

Lecture 4

Cryptography



Mobile Business II (SS 2021)

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security Goethe University Frankfurt a. M.



Introduction

- Symmetric Cryptosystems
- Public Key Cryptography





Cryptographic Systems

- 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

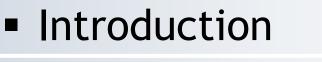
- Advantages and Problems
- Public Key Cryptography



Symmetric Encryption Systems

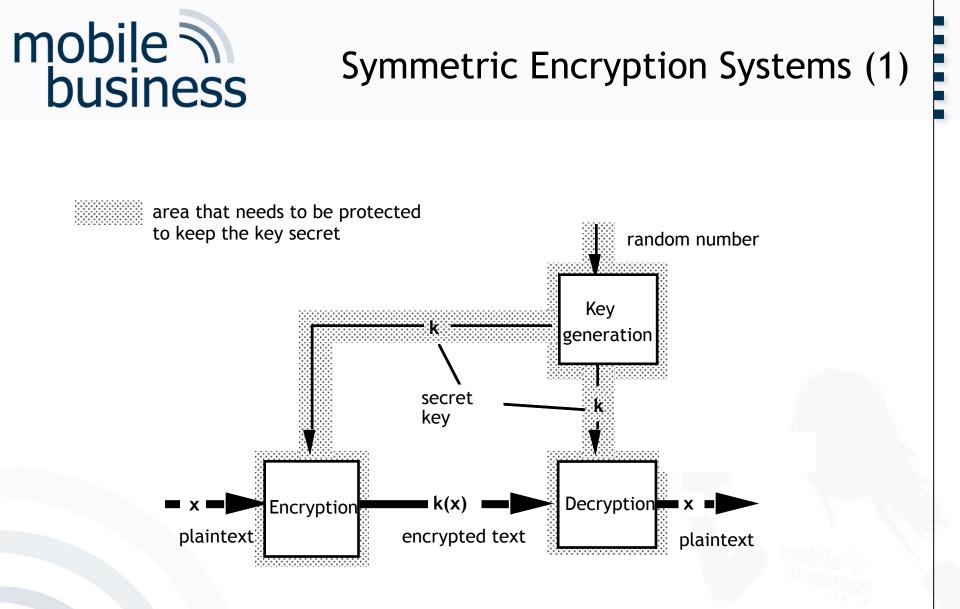
- Typical applications
 - confidential storage of user data
 - transfer of data between 2 users who negotiate a key via a secure channel
 - end-to-end channel encryption
- Examples
 - Vernam-Code (one-time pad, Gilbert Vernam)
 - key length = length of the plaintext (information theoretically secure)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





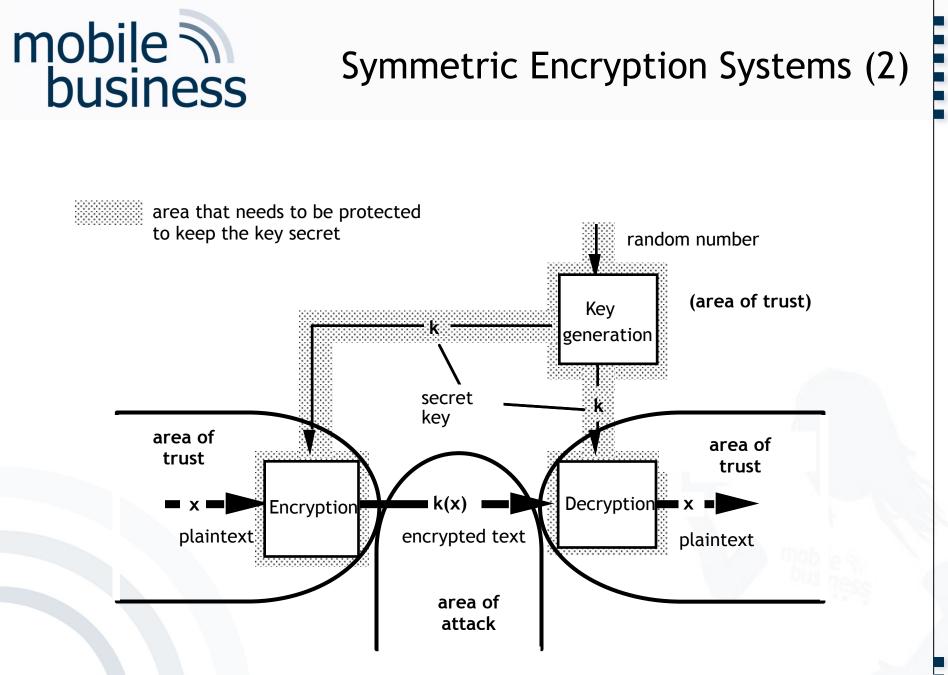
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES

- Advantages and Problems
- Public Key Cryptography



black box with lock, two equal keys

[based on Federrath and Pfitzmann 1997]



[based on Federrath and Pfitzmann 1997]



- Keys have to be kept secret (secret key crypto system).
- It must not be possible to derive the plaintext or the used keys 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.
- Security of cryptosystems should base on the strength of chosen key lengths.

