: Example



- Very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space ($n=26$)
- Therefore, the encryption is very easy and fast to compromise.

- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography

Advanced Encryption Standard

- The Data Encryption Standard (DES) was designed to encipher sensitive but not classified data.
- The standard has been issued in 1977.
- In 1998, a design for a computer system and software that could break any DES-enciphered message within a few days was published.
- By 1999, it was clear that the DES no longer provided the same level of security it had 10 years earlier, and the search was on for a new, stronger cipher.
- The successor is called Advanced Encryption Standard (AES).
- AES has been approved for Secret or even Top Secret information by the NSA.

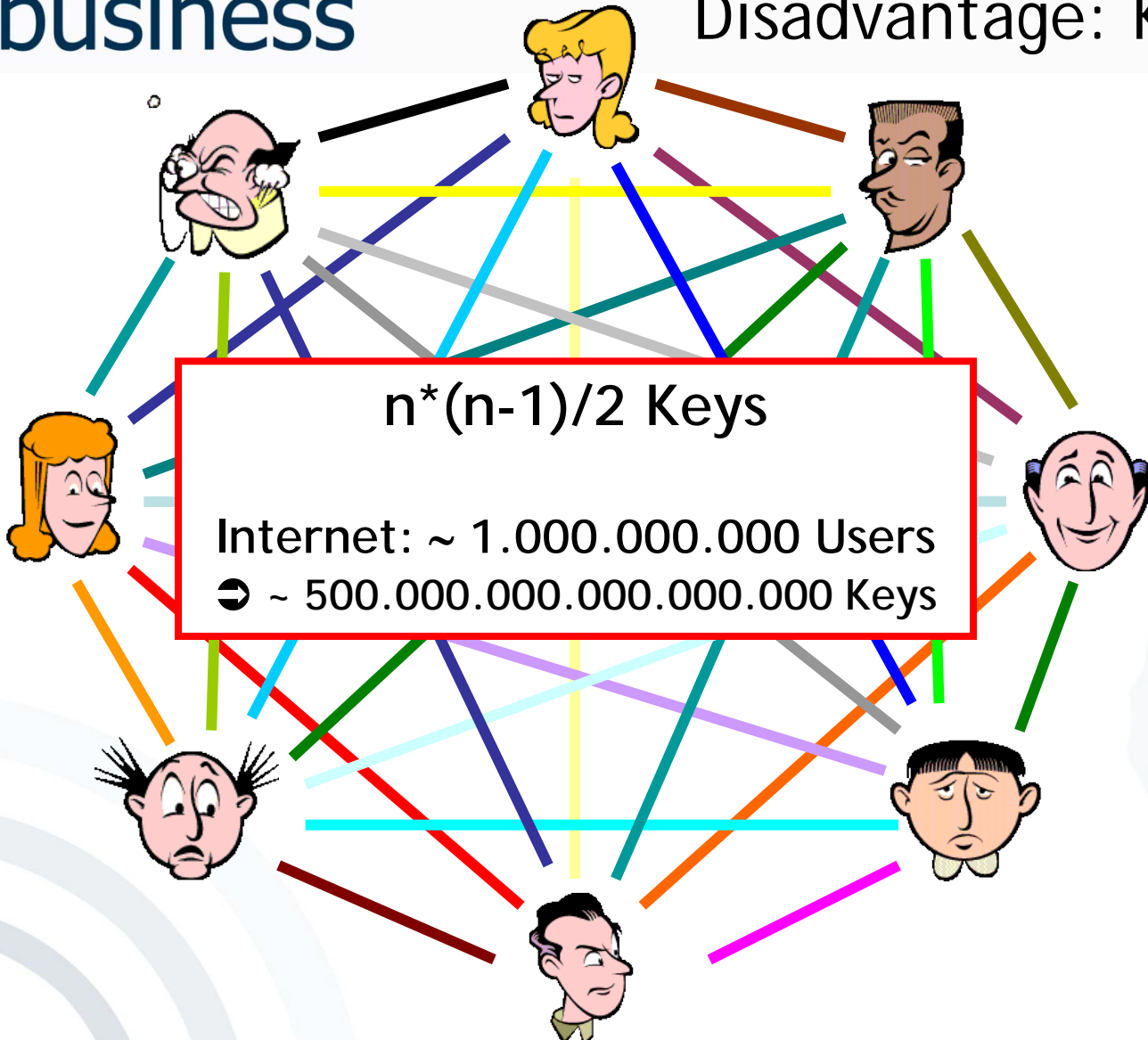
[Bishop 2005]

- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography

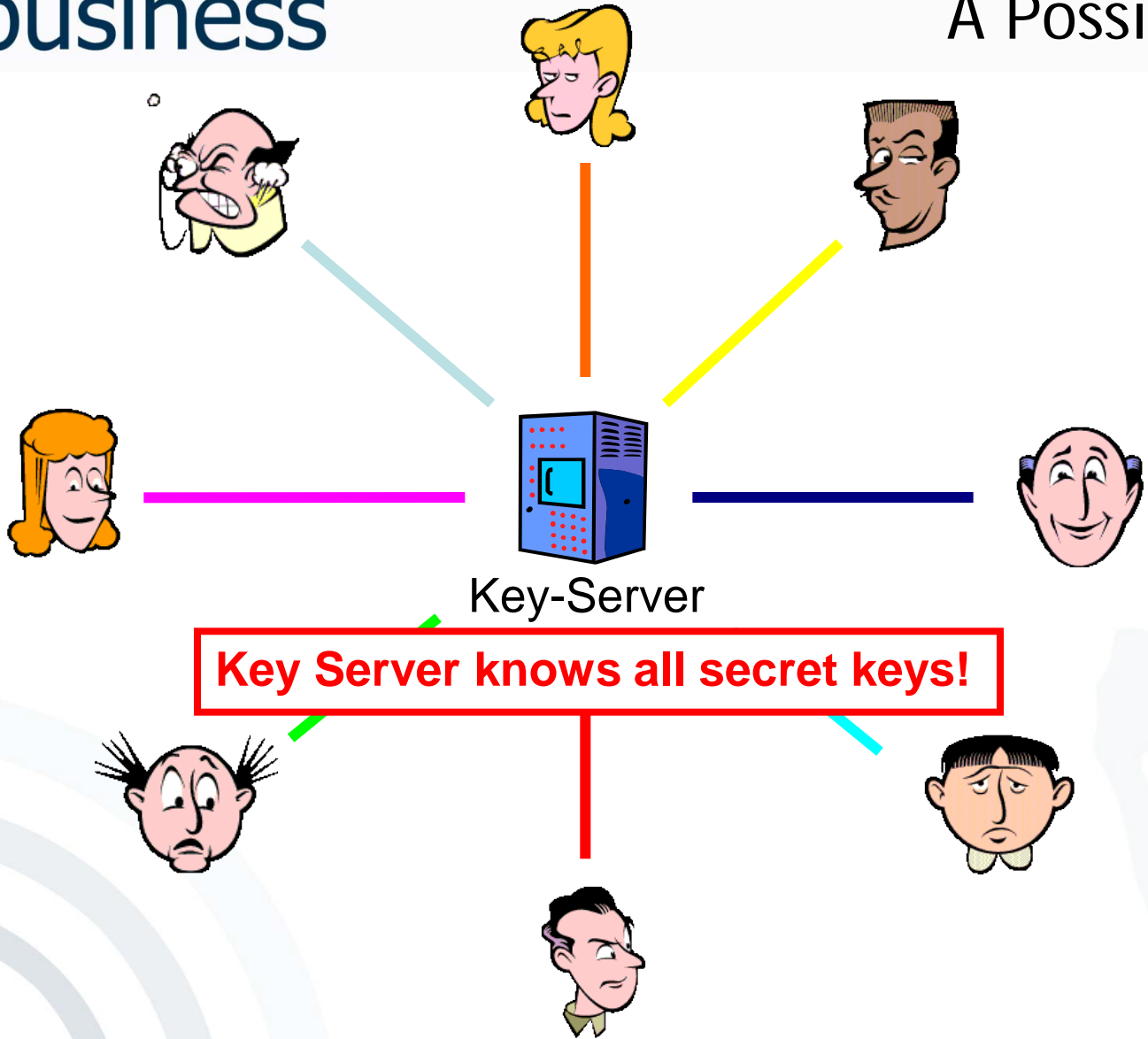
Advantage: Algorithms are very fast

| Algorithm | Performance [*] |
|-----------|--------------------------|
| RC6 | 138 ms |
| AES | 173 ms |
| SERPENT | 200 ms |
| IDEA | 288 ms |
| MARS | 394 ms |
| TWOFISH | 697 ms |
| DES-ede | 726 ms |

