

## *Lecture 7*

# Cryptography



Mobile Business II (SS 2008)

Prof. Dr. Kai Rannenberg

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

mb

- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography



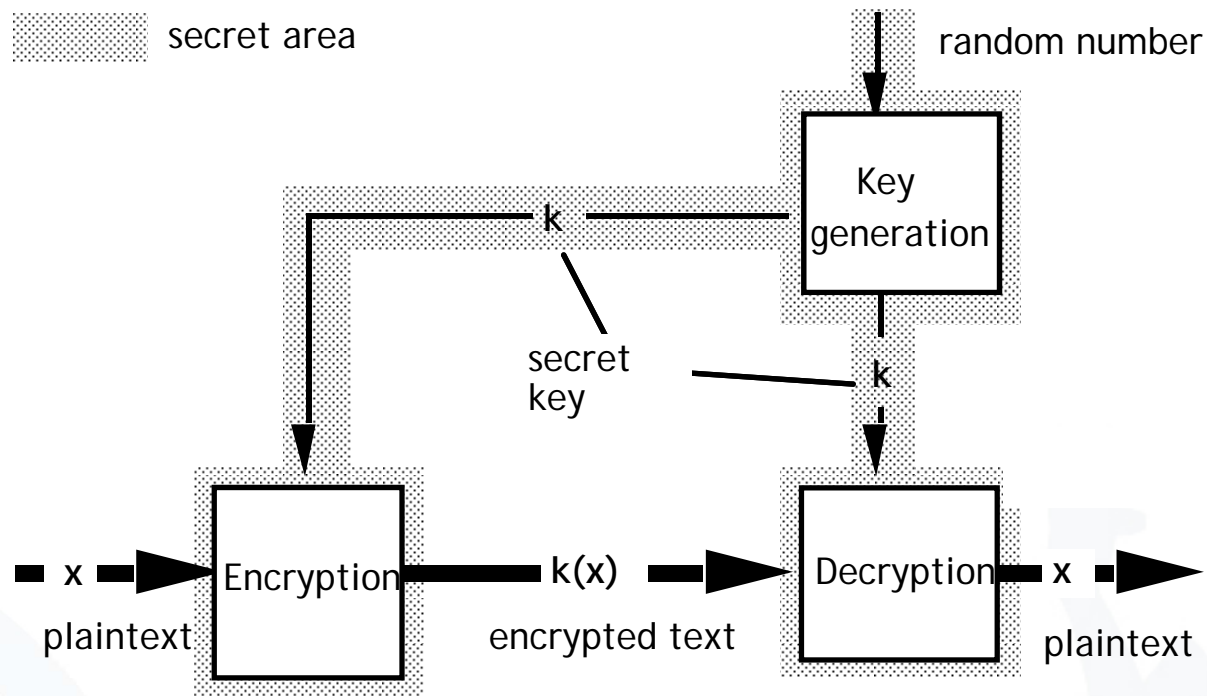
- Intention
  - Confidentiality (secrecy of messages):  
**encryption systems**
  - Integrity (protection from undetected manipulation) and accountability:  
**authentication systems** and **digital signature systems**
- Key distribution
  - **Symmetric:**  
Both partners have the same key.
  - **Asymmetric:**  
Sender and addressee have different (but related) keys.
- 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
- Examples
  - **Vernam-Code** (one-time pad, Gilbert Vernam)
    - key length = length of the plaintext (information theoretically secure)
  - **DES: Digital Encryption Standard**
    - key length 56 bit, so 256 different keys
  - **AES: Advanced Encryption Standard** (Rijndael, [NIST])
    - 3 alternatives for key length: 128, 192 und 256 bit

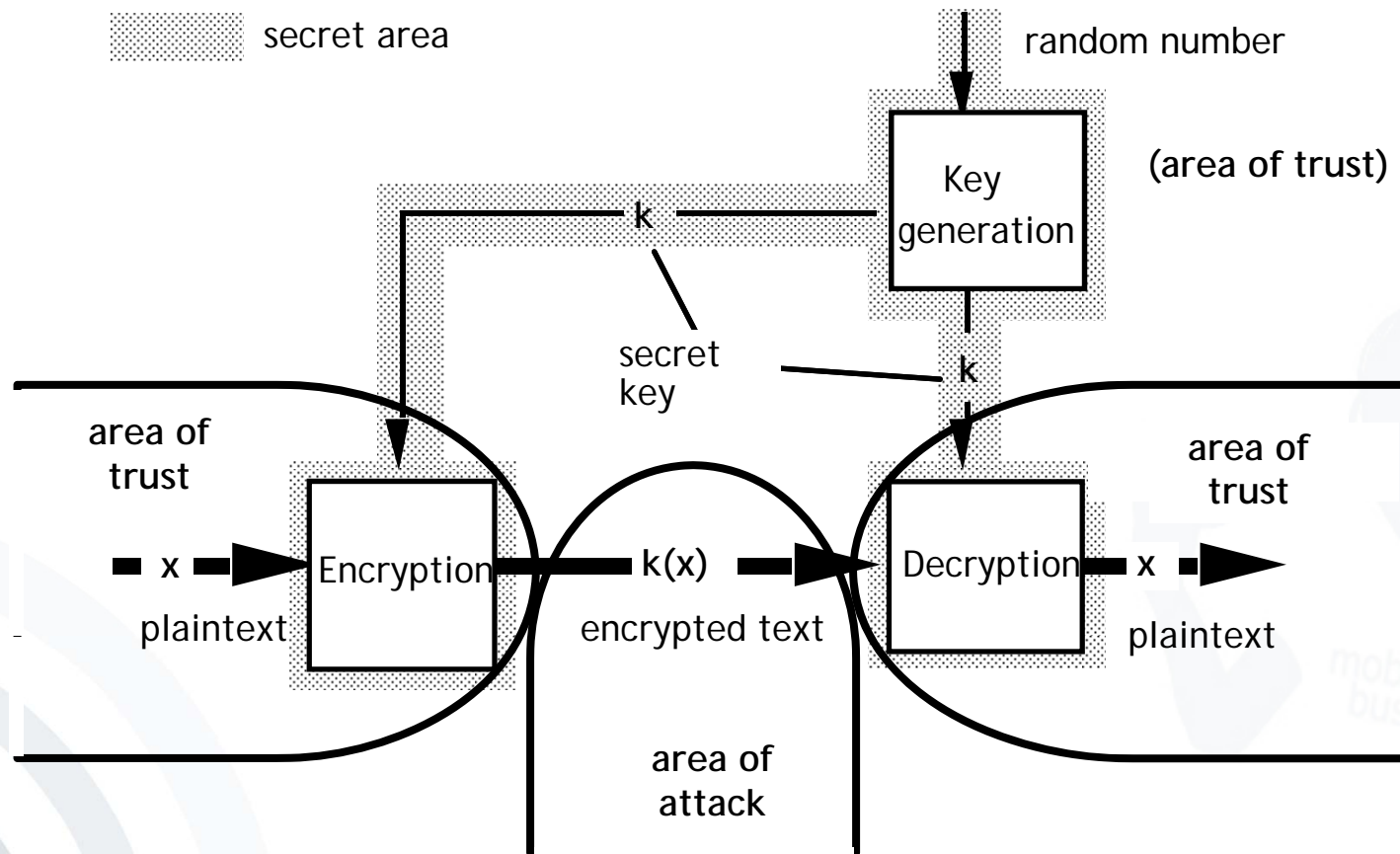
- Introduction
- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES
  - Advantages and Problems
- Public Key Cryptography

# Symmetric Encryption Systems



*black box with lock, two equal keys*

# Symmetric Encryption Systems



- 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).
- Each key shall be equally probable.
- 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.

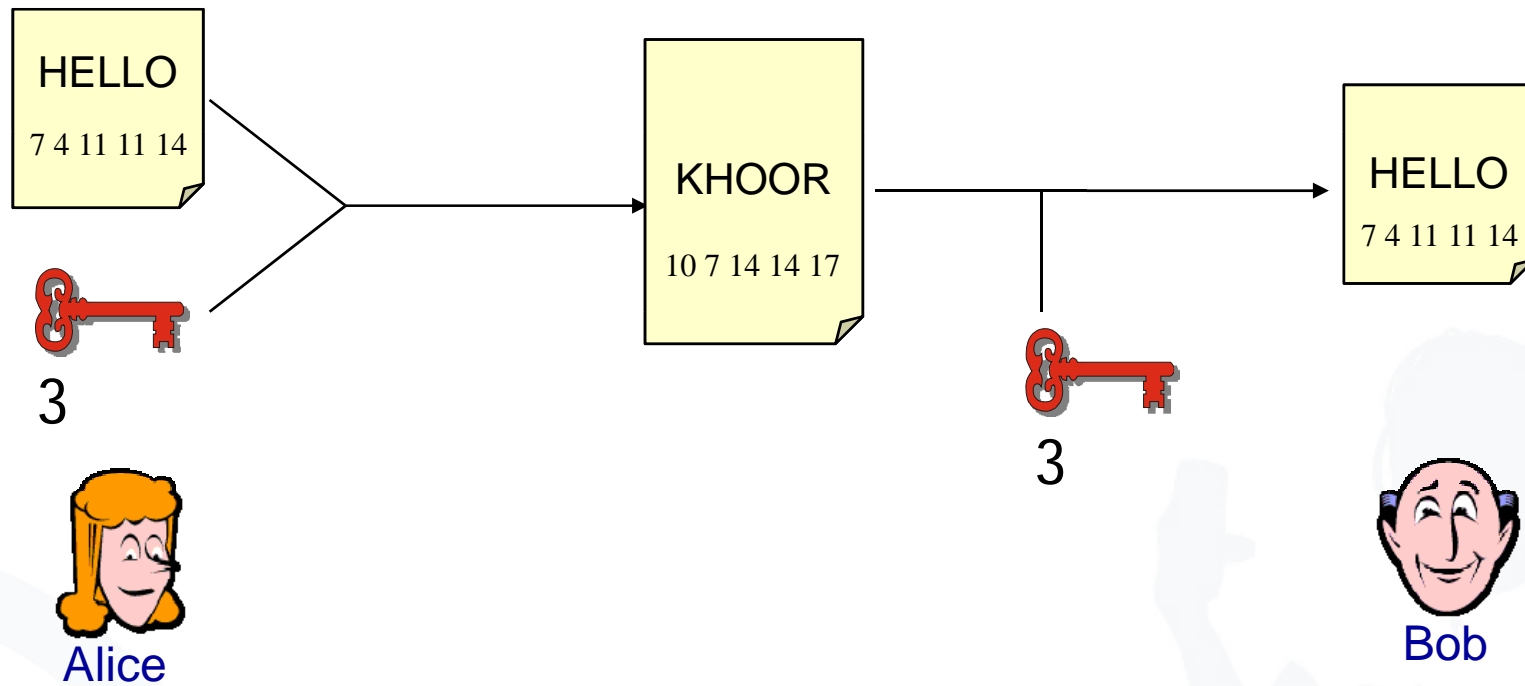
- Introduction
- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES
  - Advantages and Problems
- Public Key Cryptography

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

- 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.
- This new cipher is called Advanced Encryption Standard (AES).
- AES has been approved for Secret or even Top Secret information by the NSA.