10

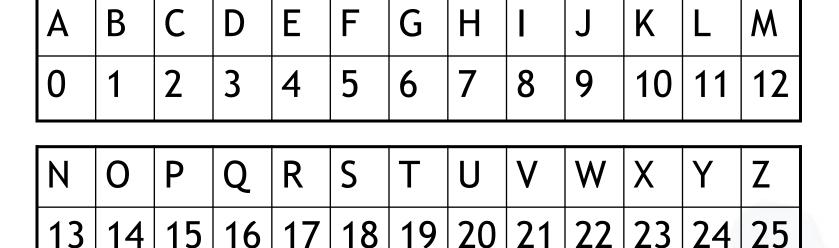
Agenda

Introduction

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



Caesar Cipher



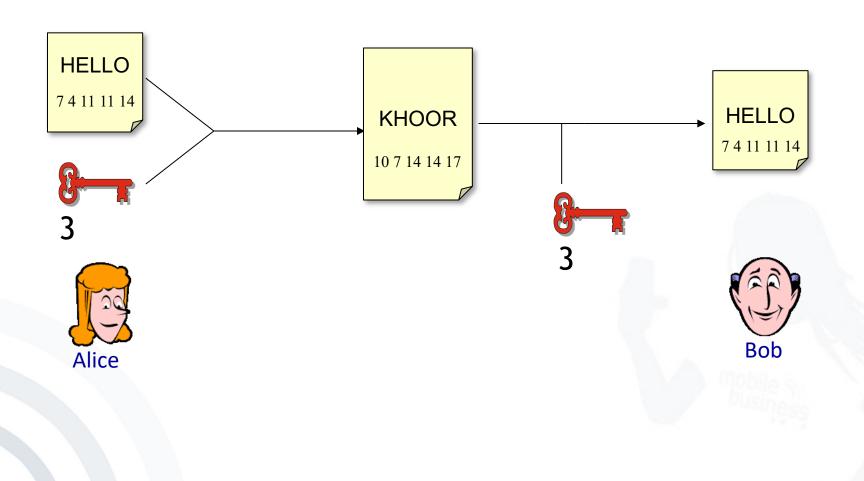
- We assign a number for every character.
- This enables us to calculate with letters as if they were numbers.







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.



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

[Bishop 2005]