*) Encryption of 1 MB-blocks with an Athlon 1GHz processor



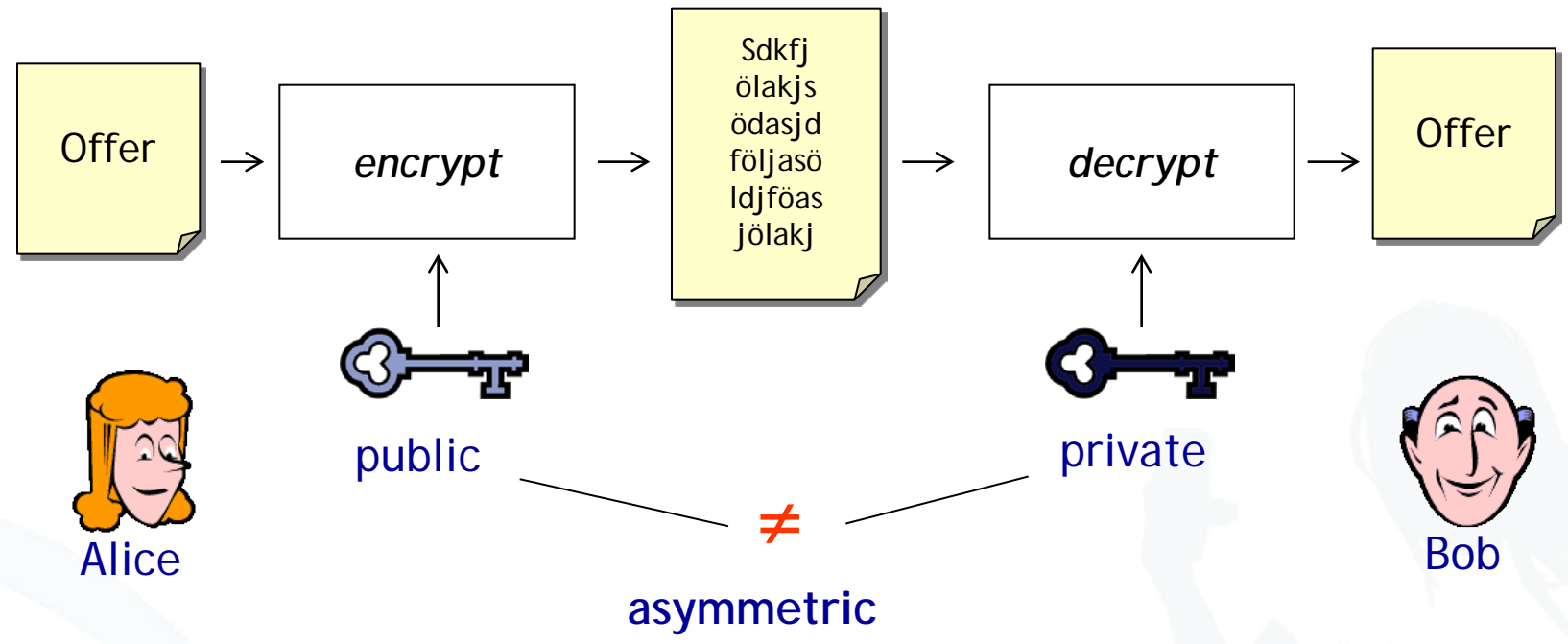
[adopted from J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]



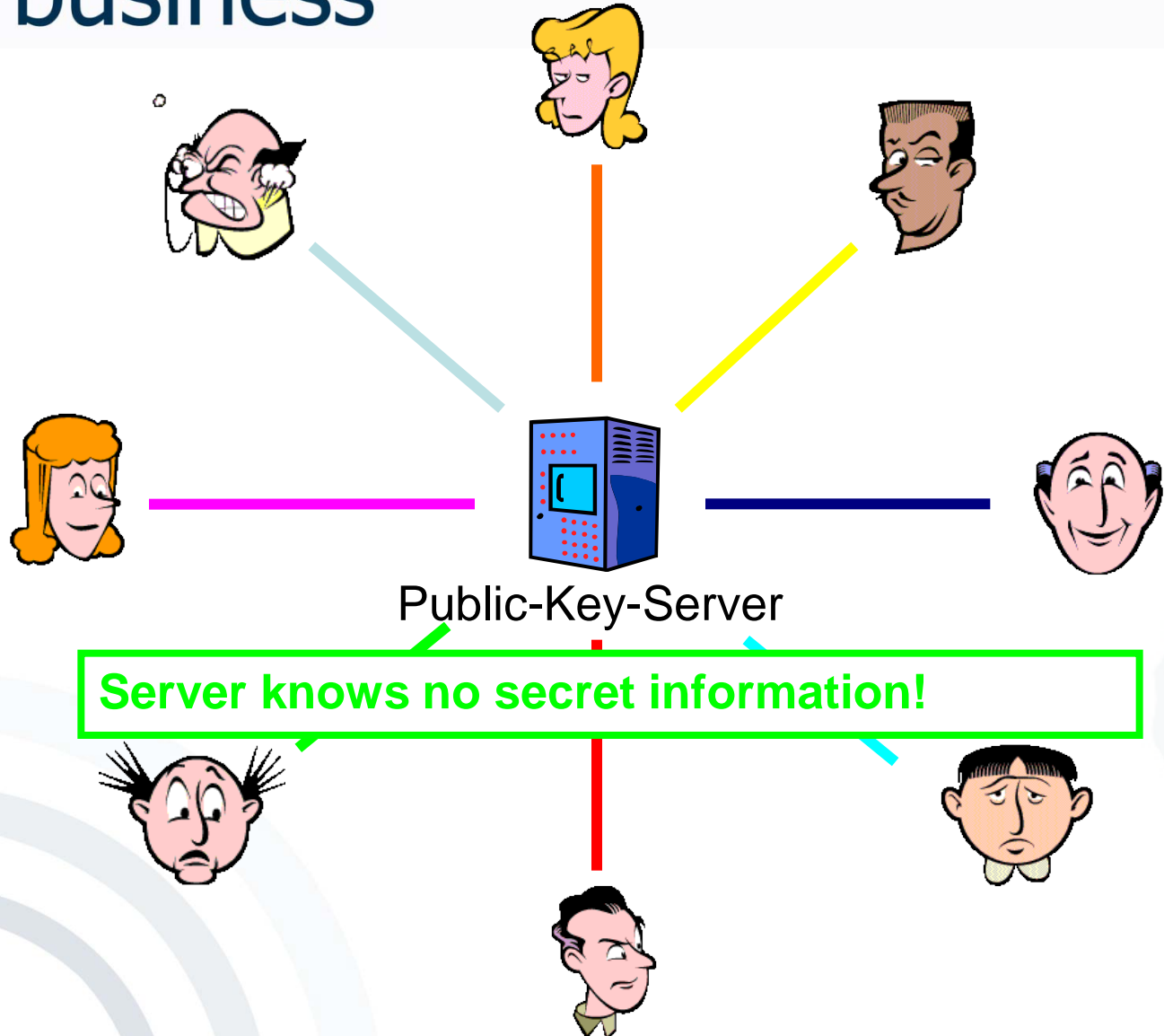
Key Server knows all secret keys!

- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

Public Key Encryption



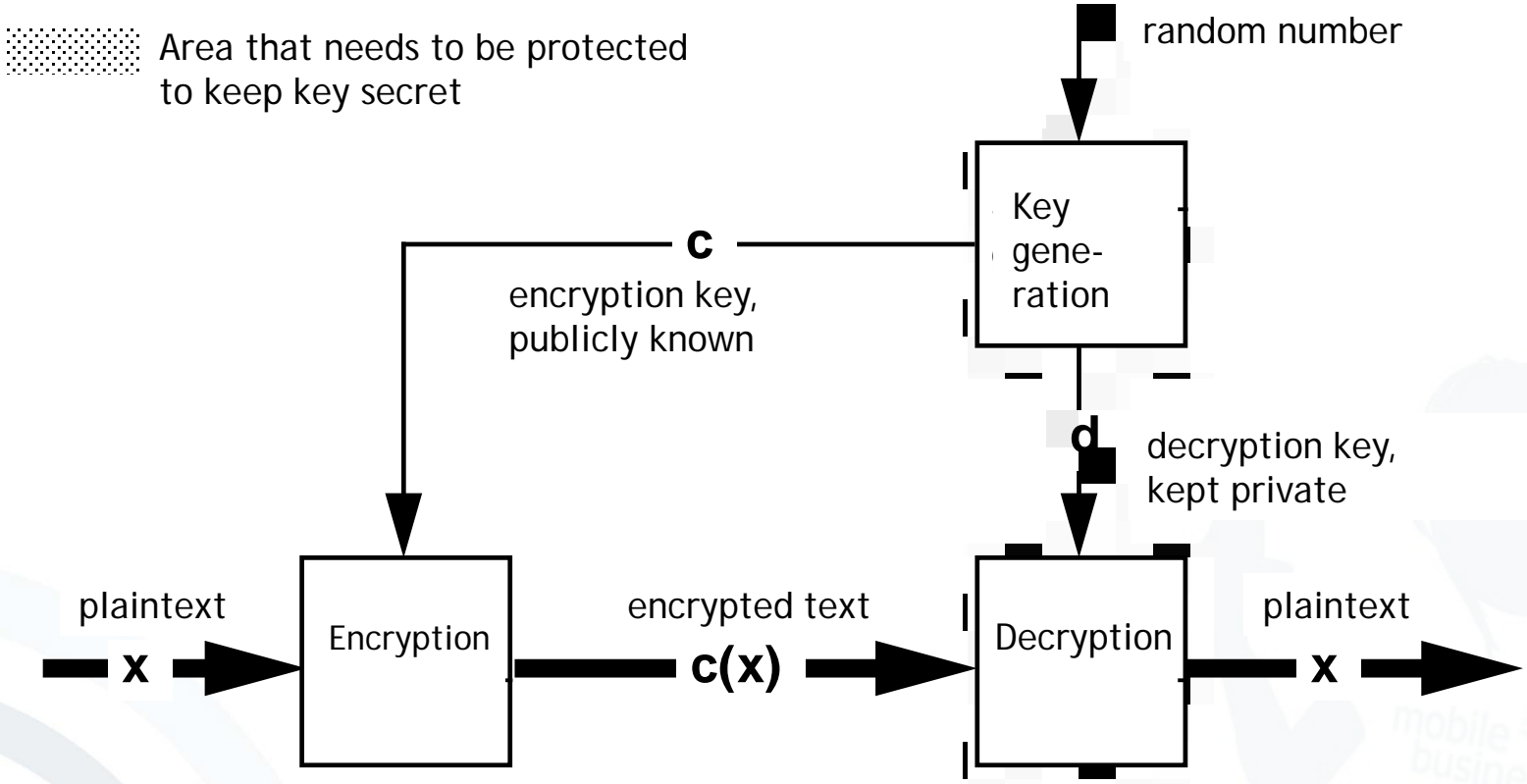
Key Exchange Problem Solved!



- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

- Use of key pairs instead of one key
 - Public key is solely for encryption
 - Encrypted text can only be decrypted with the corresponding private (undisclosed) key.
- The public key can be distributed freely, even via insecure ways (e.g. directory (*public key crypto system*))
- Messages are encoded via the public key of the addressee.
- Only the addressee possesses the private key for decoding.
- This requires some kind of 'matching' between the two keys.
- Private key is hard to derive from public key.

Asymmetric Encryption Systems



box with slot, access to messages only with a key

[based on Federrath and Pfitzmann 1997]

- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

- RSA

- Rivest, Shamir, Adleman, 1978
- is based on the assumption that the factorization of the product of two (big) prime numbers ($p \cdot q$) is “difficult” (product is basis for the keys)
- key lengths typically 1024 bit, today rather 2048 [Rivest et al., 1978]

- Diffie-Hellman

- Diffie, Hellman, 1976, first patented algorithm with public keys
- allows the exchange of a secret key
- is based on the “difficulty” of calculating discrete logarithms in a finite field

[Diffie, Hellman, 1976]

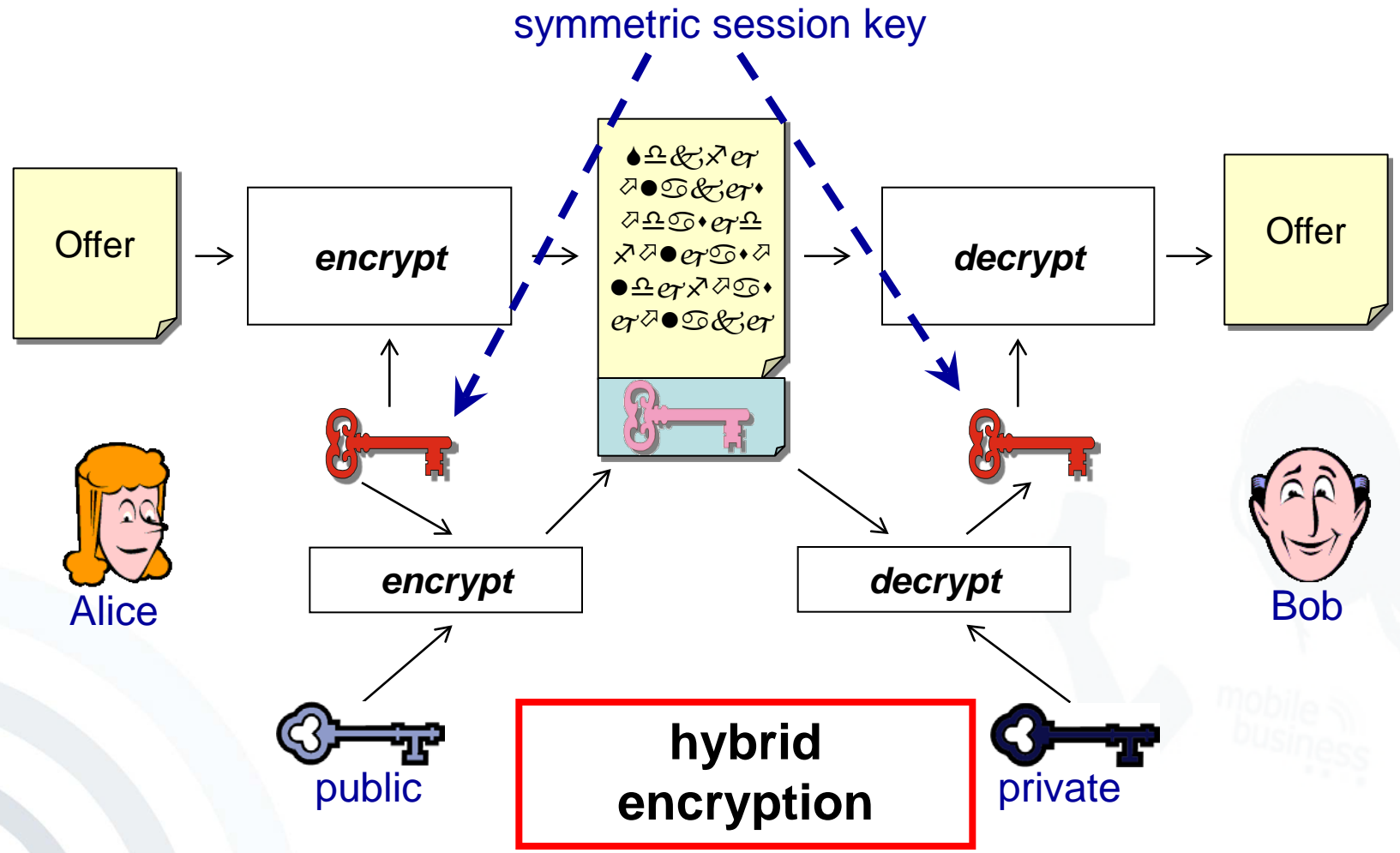
- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