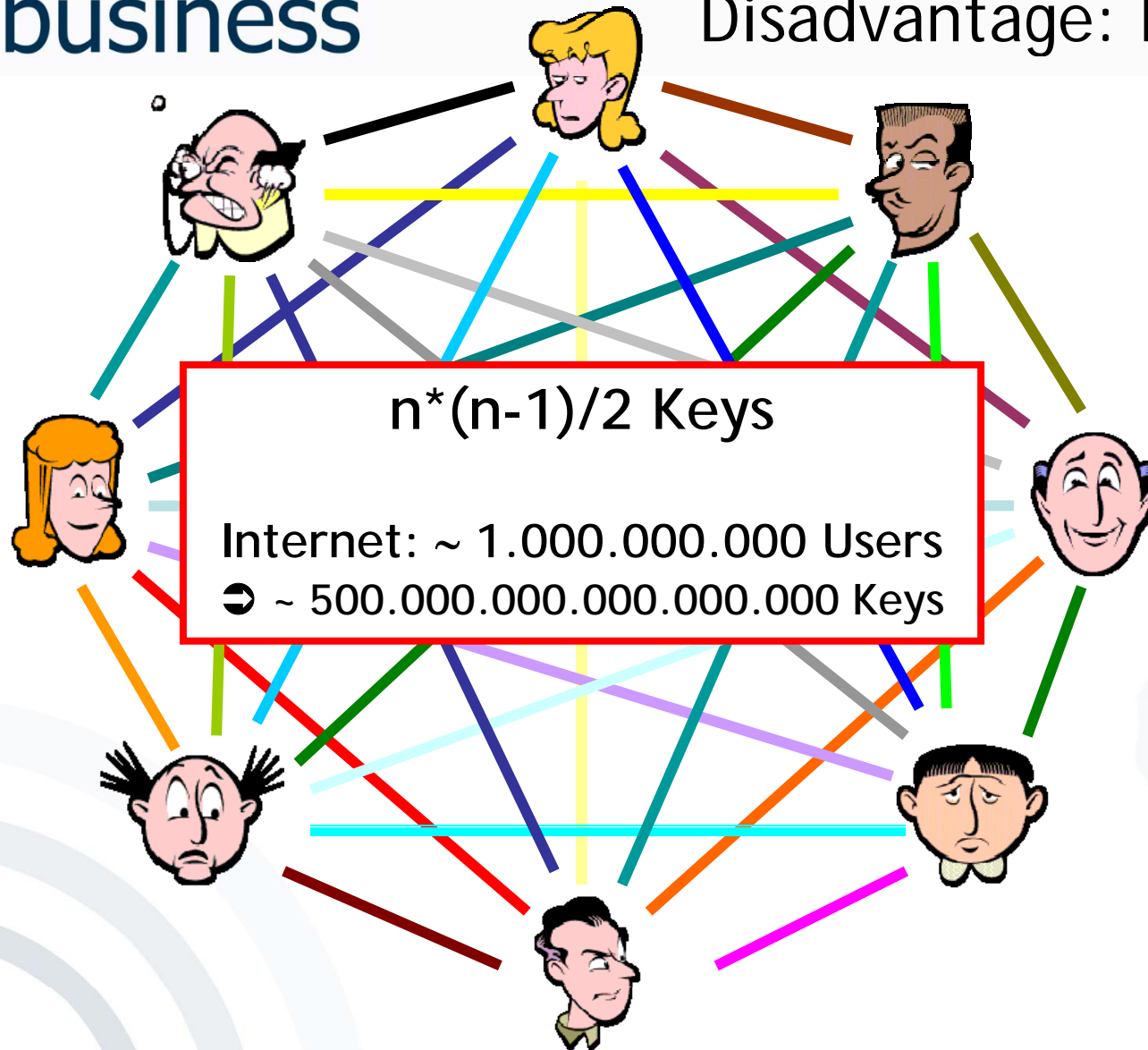
[Bishop 2005]

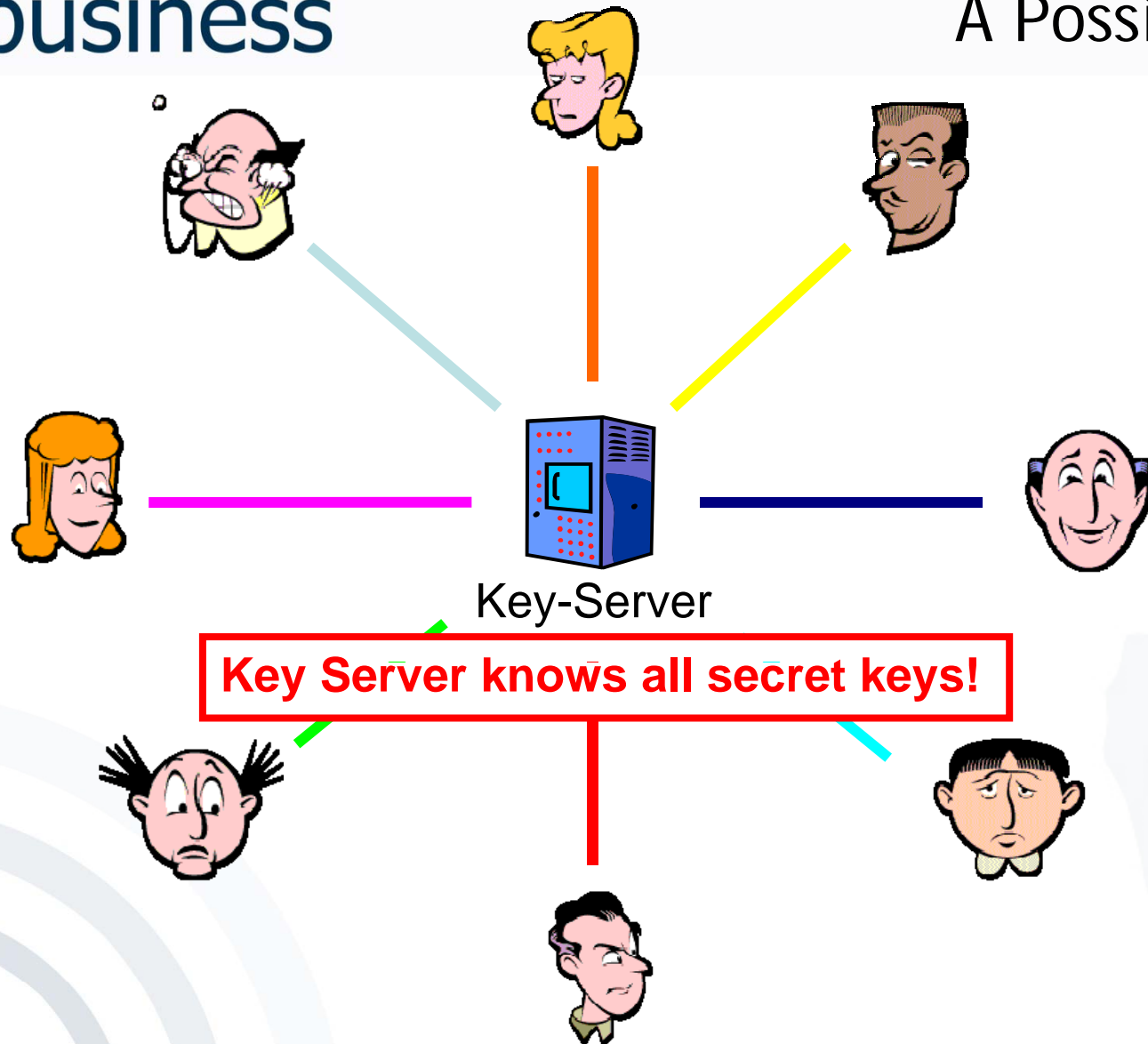
- Introduction
- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES
  - Advantages and Problems
- Public Key Cryptography