16

Agenda

Introduction

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





Symmetric Encryption



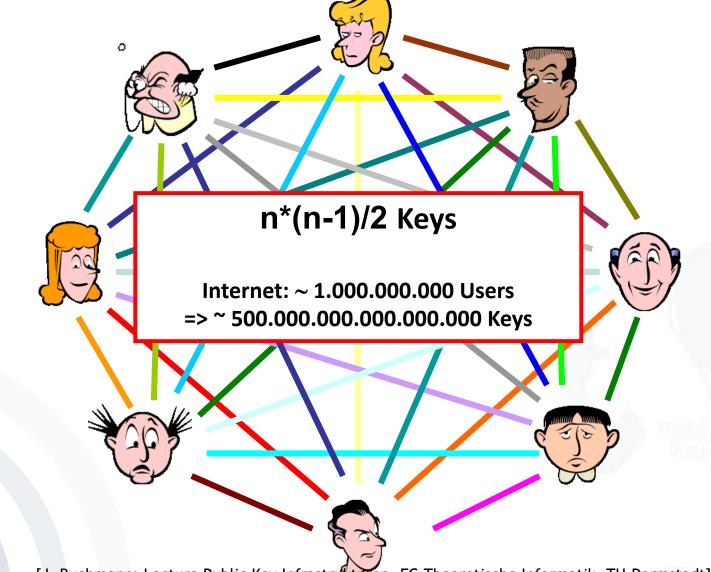
Advantage: Algorithms are very fast

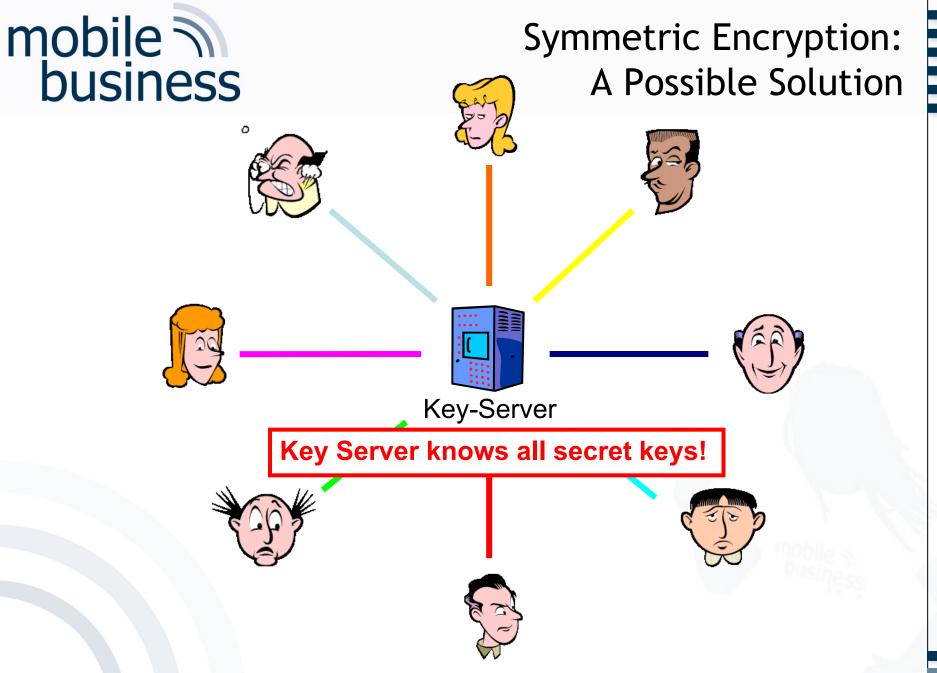
| Algorithm | Performance* |
|----------------|--------------|
| RC6 | 78 ms |
| SERPENT | 95 ms |
| IDEA | 170 ms |
| MARS | 80 ms |
| TWOFISH | 100 ms |
| DES-ede | 250 ms |
| RIJNDEAL (AES) | 65 ms |

* Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider Java)

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

Problems of Symmetric Cryptosystems: Key Exchange





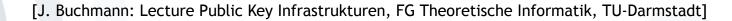
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]