| Algorithm | Performance* |
|-----------|--------------|
| El Gamal | 1826 s |
| RSA | 16 s |

Disadvantage: Complex operations
with very big numbers

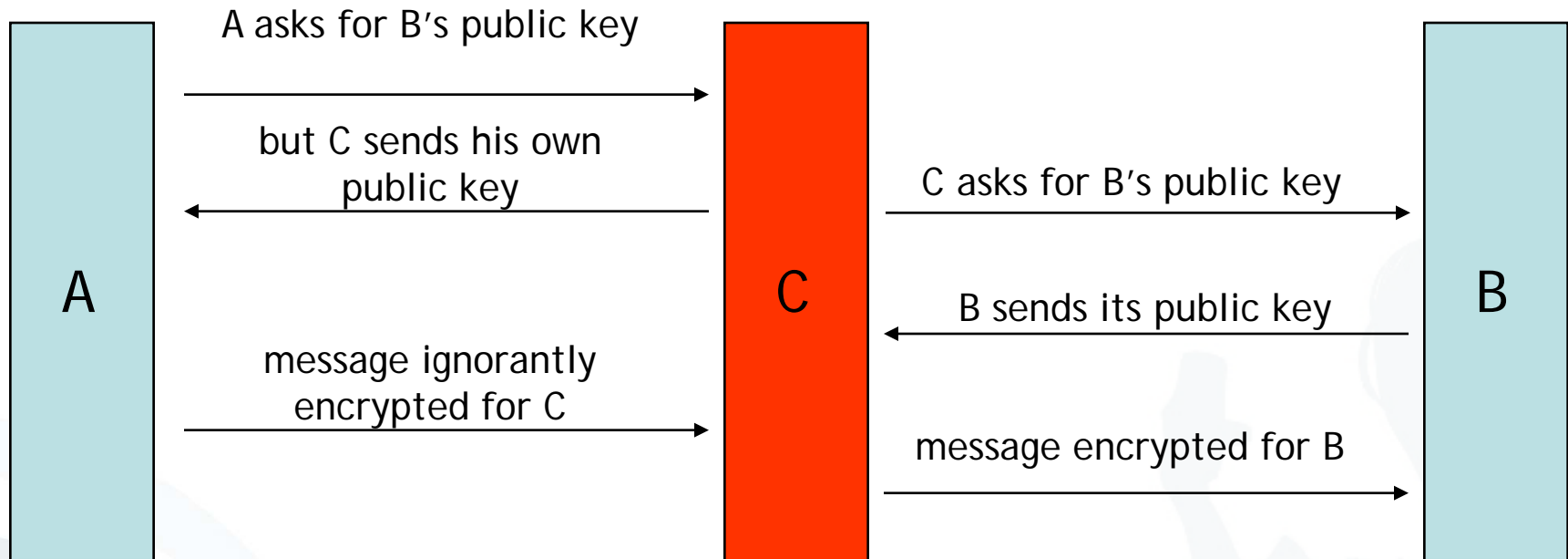
➔ **Algorithms are very slow**

*) Encryption of 1 MB-blocks with an Athlon 1GHz processor



- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

“Man in the middle attack”



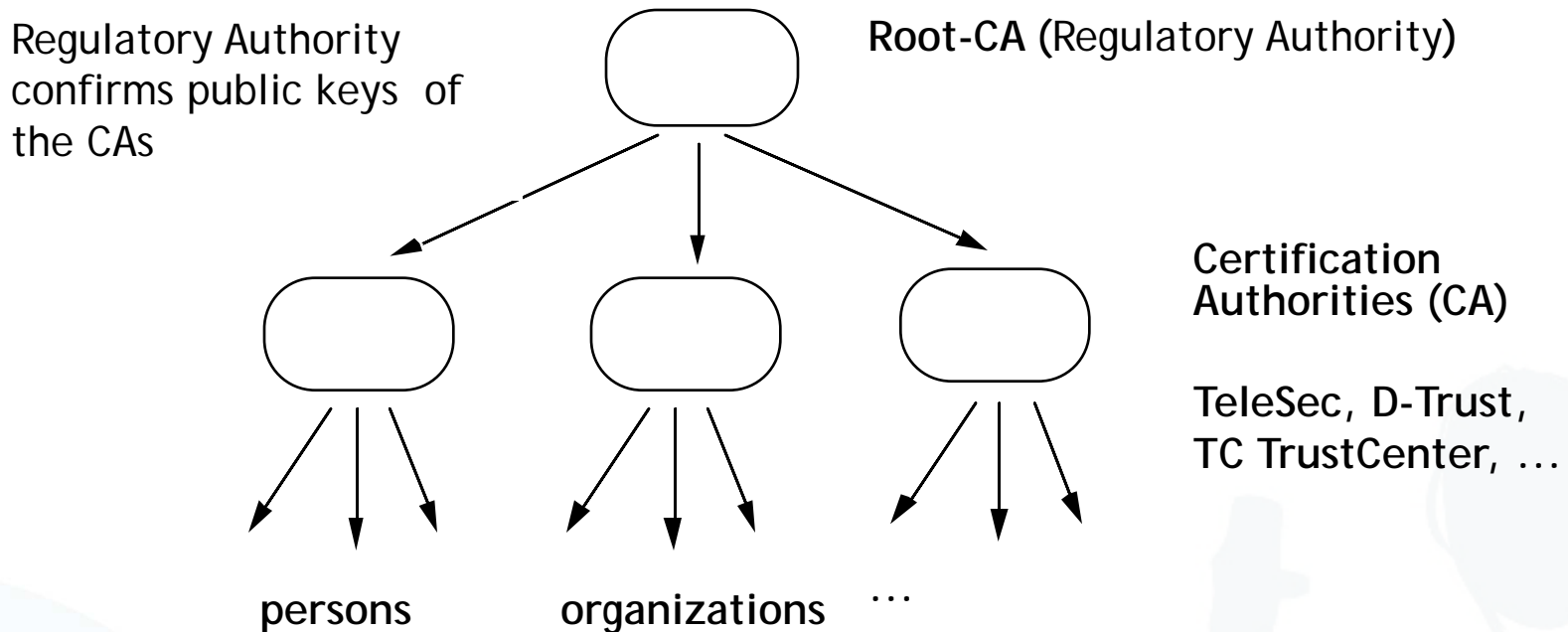
- B can freely distribute his own public key.
- But: Everybody (e.g. C) could distribute a public key and claim that this one belongs to B.
- If A uses this key to send a message to B, C will be able to read this message!
- Thus:
How can A decide if a public key was really created and distributed by B without asking B directly?
 - ➔ Keys get **certified**, i.e. a third person/institution confirms with its (digital) signature the **affiliation of a public key to entity B**.
 - ➔ Public Key Infrastructures (PKIs)