## Advantage: Algorithms are very fast

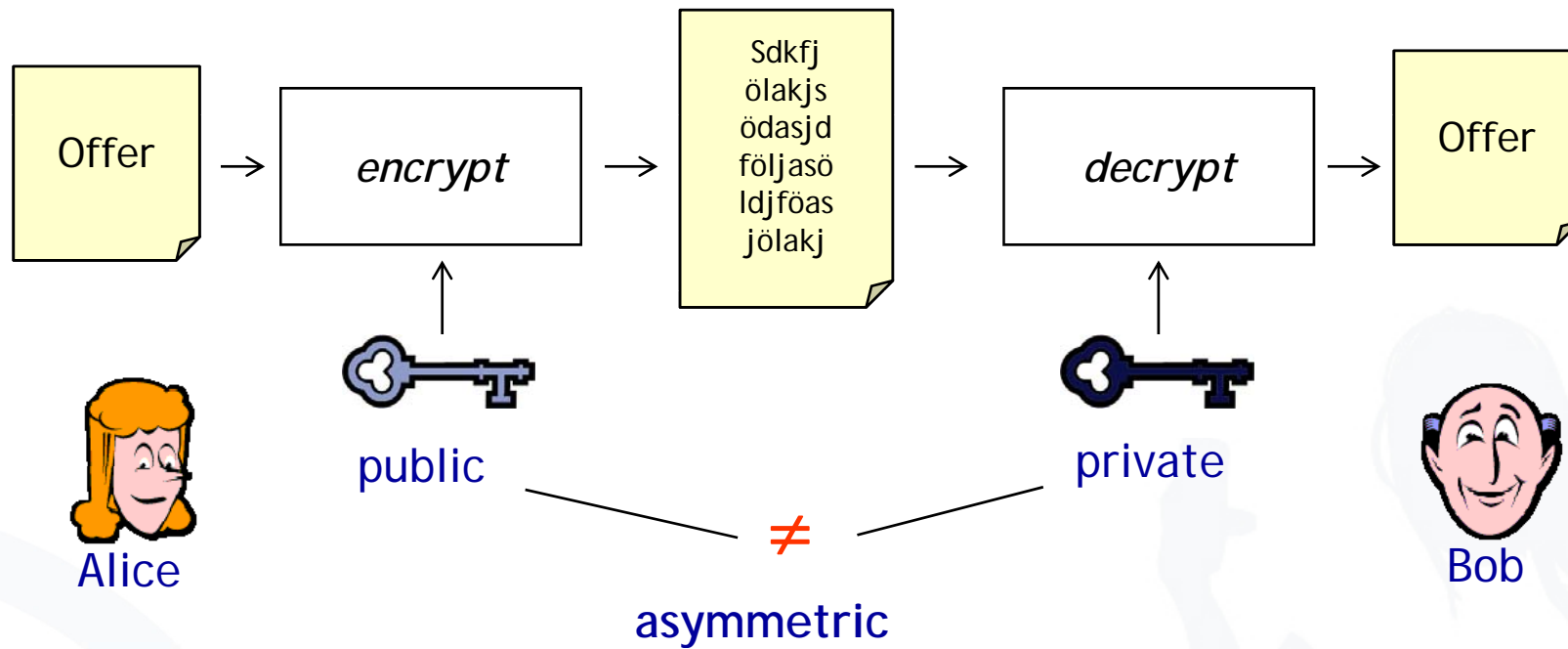
Algorithm	Performance*
RC6	138 ms
AES	173 ms
SERPENT	200 ms
IDEA	288 ms
MARS	394 ms
TWOFISH	697 ms
DES-edc	726 ms

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

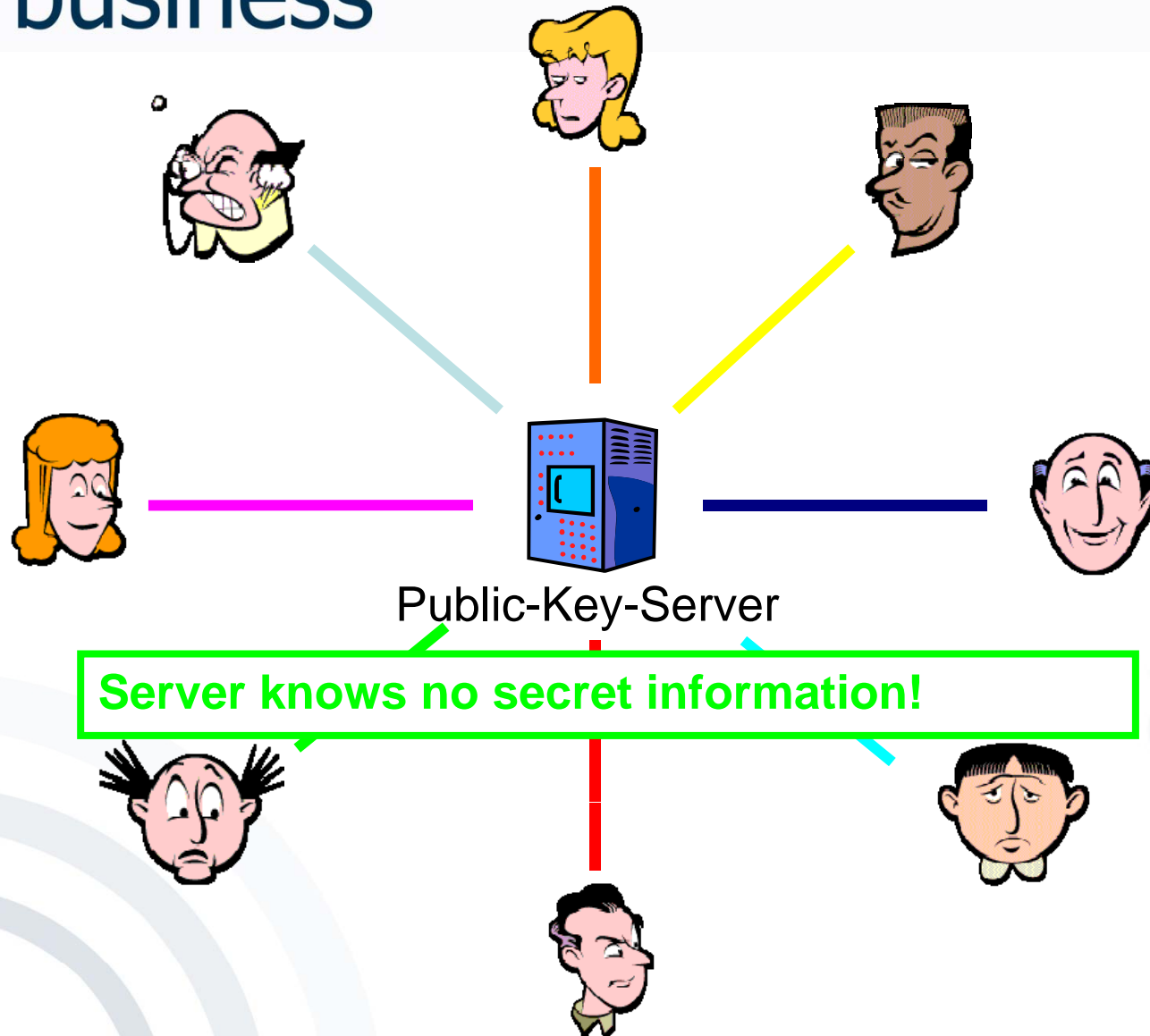




- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
  - General Concept
  - Algorithms
  - Hybrid Systems
  - Key Management
  - Example: PGP

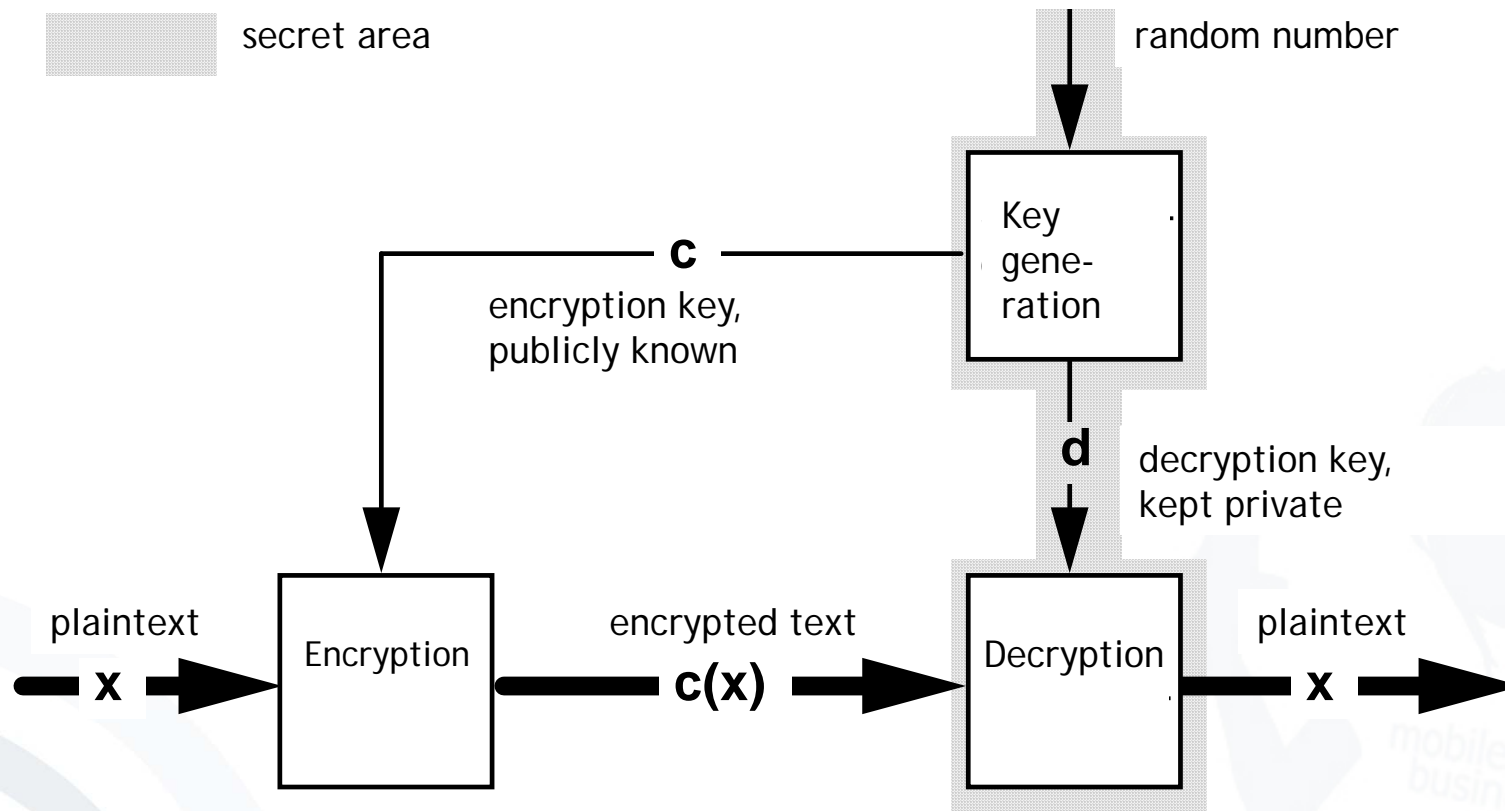


# Key Exchange Problem Solved!



- 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.
- Private key cannot be calculated from the public 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.