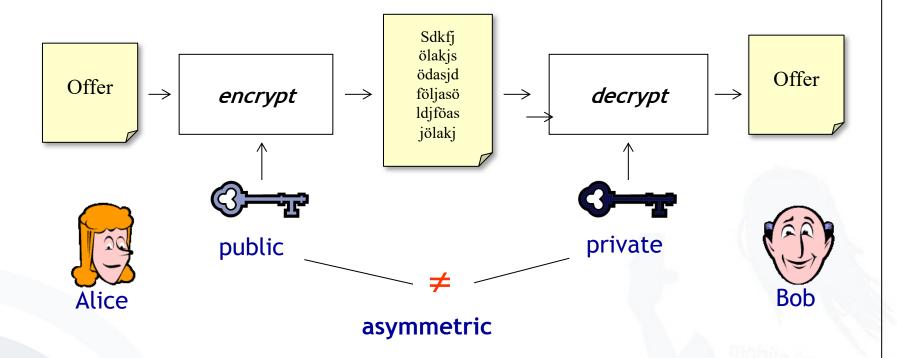
Introduction

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

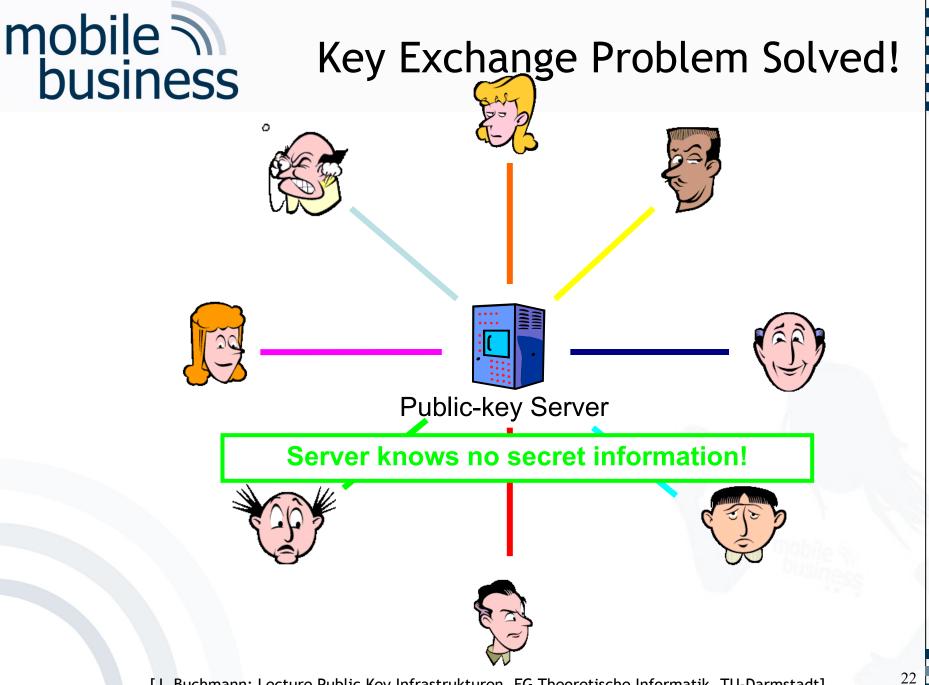




Public Key Encryption







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



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

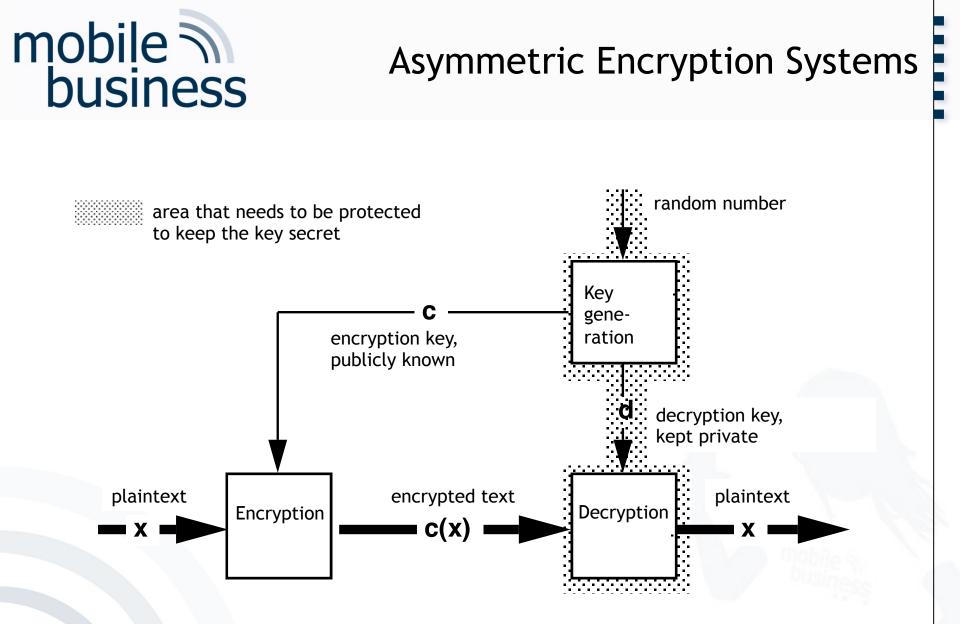






Concept of Asymmetric Encryption Systems

- Use of 'corresponding' key pairs instead of one key:
 - **Public key** is **solely** for encryption.
 - Encrypted text can only be decrypted with the corresponding private (undisclosed) key.
- Deriving the private key from the public key is hard (practically impossible).
- The public key can be distributed freely, even via insecure ways (e.g. directory (public key crypto system)).
- Messages are encrypted via the public key of the addressee.
- Only the addressee possesses the private key for decoding (and has to manage the relation between the private and the public key).



box with slot, access to messages only with a key



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



Asymmetric Encryption Systems: Examples

RSA

- Rivest, Shamir, Adleman, 1978
- is based on the assumption that the factorization of the product of two (big) prime numbers (p*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
 - Digital Signature
 - Key Management
 - Example: PGP





Performance of Public Key Algorithms

| Algorithm | Performance* Performance compared to Symmetric encryption (AES) | |
|-----------------|--|-------------------|
| RSA (1024 bits) | 6.6 s | Factor 100 slower |
| RSA (2048 bits) | 11.8 s | Factor 180 slower |