Three types of organization for certification systems (PKIs):

- Central certification authority (CA)
 - A single CA, keys often integrated in checking software
 - Example: older versions of Netscape (CA = Verisign)
- Hierarchical certification system
 - CAs which in turn are certified by “higher” CA
 - Examples: PEM, Teletrust, infrastructure according to Signature Law
- Web of Trust
 - Each owner of a key may serve as a CA
 - Users have to assess certificates on their own
 - Example: PGP (but with hierarchical overlay system)

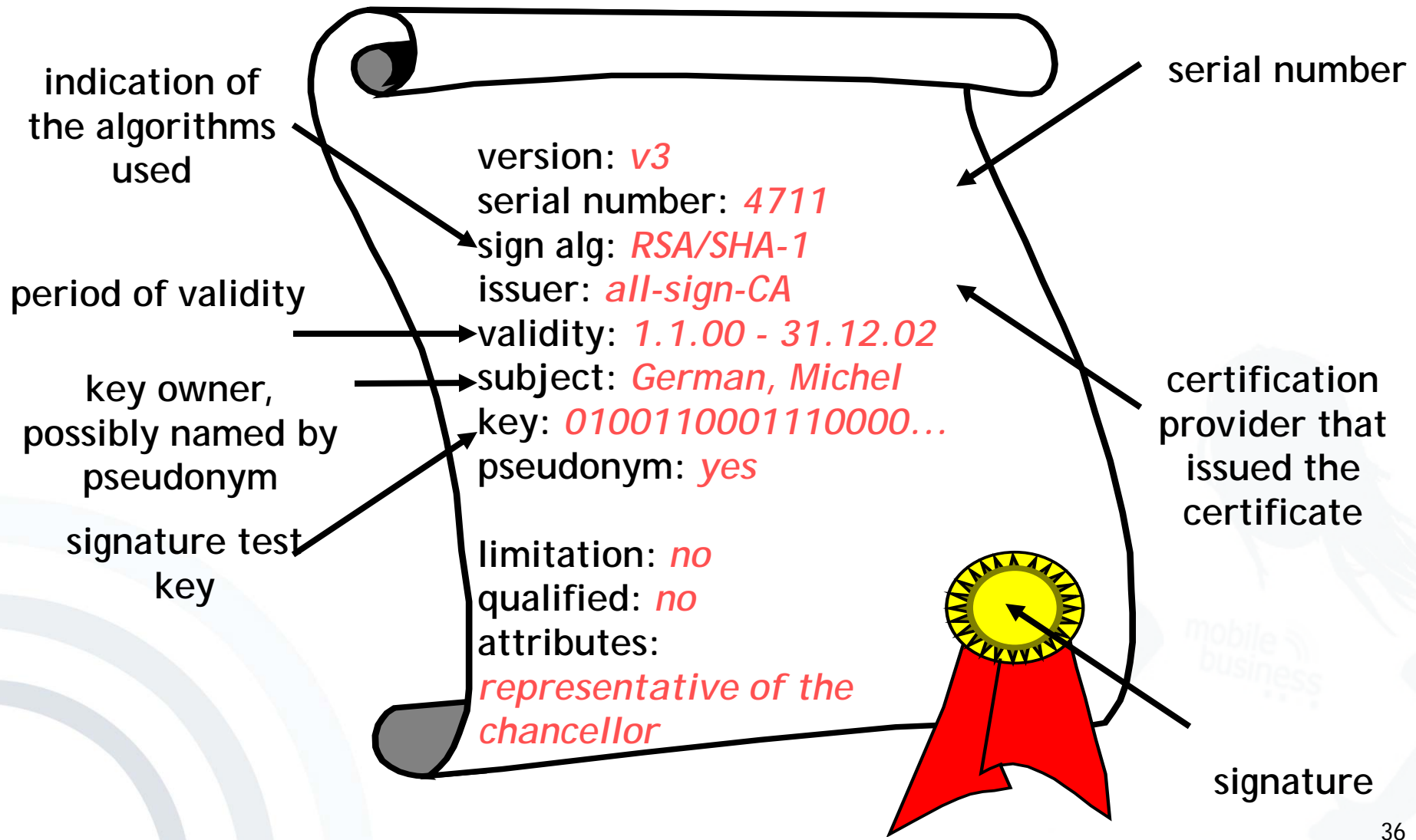
Hierarchical Certification of Public Keys

(Example: German Signature Law)



- The actual checking of the identity of the key owner takes place at so called Registration Authorities (e.g. notaries, bank branches, T-Points, ...)
- Security of the infrastructure depends on the reliability of the CAs.

Content of a Key Certificate (according to German Signature Law and Regulation)

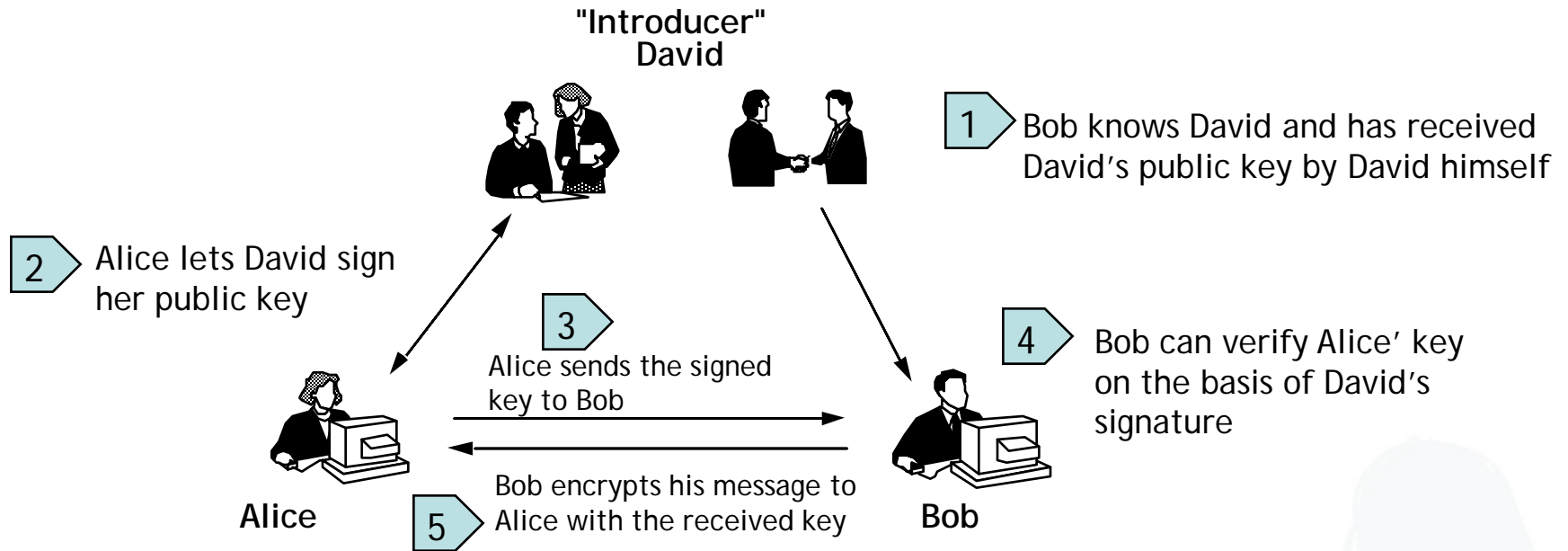


Tasks of a Certification Authority

(according to German Signature Law and Regulation)