*box with slot, access to messages only with a key*

- 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 the public key)
- 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]

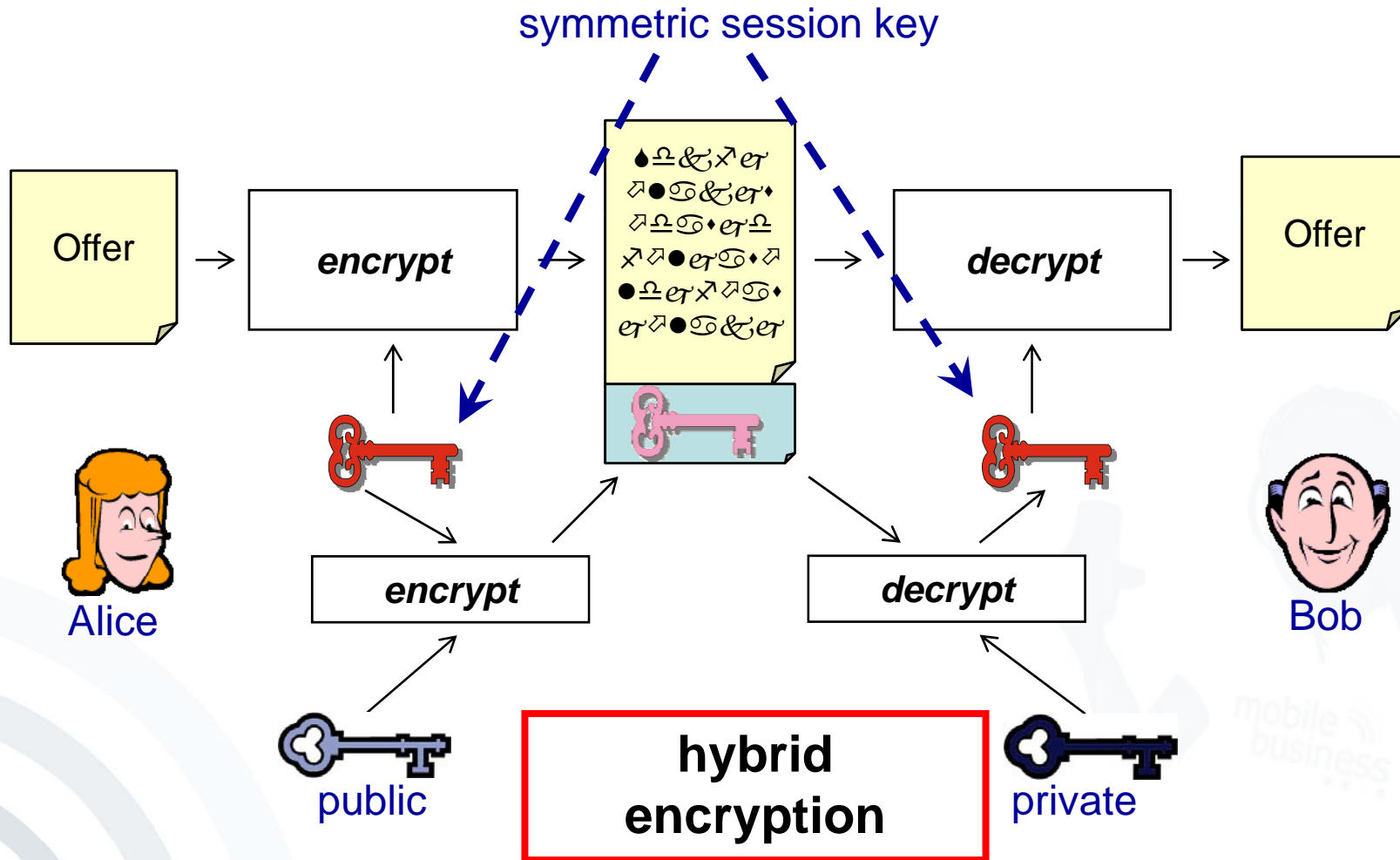
- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
  - General Concept
  - Algorithms
  - Hybrid Systems
  - Key Management
  - Example: PGP

Algorithm	Performance*
El Gamal	1826 s
RSA	16 s

**Disadvantage:** Complex operations  
with very big numbers

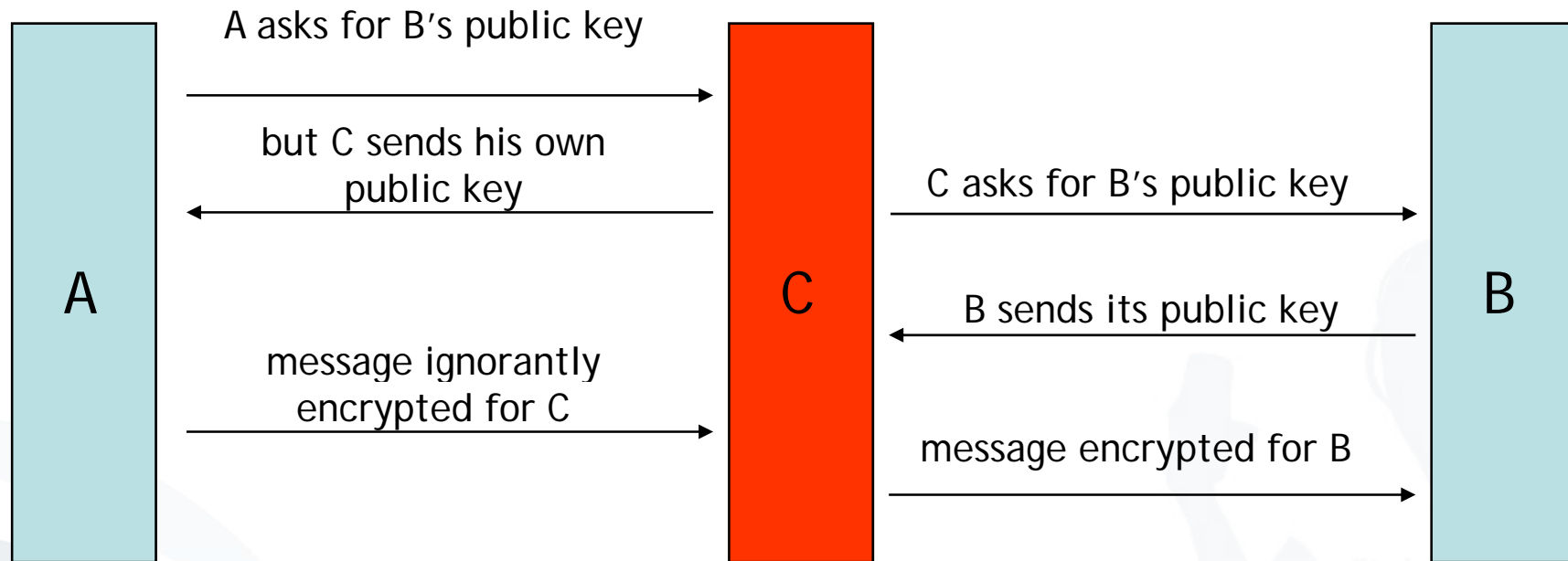
➔ **Algorithms are very slow**

\*) 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”



- ⇒ Keys are certified, that means a third person/institution confirms (with its digital signature) the affiliation of the public key to a person

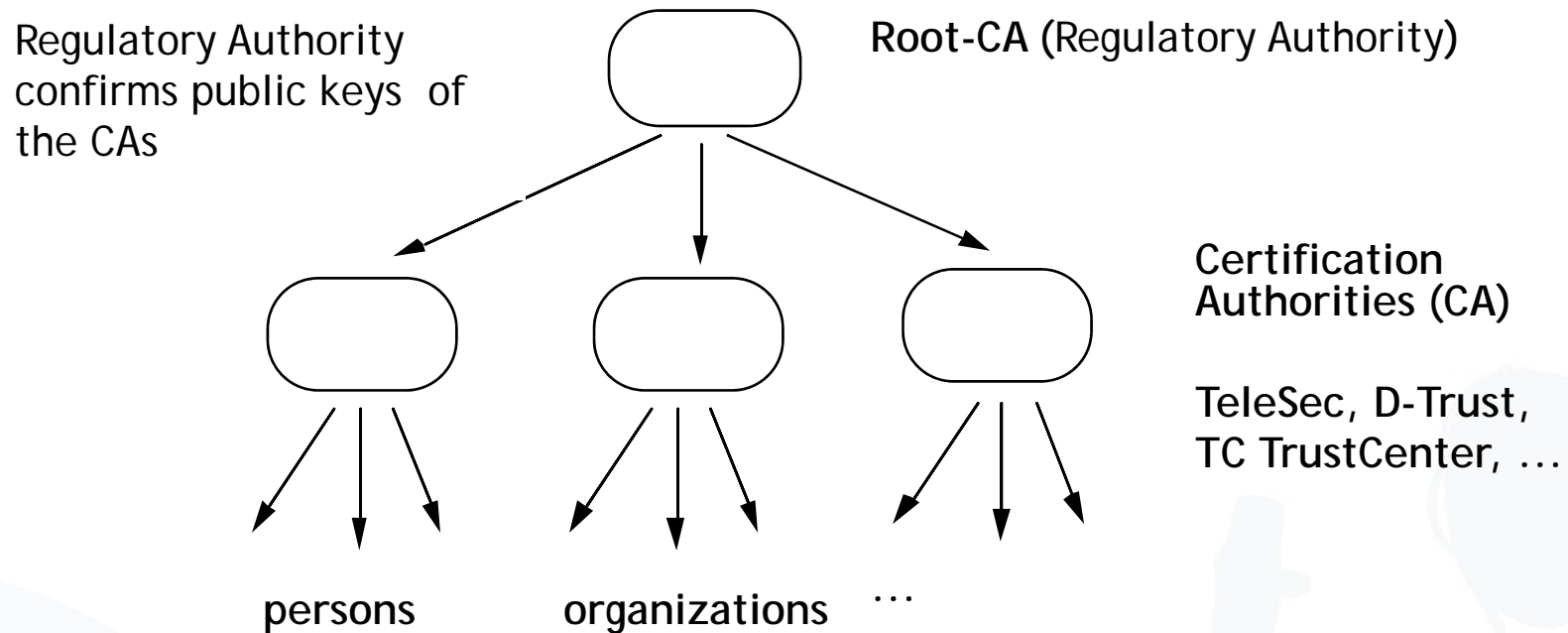
- B can freely distribute his own public key.
- But: Everybody (e.g. C) could distribute a public key and claim that this one belongs to B.
- If A uses this key to send a message to B, C will be able to read this message!
- Thus:  
How can A decide if a public key was really created and distributed by 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