Disadvantage: Complex operations with very big numbers

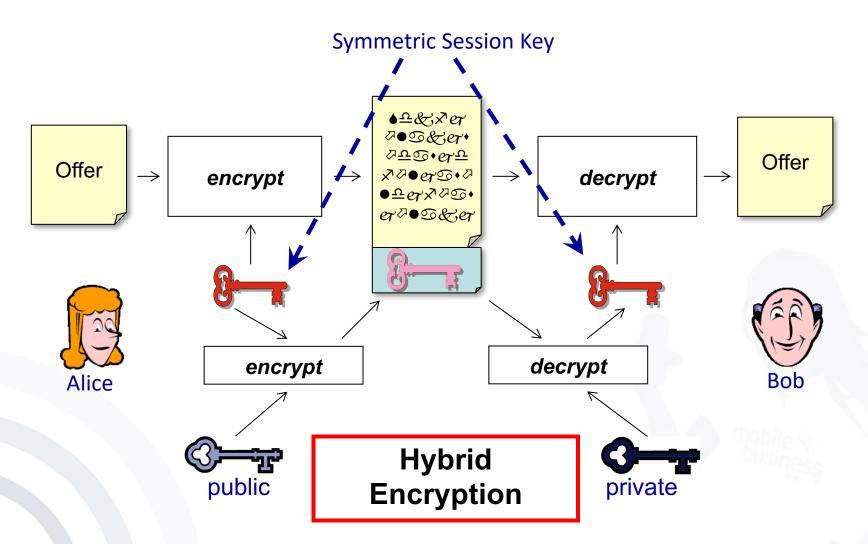
 \Rightarrow Algorithms are very slow.

* Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider (Java)

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



Solution: Hybrid Systems



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





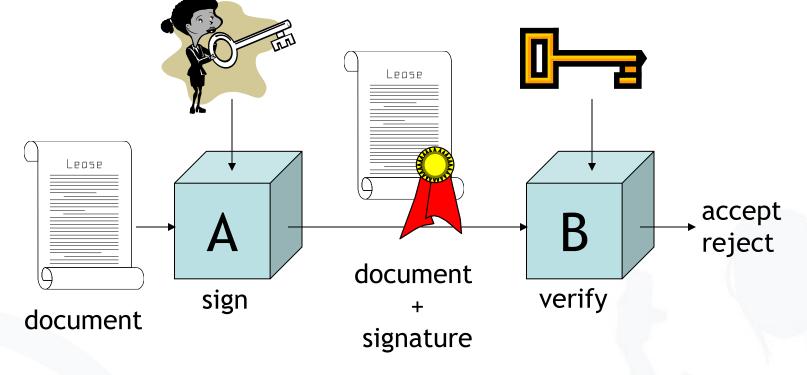
Introduction

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

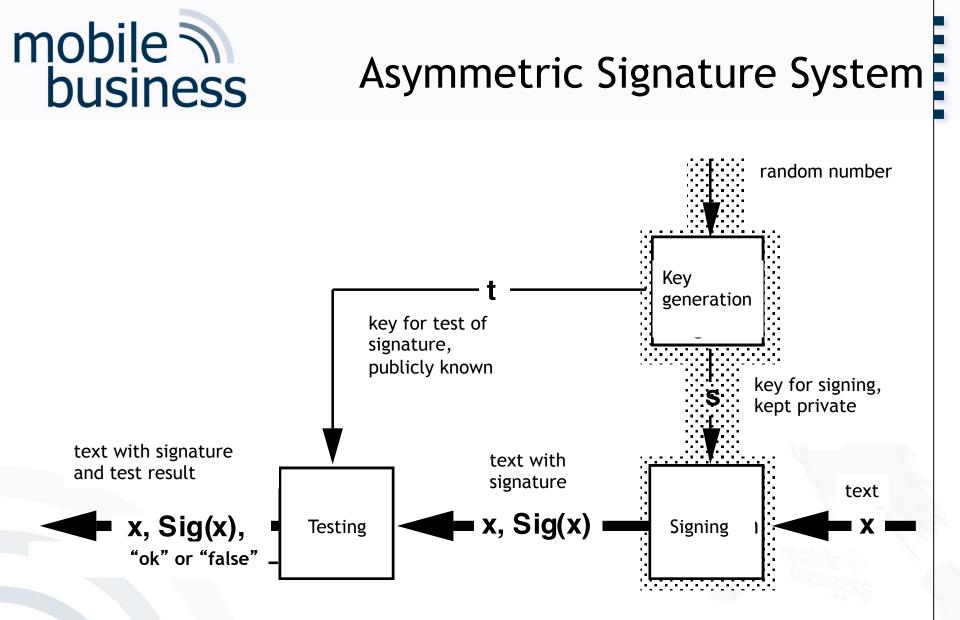
Digital Signatures

Protect the authenticity and integrity of documents signed by A

 \bigcirc B has to get an authentic copy of A' s public key.