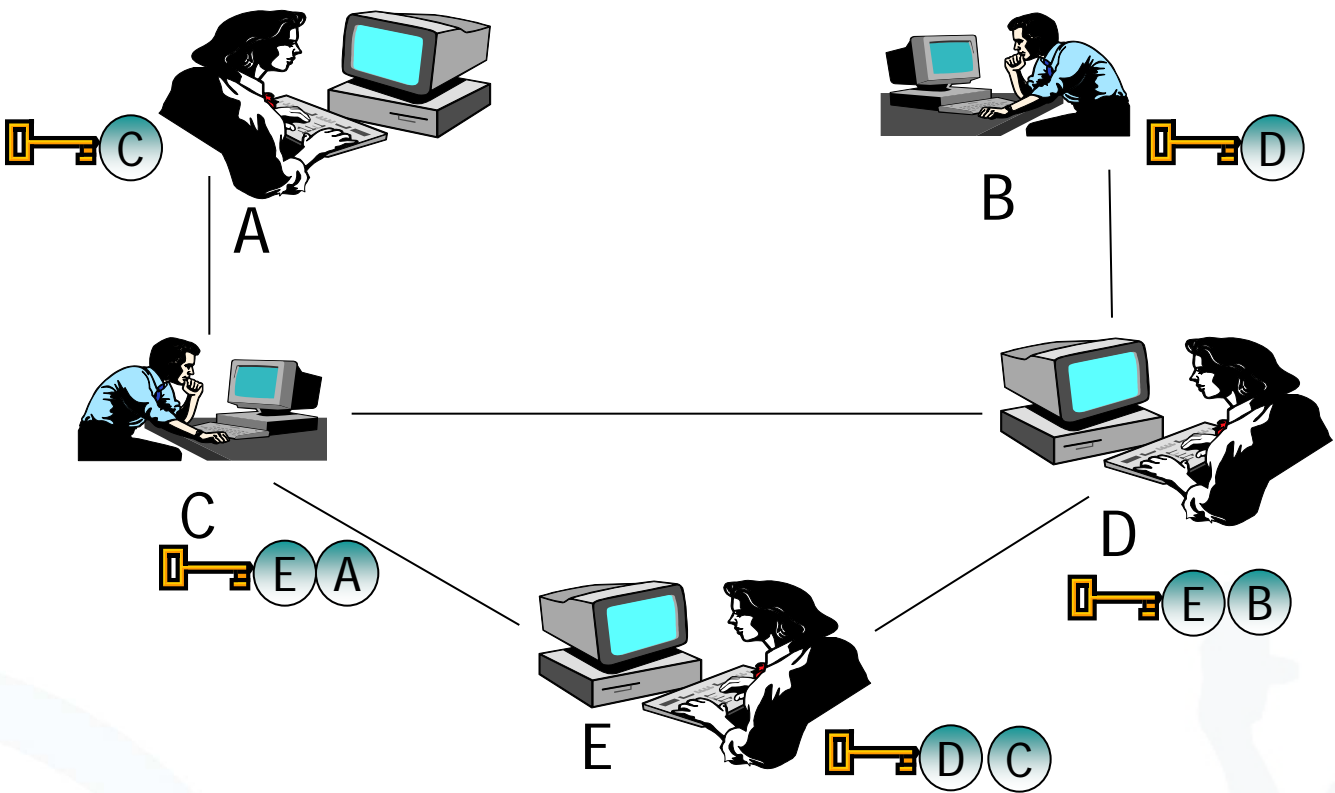
- Reliable identification of persons who apply for a certificate
- Information on necessary methods for fraud resistant creation of a signature
- Provision for secure storage of the private key
 - At least Smartcard (protected with PIN)
- Publication of the certificate (if wanted)
- Barring of certificates
- If necessary emission of time stamps
 - For a fraud resistant proof that an electronic document has been at hand at a specific time

- Checking of the following items by certain confirmation centers (BSI, TÜVIT, ...)
 - Concept of operational security
 - Reliability of the executives and of the employees as well as of their know-how
 - Financial power for continuous operation
 - Exclusive usage of licensed technical components according to SigG and SigV
 - Security requirements as to operating premises and their access controls
- Possibly license of the regulation authority



- Each user can act as a "CA".
- Mapping of the social process of creation of trust.
- Keys are "certified" through several signatures.
- Expansion is possible by public key servers and (hierarchical) CAs.

Web of Trust Example



Web of Trust:

- Certification of the public keys mutually by users
- Level of the mutual trust is adjustable.

- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Key Management
 - Example: PGP

- PGP = Pretty Good Privacy
 - De facto-Standard for freely accessible e-mail encryption systems on the Internet
 - First implementation by Phil Zimmermann
 - Long trial against Phil Zimmermann because of suspicion of violation of export clauses
 - In U.S. free version in cooperation with MIT (agreement with RSA because of the patent)
 - Meanwhile commercialized: www.pgp.com
 - Gnu Privacy Guard (GPG): non-commercial Open Source variant (OpenPGP, RFC2440)

OpenPGP: Encrypt Message

The screenshot shows an email client interface with a message draft and two dialog boxes. The main window is titled 'Verfassen: MB II Slides' and has a menu bar with 'Datei', 'Bearbeiten', 'Ansicht', 'Einstellungen', 'OpenPGP', 'Extras', and 'Hilfe'. The toolbar includes icons for 'Senden', 'Kontakte', 'Rechtschr.', 'Anhang', 'OpenPGP', 'S/MIME', and 'Speichern'. The message draft is addressed to 'Christian Kahl <christian.kahl@m-le...' and has the subject 'MB II Slides'. The body text reads: 'Hi Christian, please find attached the MB II slides for lect...'. Below the draft, contact information for Johann Wolfgang Institute of Business is visible.

The 'OpenPGP-Schlüssel auswählen' dialog box is open, showing a list of recipients for encryption. The first recipient, 'Christian Kahl <christian.kahl@m-lehrstuhl.de>', is selected. Below the list are checkboxes for 'Nachricht unverschlüsselt und nicht unterschrieben senden' and 'Diesen Dialog nicht mehr anzeigen, wenn Verschlüsselung unmöglich ist'. Buttons for 'Liste aktualisieren' and 'Fehlende Schlüssel herunterladen' are also present.

The 'OpenPGP-Bestätigung' dialog box is also open, displaying a confirmation message: 'VERSCHLÜSSELTE Nachricht an folgende Empfänger senden: christian.kahl@m-lehrstuhl.de'. It includes a warning: 'Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt: 0x42B8B29914E21EDA, 0x23EE4D96C4495AF0'. 'Ja' and 'Nein' buttons are at the bottom.