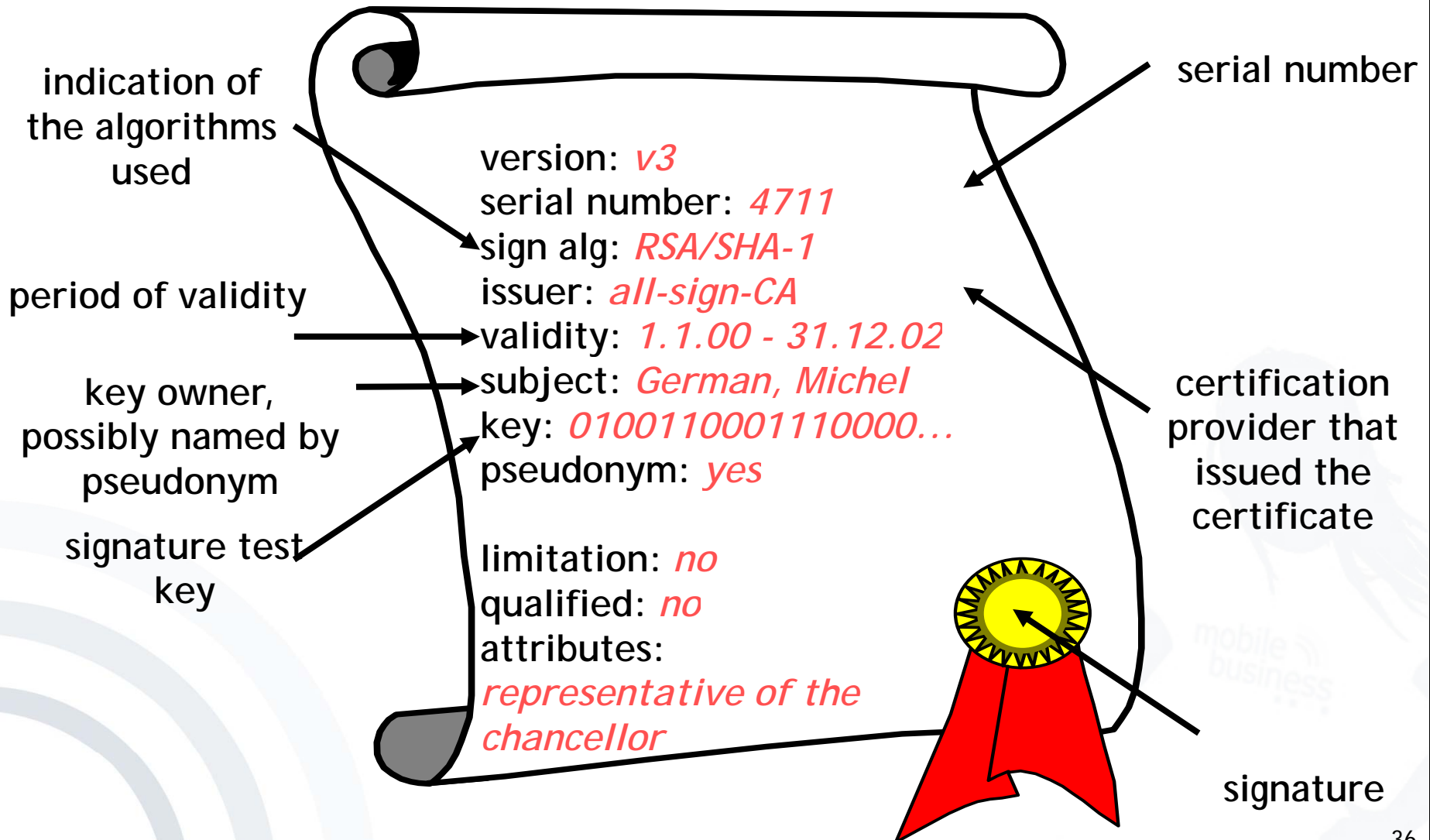
(Example: German Signature Law)



- 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.

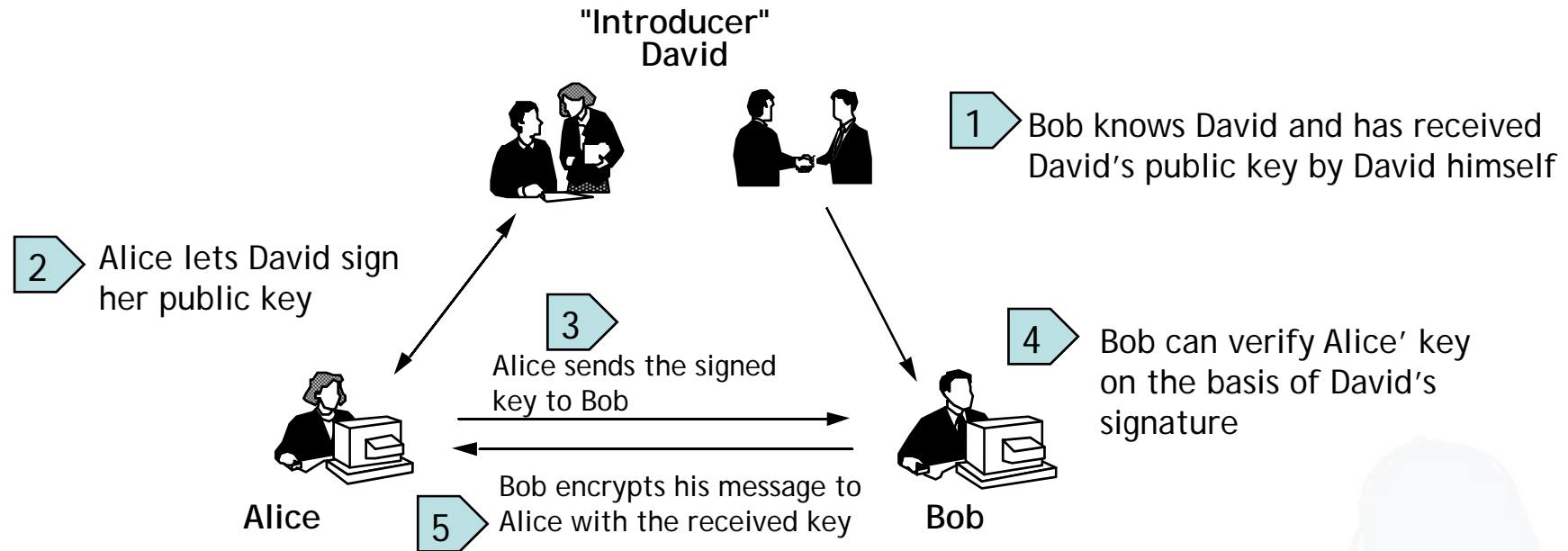
# Content of a Key Certificate

(according to German Signature Law and Regulation)



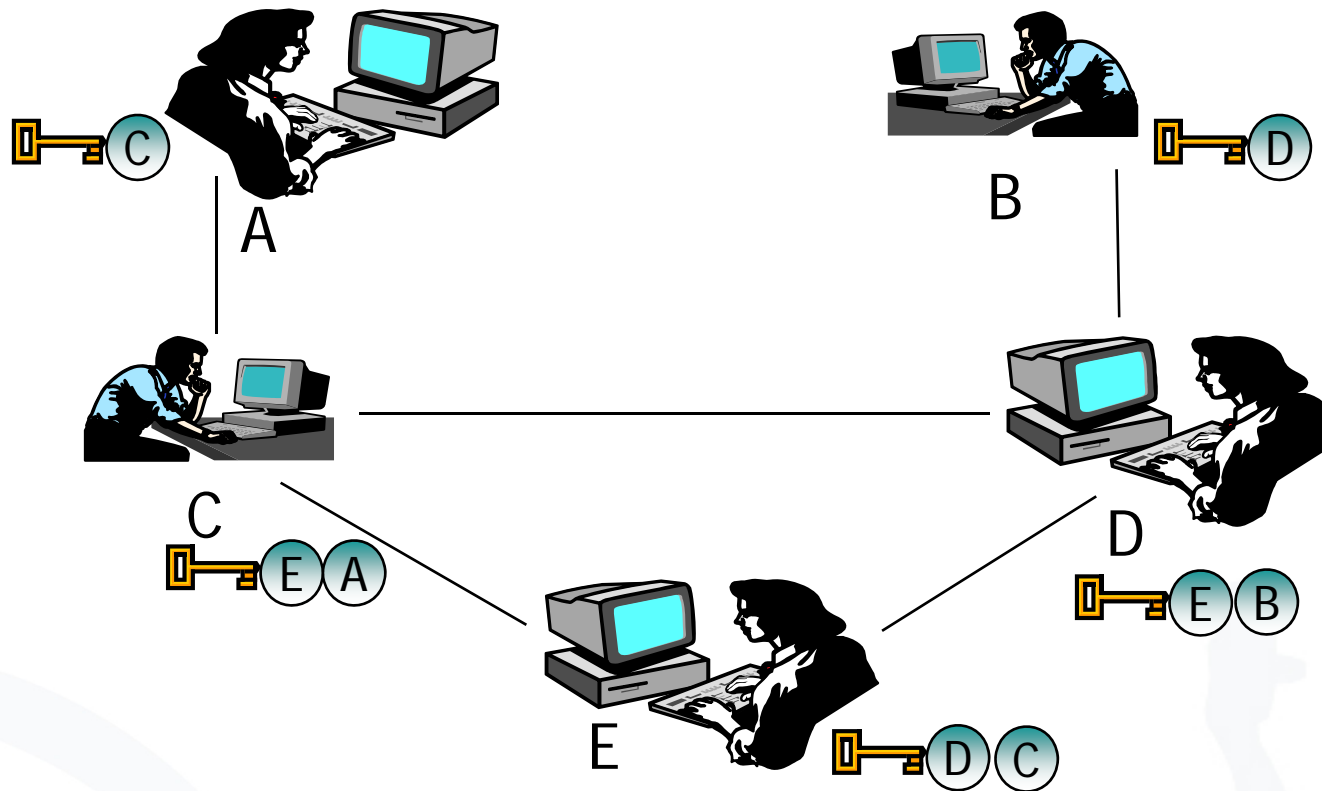
- Reliable identification of persons who apply for a certificate
- Information on necessary methods for fraud resistant creation of a signature
- Provision for secure storage of the private key
  - At least Smartcard (protected with PIN)
- Publication of the certificate (if wanted)
- Barring of certificates
- 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