Iocked glass show-case; just one key to put something in

Example PGP: Encrypt and Sign a Message

| 🖳 Klau | sur MC1 - Nachricht - Microsoft Word | | | _ 🗆 × | 1 | | |
|---------------|--|---|----------------------|----------|-------------------|------------|--|
| <u>D</u> atei | | | Frage hier eingeben | • • × | | | |
| 1 | ۶ 🖬 🛍 🎒 🕼 🖤 👗 🛍 🛍 🚿 🗠 • • • • • 🥵 🗗 🗔 💷 👪 🐼 | | | | | | |
| - <u>4</u> N | ur Text → Courier New → 10 → F K 및 = = = = ‡= → = + | ∉∉∣ ⊞・<u>⊿</u>・<u>A</u>・. | | | | | |
| Endgül | tige Version enthält Markups 🔹 Anzeigen 🔹 🌚 🌚 🖓 🔸 🌚 🔹 🏙 🗸 🦉 | 😕 PGPtray - Key Selection Dialog | | | | <u>?</u> × | |
| | nden Konten • 🕕 • 📴 🎭 🕴 🌲 🧡 🚼 O <u>p</u> tionen • Nur-Text • | Drag users from this list to the Recipients | | Validity | Size | | |
| 1 | | Andreas Albers <andreas.albers@m-le< td=""><td></td><td>•</td><td>2048/1024</td><td></td></andreas.albers@m-le<> | | • | 2048/1024 | | |
| 🔛 An | | Elvira Koch <elvira.koch@m-lehrstuhl.< td=""><td>de></td><td>•</td><td>3096/1024</td><td></td></elvira.koch@m-lehrstuhl.<> | de> | • | 3096/1024 | | |
| Cc 🛙 | | 📧 fritsch | | | 1024 | | |
| Betrefi | : Klausur MC1 | Fritsch@dfki.uni-sb.de | | | 1024 | | |
| | | Fritsch@fsinfo.cs.uni-sb.de | | • | 1024 | | |
| | allo Jan. y exercises for the "MC 2" test are enclosed: | Fritsch@pfsparc01.phil15.uni-sb.de | | 9 | 1024 | | |
| | y exercises for the Mic 2 test are enclosed. | Fritsch@phil.uni-sb.de | la hanaka hili ala s | - | 1024 | | |
| | iko rossnagel heiko.rossnagel@m-lehrstuhl.de | Heiko Rossnagel <heiko.rossnagel@m- Kai Rannenberg <kai.rannenberg@m-< p=""></kai.rannenberg@m-<></heiko.rossnagel@m- | | | 1024/1024 2048 | | |
| | iversitaet frankfurt direkt: +49-69-798-25309 aefstr. 78 fax: -25306 | Kai Rannenberg <kai rannenberg@m-<="" td=""><td></td><td></td><td>2040 2048/1024</td><td>-</td></kai> | | | 2040 2048/1024 | - | |
| - | 60054 frankfurt www.m-lehrstuhl.de | | | | 1 | | |
| | | ? × ossnagel@m- | المعاملة المعامل | Validity | Size 2048/1024 | | |
| | PGPtray - Enter Passphrase | | | | 1024 | | |
| Ξ | Trma@wiwi.uni-frankfurt.de> 🔵 1024 | | | | | | |
| Se | se Signing key : Heiko Rossnagel <heiko.rossnagel@m-lehrst (dss="" 1024="" td="" 💌<=""></heiko.rossnagel@m-lehrst> | | | | | | |
| | Enter passphrase for above key: 🔽 Hide Typing OK Cancel Help | | | | | Help | |
| - | | | | J | | | |
| | | p n | | | | | |
| | | | | | | | |
| | , | | | | | | |
| | | | | | | | |
| | OK | Cancel | | | | | |
| | | | | | | | |
| | | | | | | 34 | |