| Empfänger für Verschlüsselung wählen | Vertrauen | Ablauf... | Schlüssel-ID |
|---|------------------|------------|--------------|
| <input checked="" type="checkbox"/> Benutzer-ID | | | |
| <input checked="" type="checkbox"/> Christian Kahl <christian.kahl@m-lehrstuhl.de> | absolutes Ver... | | 14E21EDA |
| <input type="checkbox"/> Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um zu...) | abgelaufen | 02.09.2006 | 8D539C6E |
| <input type="checkbox"/> Alexander Boettcher <ab764283@inf.tu-dresden.de> | - | | A63325B3 |
| <input type="checkbox"/> Alexander Boettcher <ab764283@os.inf.tu-dresden.de> | abgelaufen | 11.10.2005 | F26EE0CD |
| <input type="checkbox"/> Andre Meixner <s4538672@inf.tu-dresden.de> | - | | 7C433232 |
| <input type="checkbox"/> ... | - | | 7E39E652 |
| <input type="checkbox"/> ... | - | | 52B1B05D |
| <input type="checkbox"/> ... | - | | A0D40924 |
| <input type="checkbox"/> ... | - | | 79B42C58 |
| <input type="checkbox"/> ... | - | | B06F3816 |
| <input type="checkbox"/> ... | - | | 0789B57F |
| <input type="checkbox"/> ... | - | 11.04.2011 | 165A5F90 |
| <input type="checkbox"/> ... | - | | 9347DB3C |
| <input type="checkbox"/> ... | - | 20.02.2009 | 48CC64C2 |
| <input type="checkbox"/> ... | - | | 8EF041F1 |
| <input type="checkbox"/> ... | - | | 289E7DB2 |
| <input type="checkbox"/> Katja Liesebach <katja.liesebach@m-chair.net> | absolutes Ver... | | C4495AF0 |
| <input type="checkbox"/> Katrin Borcea <kati@inf.tu-dresden.de> | - | | F7C207CE |

OpenPGP: Decrypt Message

☐ **Betreff:** MB II Slides
Von: [Katja Liesebach <katja.liesebach@m-chair.net>](mailto:katja.liesebach@m-chair.net)
Datum: 19:18
An: [Christian Kahl <christian.kahl@m-chair.net>](mailto:christian.kahl@m-chair.net)

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.7 (MingW32)
Comment: Using GnuPG with Mozilla

hQE0Azxc3rSs71RREAQAoa4NK8beVOV:
iEsWpmlxA11HIpTZtIKd9ecdjV1OFOJ:
6xxXLtS6PkSb0k5nKkMZ1147F80IrvW
/0md5jC1R8N/NJeuSfsW6w1LUpTVHQQ
zQAvcf2AvjqHHw4UldKW8ewB3GG4zqD
XxkOviAC+ADTcPgF5FvYPpbEiKS9D8dgzZrBd07YIfdH0oMBgga9K
JMwn2/s+Mn6AqNVhdPJuh8VaFvLW+up3GZ+msGd3v4P80Z1VBS4sq
jOkaydJkxKqriLNqgiY39ltyZUtowlJaa+uPK2pq1A311DHEoqm8y
cFJW5KxpqNFGyixn7wU6I+e7d6Df8Q==
=eEkh

-----END PGP MESSAGE-----

OpenPGP-Eingabe

Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein

Erst nach 5 Minuten

OK

☐ **Betreff:** MB II Slides
Von: [Katja Liesebach <katja.liesebach@m-chair.net>](mailto:katja.liesebach@m-chair.net)
Datum: 19:18
An: [Christian Kahl <christian.kahl@m-chair.net>](mailto:christian.kahl@m-chair.net)

Hi Christian,

please find attached the MB II slides for lecture 7.

--
Dipl.-Medien-inf. Katja Liesebach

Johann Wolfgang Goethe University Frankfurt a. M.
Institute of Business Informatics
Chair of Mobile Business and Multilateral Security
Graefstr. 78, D-60486 Frankfurt a. M., Germany

Internet: <http://m-chair.net>
Fon: +49 (69) 798-25313
Fax: +49 (69) 798-25306

- Certification of public keys by users: “Web of Trust”
- Differentiation between ‘validity’ and ‘trust’
 - ‘Trust’:
trust that a person / an institution signs keys only if their authenticity has really been checked
 - ‘Validity’:
A key is valid for me if it has been signed by a person / an institution I trust (ideally by myself).
- Support through key-servers:
collection of keys, allocation of ‘validity’ and ‘trust’ remains task of the users
- Path server:
finding certification paths between keys

OpenPGP-Schlüssel verwalten

Zeige Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten: Alle zeigen

| Benutzer-ID | Vertrauen | Ablauf-D... | Typ |
|--|---------------------|-------------|------------|
| Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um z... | abgelaufen | 02.09.2006 | öffentlich |
| ⊕ Alexander Boettcher <ab764283@inf.tu-dresden.de> | absolutes Vertrauen | | öffentlich |
| ⊕ Alexander Boettcher <ab764283@os.inf.tu-dresden.de> | abgelaufen | 11.10.2005 | öffentlich |
| Andre Meixner <s4538672@inf.tu-dresden.de> | - | | öffentlich |
| Andreas Albers <andreas.albers@m-lehrstuhl.de> | absolutes Vertrauen | | öffentlich |
| Andreas Pfitzmann <pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE | absolutes Vertrauen | | öffentlich |
| André Deuker <andre.deuker@m-lehrstuhl.de> | absolutes Ve | | |
| Birgit Pretscheck <birgit.pretscheck@gmx.net> | - | | |
| Christian Kahl <christian.kahl@m-lehrstuhl.de> | absolutes Ve | | |
| ⊕ Denis Royer <me@myasterisk.de> | absolutes Ve | | |
| Elvira Koch <Elvira.Koch@m-lehrstuhl.de> | volles Vertra | | |
| Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> | - | | |
| ⊕ Hagen Wahrig <wahrig@web.de> | - | | |
| ⊕ Jan Zibuschka <zibuschka@m-lehrstuhl.de> | absolutes Ve | | |
| ⊕ Kai Rannenber <Kai.Rannenber@m-lehrstuhl.de> | absolutes Ve | | |
| Katja Liesebach <katja.liesebach@inf.tu-dresden.de> | - | | |
| Katja Liesebach <katja.liesebach@m-chair> | absolutes V | | |
| ⊕ Katrin Borcea <kati@inf.tu-dresden.de> | - | | |
| Marco Lehmann <m99@gmx.li> | - | | |
| ⊕ Mathias Staab <mathias.staab@arcor.de> | - | | |
| Mike Beremann (dienstlich, TU Dresden, unbeschrnkt altia) <mb41@inf.t... | - | | |

Schlüsseleigenschaften

Primäre Benutzer-ID:

Schlüssel-ID:

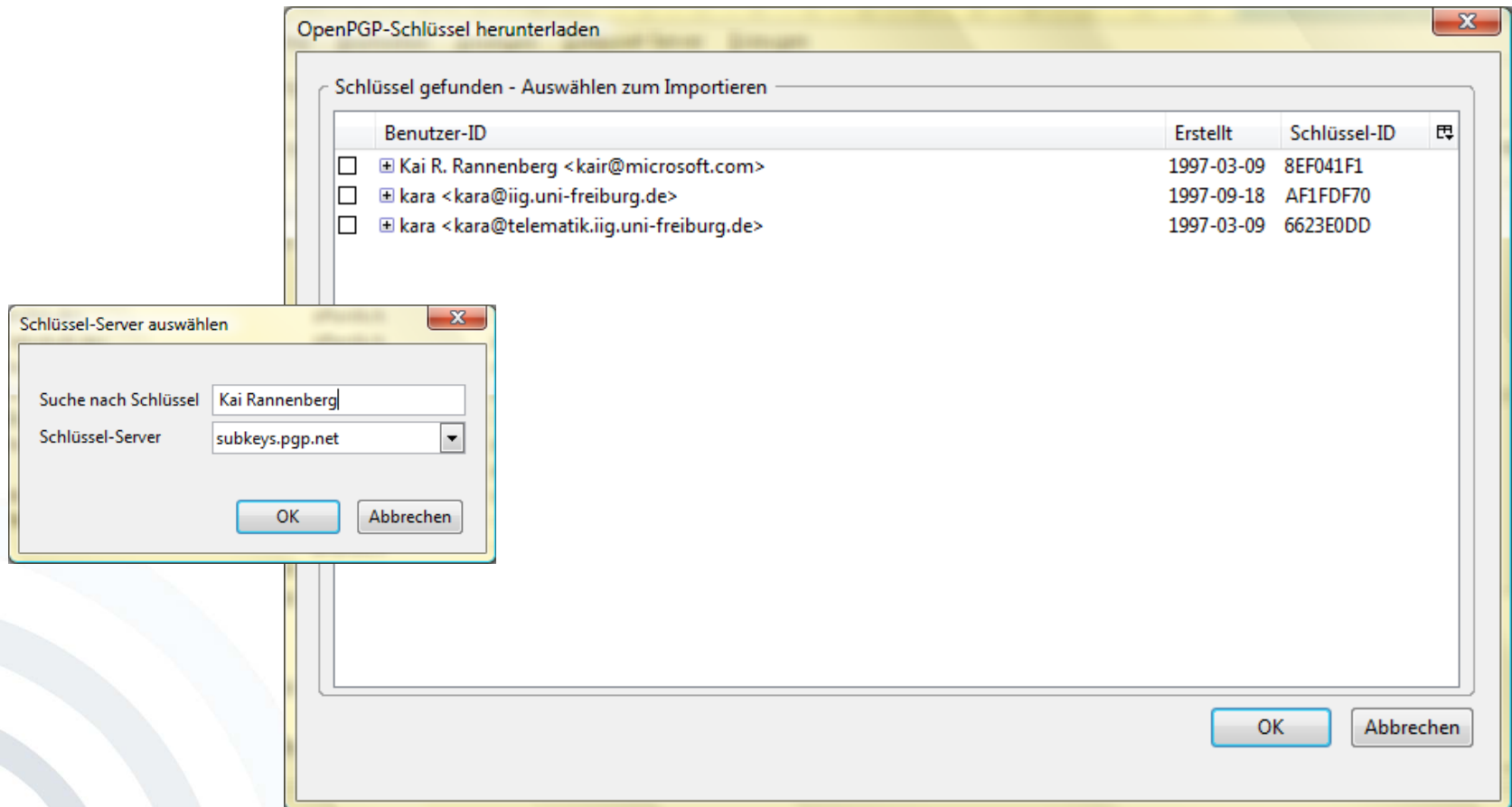
Typ:

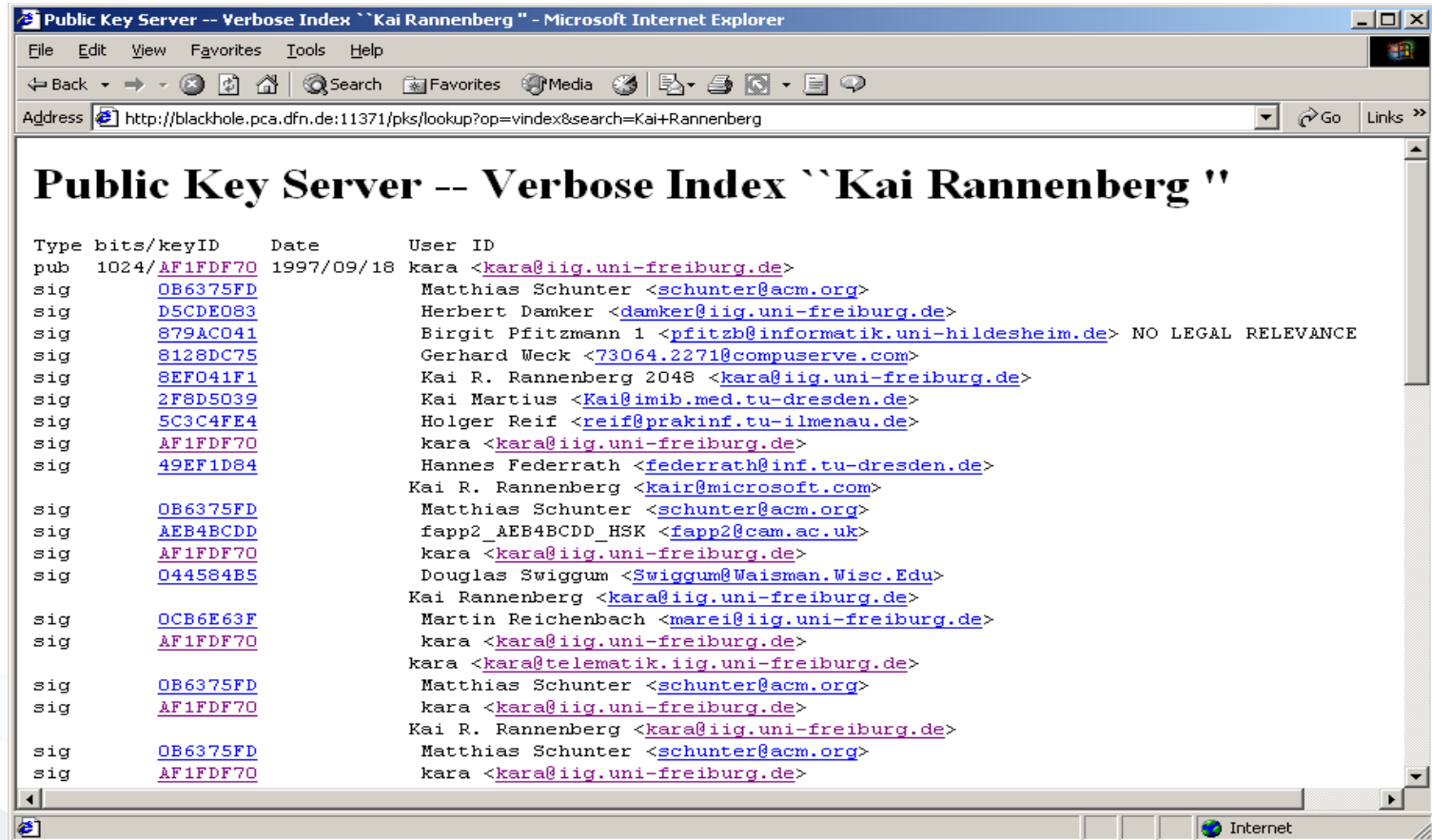
Vertrauen:

Besitzer-Vertrauen:

Fingerabdruck:

| Typ | ID | Algo... | Stär... | Erzeugt | Ablauf-Datum |
|----------------|-----------|---------|---------|------------|--------------|
| Unterschlüssel | 0x98F0... | ELG | 2048 | 07.09.2007 | nie |





- Network of public-key-servers:
www.pca.dfn.de/eng/dfnpca/pgpkserv
www.openpgp.net/pgpsrv.html

- Brute-Force-Attacks on the pass phrase
 - PGPCrack for conventionally encrypted files
- Trojan horses, changed PGP-Code
 - e.g. predictable random numbers, encryption with an additional key
- Attacks on the computer of the user
 - not physically deleted files
 - paged memory
 - keyboard monitoring
- Analysis of electromagnetic radiation
- Non-technical attacks
- Confusion of users [Whitten, Tygar 1999]

“Anybody who asserts that a problem is readily solved by encryption, understands neither encryption nor the problem.”

(Roger Needham /
Butler Lampson)



- Bishop, M. (2005)
Introduction to Computer Security, Addison Wesley, Boston, pp. 97-116.
- Diffie, W. and Hellman, M. E. (1976)
New Directions in Cryptography, *IEEE Transactions on Information Theory* (22:6), pp. 644-654.
- Federrath, H. and Pfitzmann, A. (1997)
Bausteine zur Realisierung mehrseitiger Sicherheit, in: G. Müller and A. Pfitzmann (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Boston, Addison Wesley, pp. 83-104.
- Rivest, R. L.; Shamir, A. and Adleman, L. (1978)
A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM* (21:2), pp. 120-126.
- Whitten, A. and Tygar, J. (1999) *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In: Proceedings of the 9th USENIX Security Symposium, August 1999, www.gaudior.net/alma/johnny.pdf