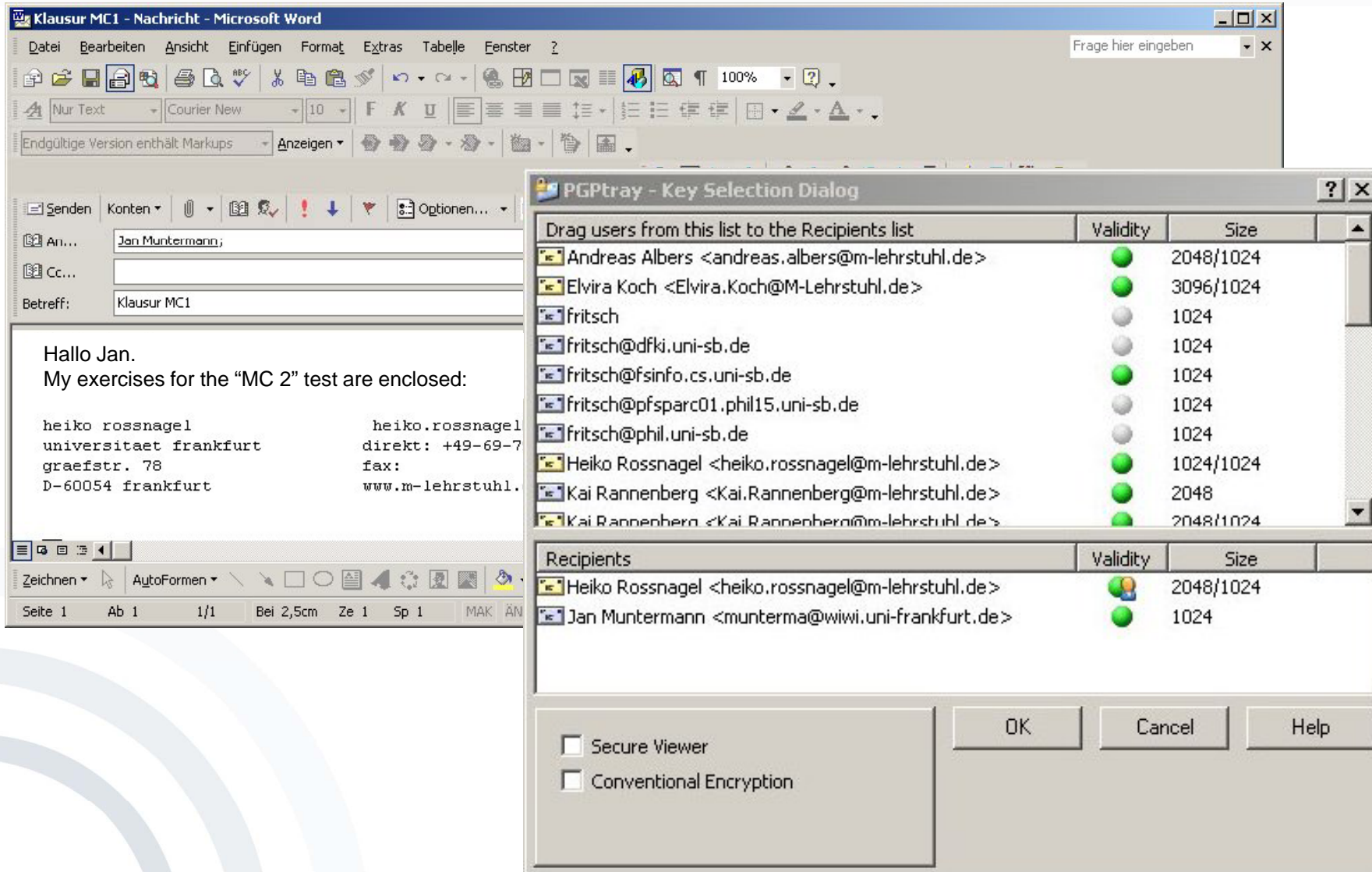


## Web of Trust:

- 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](http://www.pgp.com)
  - Gnu Privacy Guard (GPG): non-commercial Open Source variant (OpenPGP, RFC2440)



The screenshot shows a Microsoft Word window titled 'Klausur MC1 - Nachricht - Microsoft Word' with a PGP Key Selection Dialog box overlaid on top.

**Microsoft Word Content:**

Senden: Konten, Anhang, Optionen...

An...: Jan Muntermann;

Cc...:

Betreff: Klausur MC1

Hallo Jan.  
My exercises for the "MC 2" test are enclosed:

```

heiko rossnagel                heiko.rossnagel
universitaet frankfurt         direkt: +49-69-7
graefstr. 78                   fax:
D-60054 frankfurt              www.m-lehrstuhl.
    
```

**PGP Key Selection Dialog:**

Drag users from this list to the Recipients list

	Validity	Size
Andreas Albers <andreas.albers@m-lehrstuhl.de>	●	2048/1024
Elvira Koch <Elvira.Koch@M-Lehrstuhl.de>	●	3096/1024
fritsch	●	1024
fritsch@dfki.uni-sb.de	●	1024
fritsch@fsinfo.cs.uni-sb.de	●	1024
fritsch@pfsparc01.phil15.uni-sb.de	●	1024
fritsch@phil.uni-sb.de	●	1024
Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de>	●	1024/1024
Kai Rannenberg <Kai.Rannenberg@m-lehrstuhl.de>	●	2048
Kai Rannenberg <Kai.Rannenberg@m-lehrstuhl.de>	●	2048/1024

Recipients

	Validity	Size
Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de>	●	2048/1024
Jan Muntermann <munterm@wiwi.uni-frankfurt.de>	●	1024

Secure Viewer  
 Conventional Encryption

Buttons: OK, Cancel, Help

# OpenPGP: Encrypt Message

Verfassen: MB II Slides

Menü: Datei Bearbeiten Ansicht Einstellungen OpenPGP Extras Hilfe

Toolbar: Senden Kontakte Rechtschr. Anhang OpenPGP S/MIME Speichern

Von: Katja Liesebach <katja.liesebach@m-chair.net>

An: Christian Kahl <christian.kahl@m-lehrstuhl.de>

Betreff: MB II Slides

Hi Christian,

please find attached the MB II slides for lec...

--

Dipl.-Medien-Inf...

Johann Wolfgang  
Institute of Bus  
Chair of Mobile  
Graefstr. 78, D...

Internet: http://...  
Fon: +49 (69) 79...  
Fax: +49 (69) 79...

**OpenPGP-Schlüssel auswählen**

Nicht gefundene Empfänger

Empfänger für Verschlüsselung wählen

<input checked="" type="checkbox"/>	Benutzer-ID	Vertrauen	Ablauf...	Schlüssel-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"/>		-		C4495AF0
<input type="checkbox"/>		-		F7C207CE

Katja Liesebach <katja.liesebach@m-chair.net>

Katrin Borcea <kati@inf.tu-dresden.de>

Nachricht unverschlüsselt und nicht unterschrieben senden

Diesen Dialog nicht mehr anzeigen, wenn Verschlüsselung unmöglich ist

Liste aktualisieren Fehlende Schlüssel herunterladen

OK Abbrechen

**OpenPGP-Bestätigung**

VERSCHLÜSSELTE Nachricht an folgende Empfänger senden:

christian.kahl@m-lehrstuhl.de

Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:  
0x42B8B29914E21EDA, 0x23EE4D96C4495AF0

Ja Nein

# OpenPGP: Decrypt Message

**Betreff:** MB II Slides  
**Von:** [Katja Liesebach <katja.lieseback@m-chair.net>](mailto:katja.lieseback@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

hQEOAzxc3rSs71RREAQAoa4NK8beVOV:  
iEsWpmlxA11HIpTZtIKd9ecdjV1OFOJ:  
6xxXLtS6PkSb0k5nKkMZ1147F80IrvW  
/0md5jC1R8N/NJeuSfsW6w1LUpTVHQQ  
zQAvcf2AvjqHHw4UldKW8ewB3GG4zqD  
XxkOviAC+ADTcPgF5FvYPpbEiKS9D8dgzZrBd07YIfdH0oMBgga9  
JMwn2/s+Mn6AqNVhdPJuh8VaFvLW+up3GZ+msGd3v4P80Z1VBS4sc  
jOkaydJkxKqriLNqqiY39ltyZUtowlJaa+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.lieseback@m-chair.net>](mailto:katja.lieseback@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

**Von:** Heiko Rossnagel  
**Betreff:** Klausur MC1  
**An:** Jan Muntermann  
**Cc:**

-----BEGIN PGP MESSAGE-----  
Version: PGP 8.0 - not licensed for commercial use: [www.pgp.com](http://www.pgp.com)

hQCMA5/VPPIP3satAQP+LqxvxFSk4G/TAexpMLX436biwBp6xP8pa89R7ro5Xo  
uHEs07/tFrJFQJpPBcUWouy47p4sR2FO+IXqJuJyHp5ExMGIdmQCpGXEoS2Ijw  
B5TXKtUB8YJdpPnc61as78RBP1sq8VDrAlYopEAeqMMw2pkBuoxyo3KCiRkhi  
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n5+oafTBF+ROlv6UOz2TO55  
Alkh23iQ0LI9Drye/uygpcQpT2HhTtZYlAjjudLvi+GsegOlWmBjY8q8G1Y61C  
kDP3GEanyDiDU6R9F1XF0vxPNMk6Ek8hH6qZ37hhDNDcXkxksjM3nJ2VuuLvXb  
uOuXNA9iA96dhg7NpvzCJI2J7xRMtuBc9BUI8LXODrvGLwnLtaD5+EvgL1xTu  
dfvQ3NiGrUEQsOHVxwjQdMtr8C09kREYLuAdD7j/05WtsAdbAVMn72PYFOIRfZ  
i77MitBfAbxXF0gFS7/b2LccbaK8fx6e1VNFnVO7B/9qpdOGg5WZVP2eQA5fbw  
h2oTOSjWCRp/v5s9Og1aUtcAxd1RAjQPHpVsFS2eXXMn9ZzvNIFMh6Ktqnt6E  
m39jRjPE9Ob/HLjMwPAXUHyneh9QrCX1X5qHORNcjIYVrnQyZGIk8t39059FBd  
cr1rhf6ht7SwGgfgGW2aL8HyiFEVRC6piJaJFmrzifnzliwfuf82Tc42GBd9bP  
E1IJGt9QLiwMmXormxcOg+WR2Ix4nGFX17Hy1vjKqpn7gfyLxXjgeDCnjxm708J  
NjwR+1SkqMCXs+PzcAHDsiuG  
pE3huhK5cfvu1Ug7+Oa9SUay4  
NZncI3vJgkZeZr1bh+pi4dRjs  
=hCO9  
-----END PGP MESSAGE-----

heiko rossnagel  
frankfurt direkt  
-25306 D-60054 frankfurt

PGPTray - Enter Passphrase

Message was encrypted to the following public key(s):

- Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de> (DH/2048)
- Jan Muntermann <munterma@wiwi.uni-frankfurt.de> (RSA/1024)

Enter passphrase for your private key:  Hide Typing

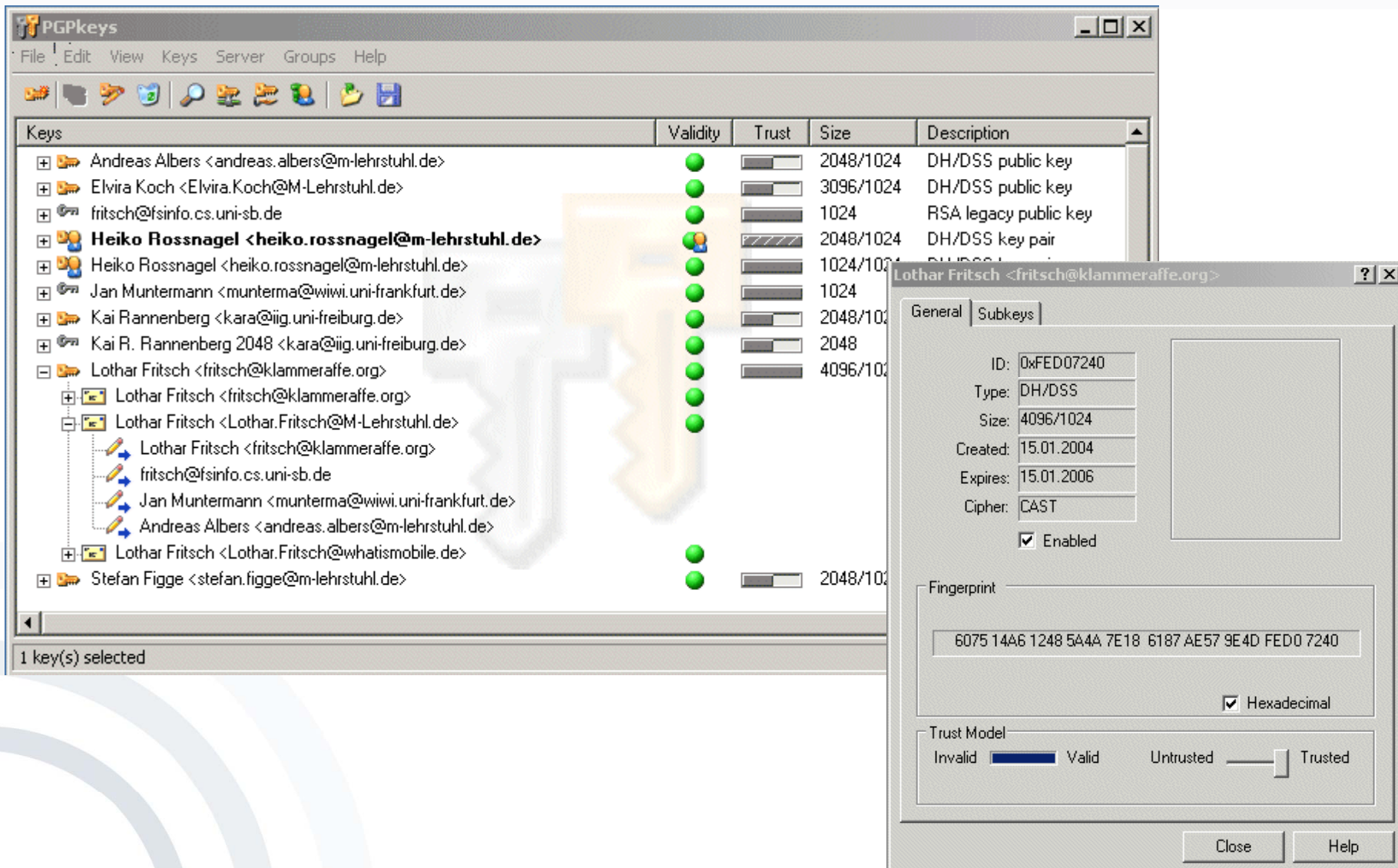
OK Cancel

Text Viewer

Hallo Jan.  
My exercises for the "MC 2" test are enclosed:

Copy to Clipboard OK

- 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

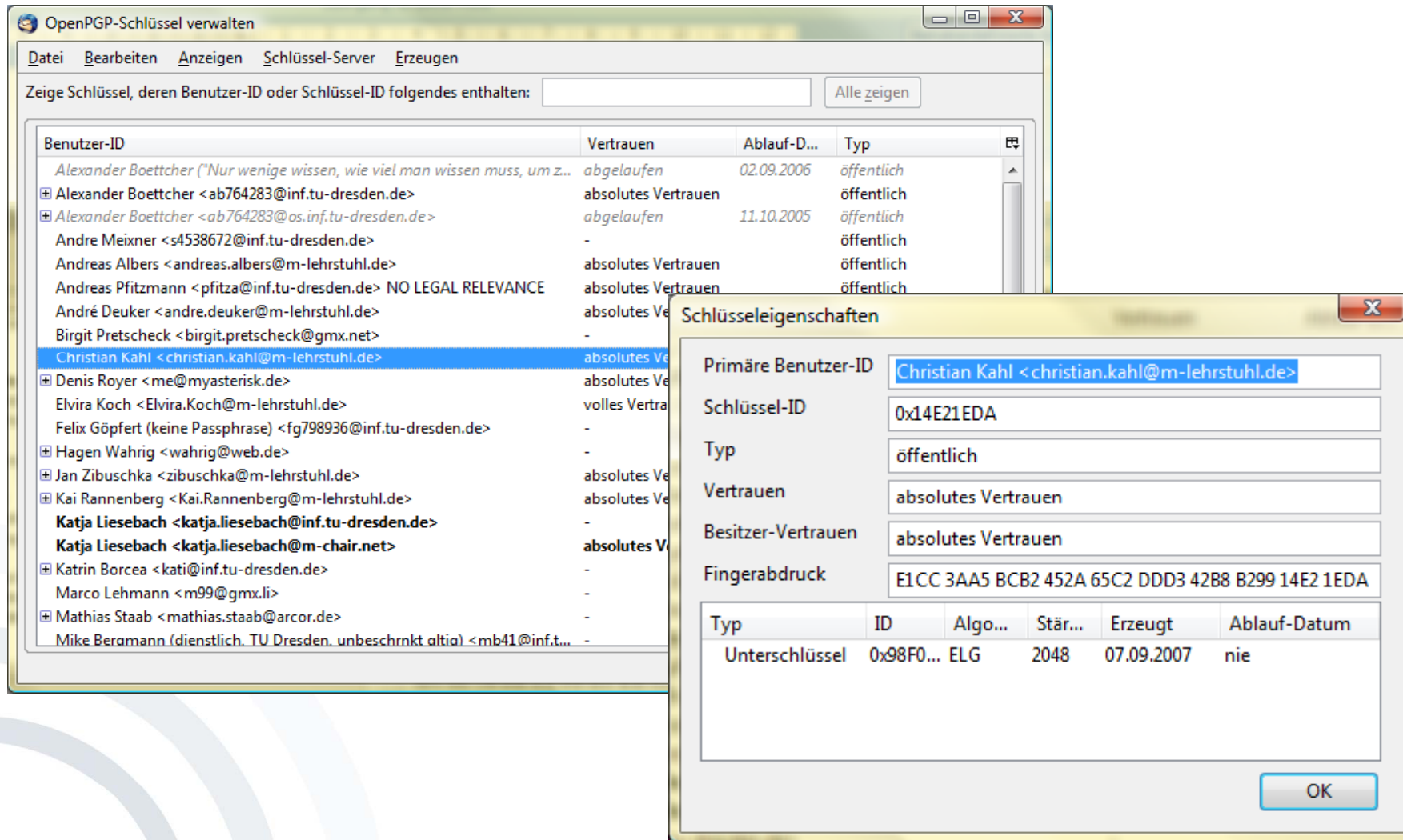


The screenshot shows the PGPkeys application window. The main window displays a list of keys with columns for Validity, Trust, Size, and Description. A key for Lothar Fritsch is selected, and a detailed dialog box is open for it.

Keys	Validity	Trust	Size	Description
Andreas Albers <andreas.albers@m-lehrstuhl.de>	●	▬	2048/1024	DH/DSS public key
Elvira Koch <Elvira.Koch@M-Lehrstuhl.de>	●	▬	3096/1024	DH/DSS public key
fritsch@fsinfo.cs.uni-sb.de	●	▬	1024	RSA legacy public key
<b>Heiko Rossnagel &lt;heiko.rossnagel@m-lehrstuhl.de&gt;</b>	●	▬	2048/1024	DH/DSS key pair
Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de>	●	▬	1024/1024	DH/DSS public key
Jan Muntermann <munterma@wiwi.uni-frankfurt.de>	●	▬	1024	RSA legacy public key
Kai Rannenber <kara@iig.uni-freiburg.de>	●	▬	2048/1024	DH/DSS public key
Kai R. Rannenber 2048 <kara@iig.uni-freiburg.de>	●	▬	2048	RSA legacy public key
Lothar Fritsch <fritsch@klammeraffe.org>	●	▬	4096/1024	DH/DSS key pair
Lothar Fritsch <fritsch@klammeraffe.org>	●	▬	4096/1024	DH/DSS key pair
Lothar Fritsch <Lothar.Fritsch@M-Lehrstuhl.de>	●	▬	4096/1024	DH/DSS key pair
Lothar Fritsch <fritsch@fsinfo.cs.uni-sb.de>	●	▬	1024	RSA legacy public key
Jan Muntermann <munterma@wiwi.uni-frankfurt.de>	●	▬	1024	RSA legacy public key
Andreas Albers <andreas.albers@m-lehrstuhl.de>	●	▬	2048/1024	DH/DSS public key
Lothar Fritsch <Lothar.Fritsch@whatismobile.de>	●	▬	2048/1024	DH/DSS public key
Stefan Figge <stefan.figge@m-lehrstuhl.de>	●	▬	2048/1024	DH/DSS public key

**Lothar Fritsch <fritsch@klammeraffe.org>** Key Details:

- General Tab:
  - ID: 0xFED07240
  - Type: DH/DSS
  - Size: 4096/1024
  - Created: 15.01.2004
  - Expires: 15.01.2006
  - Cipher: CAST
  - Enabled
- Subkeys Tab:
  - Fingerprint: 6075 14A6 1248 5A4A 7E18 6187 AE57 9E4D FED0 7240
  - Hexadecimal
- Trust Model:
  - Invalid  Valid  Untrusted  Trusted



The screenshot shows the 'OpenPGP-Schlüssel verwalten' window. The main window displays a list of keys with columns for 'Benutzer-ID', 'Vertrauen', 'Ablauf-D...', and 'Typ'. A search bar at the top allows filtering by user ID or key ID. The 'Schlüsseleigenschaften' dialog box is open, showing details for a key owned by 'Christian Kahl <christian.kahl@m-lehrstuhl.de>'. The dialog includes fields for 'Primäre Benutzer-ID', 'Schlüssel-ID', 'Typ', 'Vertrauen', 'Besitzer-Vertrauen', and 'Fingerabdruck'. Below these fields is a table of subkeys.