Example PGP: Decrypt and Check a Message

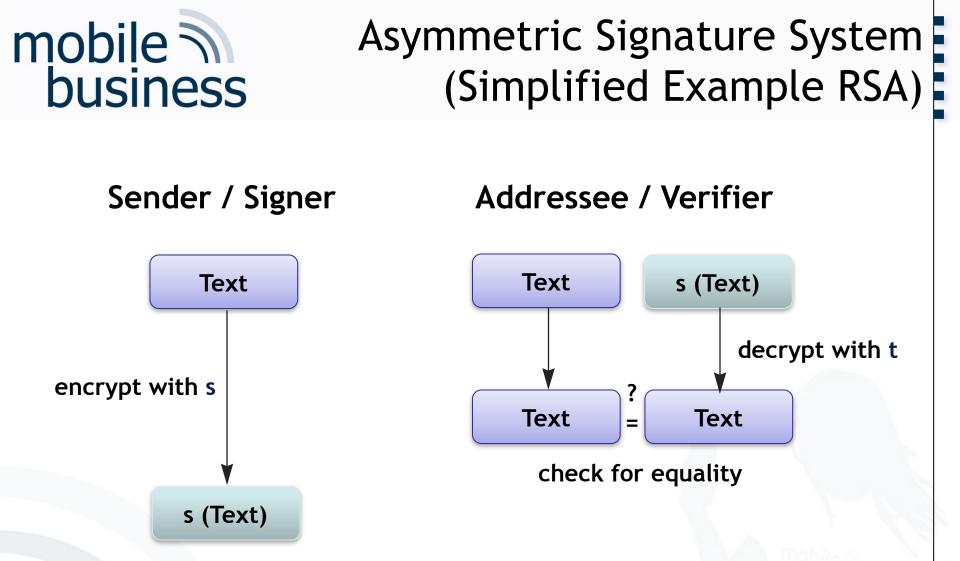
| Von: Heiko Rossnagel | An: Jan Mu | ntermann | | | |
|---|---|---|--|--|--|
| Betreff: Klausur MC1 | Cc: | PGPtray - Enter Passphrase 🛛 🤶 🗙 | | | |
| BEGIN PGP MESSAGE | - | Message was encrypted to the following public key(s) : | | | |
| Version: PGP 8.0 - not lice | ensed for commercial use: www.pgp | | | | |
| | | Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de> (DH/2048)</heiko.rossnagel@m-lehrstuhl.de> | | | |
| hQCMA5/VPPIP3satAQP+LqxvxF | 5k4G/TAexpMLX436biwBp6xP8pa89R7ro! | Jan Muntermann <munterma@wiwi.uni-frankfurt.de> (RSA/1024)</munterma@wiwi.uni-frankfurt.de> | | | |
| uHEs07/tFrJFQJpPBcUWouy47p4 | 4sR2F0+IXqJuJyHp5ExMGIdmQCpGXEoS2) | | | | |
| B5TXKtUB8YJdpPnck61as78RBP: | 1sq8VDrAlYopEAeqMMw2pkBuoxyo3KCiR] | | | | |
| Ag4DIYlowhVX6ZwQCAD2L9WAA9 | 7xEUBWMET6kR9n5+oafTBF+R01v6UOz2T(| | | | |
| Alkh23iQO1I9Drye/uygpcQpT21 | HhTtZYlAjjudLvi+GsegOlWmBjY8q8G1Y(| Enter passphrase for your private key : 🔽 Hide Typing | | | |
| kDP3GEanyDiDU6R9F1XFOvxPNM | k6Ek8hH6qZ37hhDNDCXkxkSjM3nJ2VuuL | | | | |
| uOuXNA9iAC96dhg7NpvzCJI2J7: | xRMtuBc9BUI8LXODrvGLwnLtaD5+EvgL1; | | | | |
| dfvQ3NiGrUEQsOHVxwjQdMtr8C(| D9kREYLuAdD7j/05WtsAdbAVMn72PYF0I | | | | |
| i77MitBfAbxXF0gFS7/b2Lccbal | K8fx6e1VNFnV07B/9qpd0Gg5WZVP2eQA5: | | | | |
| h2oTOSjWCRp/v5s9Og1aUtcAxd. | lRAjQPHpVsFS2eXXMnC9ZZvNIFMh6Ktqm ¹ | OK Cancel | | | |
| | 9QrCX1X5qHORNcjIYVrnQyZGIk8t390591 | | | | |
| cr1rhf6ht7SwGgfgGW2aL8HyiF1 | PUDACui la TRussifuslist.foots400Ddf | | | | |
| E1IJGt9QLiwMmXormxcOg+WR2I: | Text Viewer | | | | |
| NjwtR+1SkqMCXs+PzcAHDsiuGz www.pcp.cicultupe.uppipication.www | | | | | |
| pE3huhK5cfvu1Ug7+Oa9SUAy4J | ^{74J} *** Status: Good Signature from Valid Key | | | | |
| NZncI3vJgkZeZrlbh+pi4dRjs0 | *** Signer: Heiko Rossnagel <heiko.rossnagel@m-lehrstuhl.de></heiko.rossnagel@m-lehrstuhl.de> | | | | |
| =hCO9 | (0x85964FC9) | | | | |
| END PGP MESSAGE | *** Signed: 26.02.2004 11: | | | | |
| · · · · · · · · · · · · · · · · · · · | *** Verified: 26.02.2004 11: | | | | |
| heiko rossnagel | *** BEGIN PGP DECRYPTED/VERI | FIED MESSAGE *** | | | |
| frankfurt direkt: | | | | | |
| -25306 D-60054 frankfurt | Hallo Jan. | | | | |
| | My exercises for the "MC1" test are enclosed: | | | | |
| | | | | | |
| | *** END PGP DECRYPTED/VERIFIED MESSAGE *** | | | | |
| | *** END FOF DECRIFIED/VERIFIED NEODAGE *** | | | | |
| | | | | | |
| | 1 | | | | |
| | | | | | |
| | | Copy to Clipboard OK | | | |
| | | | | | |

Asymmetric Signature Systems: Examples

- RSA: Rivest, Shamir, Adleman
 - Asymmetric encryption system which also can be used as a signature system via "inverted use",
 - Message encrypted with the private key (= signing key) gives the signature,
 - Decoding with the public key (=testing key) has to produce the message.