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 Rannenberg <Kai.Rannenberg@m-lehrstuhl.de>	absolutes Ve		
<b>Katja Liesebach &lt;katja.liesebach@inf.tu-dresden.de&gt;</b>	-		
<b>Katja Liesebach &lt;katja.liesebach@m-chair.net&gt;</b>	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	Christian Kahl <christian.kahl@m-lehrstuhl.de>				
Schlüssel-ID	0x14E21EDA				
Typ	öffentlich				
Vertrauen	absolutes Vertrauen				
Besitzer-Vertrauen	absolutes Vertrauen				
Fingerabdruck	E1CC 3AA5 BCB2 452A 65C2 DDD3 42B8 B299 14E2 1EDA				
Typ	ID	Algo...	Stär...	Erzeugt	Ablauf-Datum
Unterschlüssel	0x98F0...	ELG	2048	07.09.2007	nie

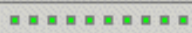
PGPkeys Search Window

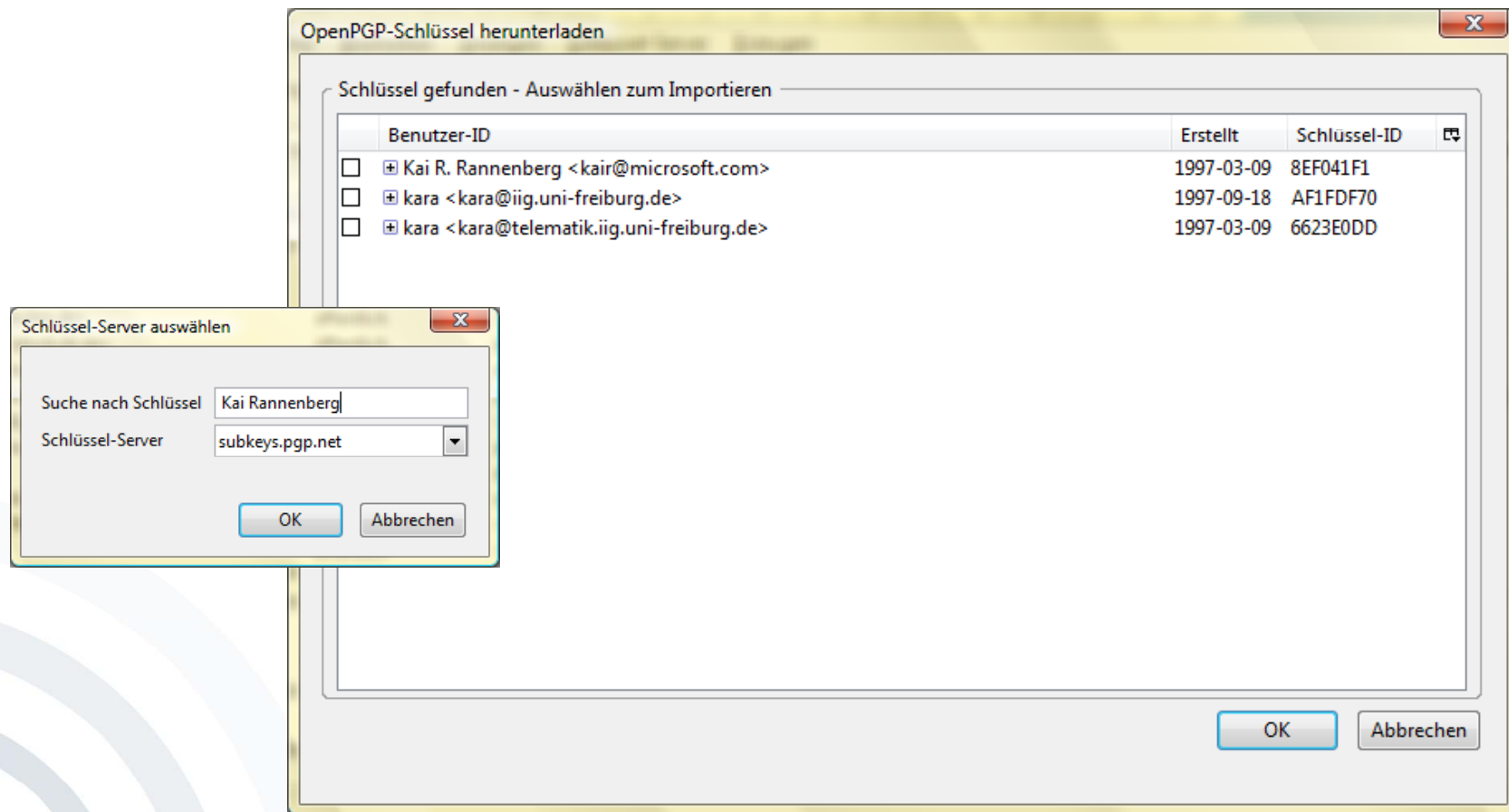
Search for keys on  where

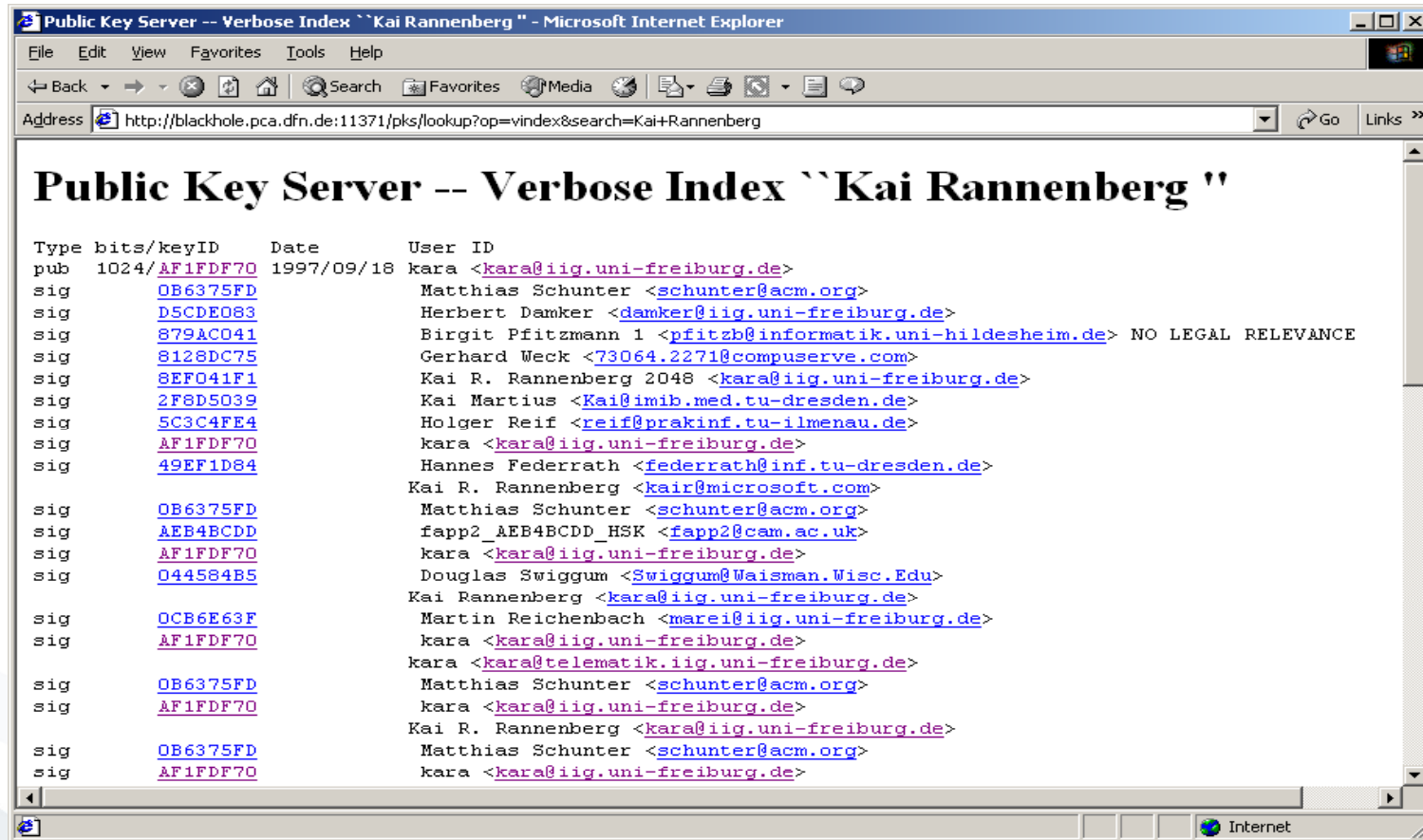
User ID

Search Pending Area

Keys	Validity	Trust	Size	Description
<input type="checkbox"/>  Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de>		<input type="text" value=""/>	2048	RSA legacy public key
<input type="checkbox"/>  Kai R. Rannenberg <kara@iig.uni-freiburg.de>		<input type="text" value=""/>	1024	RSA legacy public key
<input type="checkbox"/>  kara <kara@iig.uni-freiburg.de>		<input type="text" value=""/>	2048/1024	DH/DSS public key







- Network of public-key-servers:  
[www.pca.dfn.de/eng/dfnpca/pgpkserv](http://www.pca.dfn.de/eng/dfnpca/pgpkserv)  
[www.openpgp.net/pgpsrv.html](http://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](http://www.gaudior.net/alma/johnny.pdf)