[Rivest et al. 1978]

- DSA: Digital Signature Algorithm
 - Determined in the Digital Signature Standard of the NIST (USA),
 - Based on discrete logarithms (Schnorr, ElGamal),
 - Key length is set to 1024 bit.



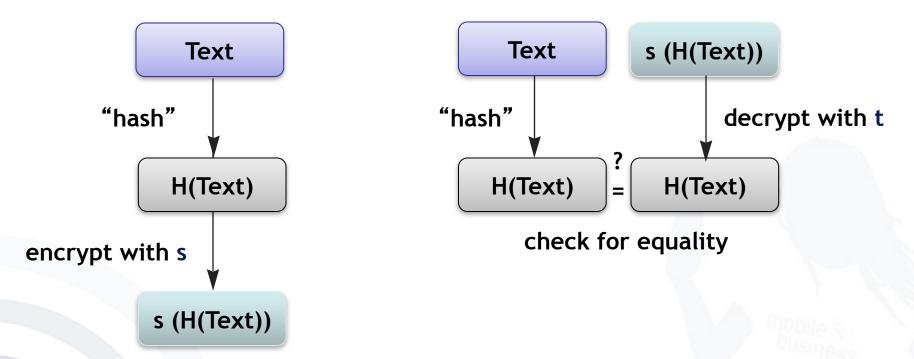
Signing key s only with the sender, test key t public
 Example is often mistakenly generalized.



Asymmetric Signature System (Example RSA)

Sender / Signer





Signing key s only with the sender, test key t public
 Example is often mistakenly generalized.



Hash Functions

- General hash functions (H(s))
 - Transformation of an input string s into an output string h of fixed length which is called hash value.
 - Example: mod 10 in the decimal system
- Cryptographic hash functions
 - Generally require further characteristics
 - H(s) is easily to compute for each s.
 - H(s) must be difficult to invert: In terms of figures it is difficult to compute s from h.
 - Virtual collision freedom: In terms of figures it is difficult to create collisions H(s1) = H(s2).
 - Examples: SHA-1, MD5, MD4



Agenda

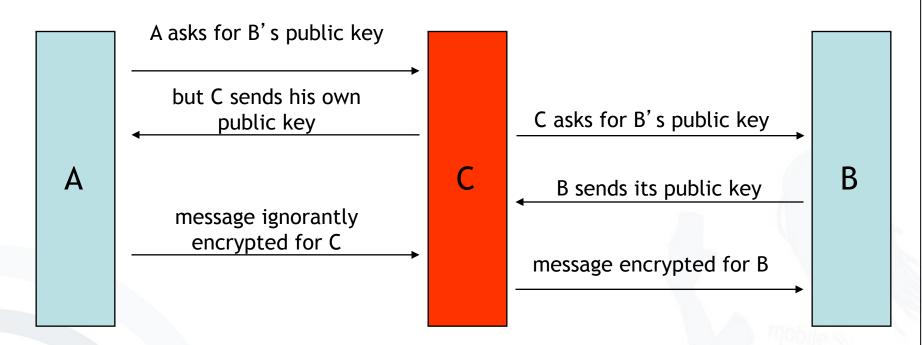


mobile business

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



"Man in the middle attack"



Keys are certified: a 3rd person/institution confirms (with its digital signature) the affiliation of the public key to a person.

Certification of Public Keys (1)

- **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)

Certification of Public Keys (2)

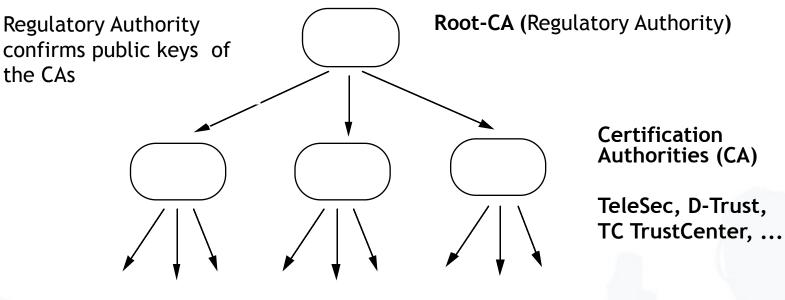
Three types of organization for certification systems (PKIs?):

- 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)

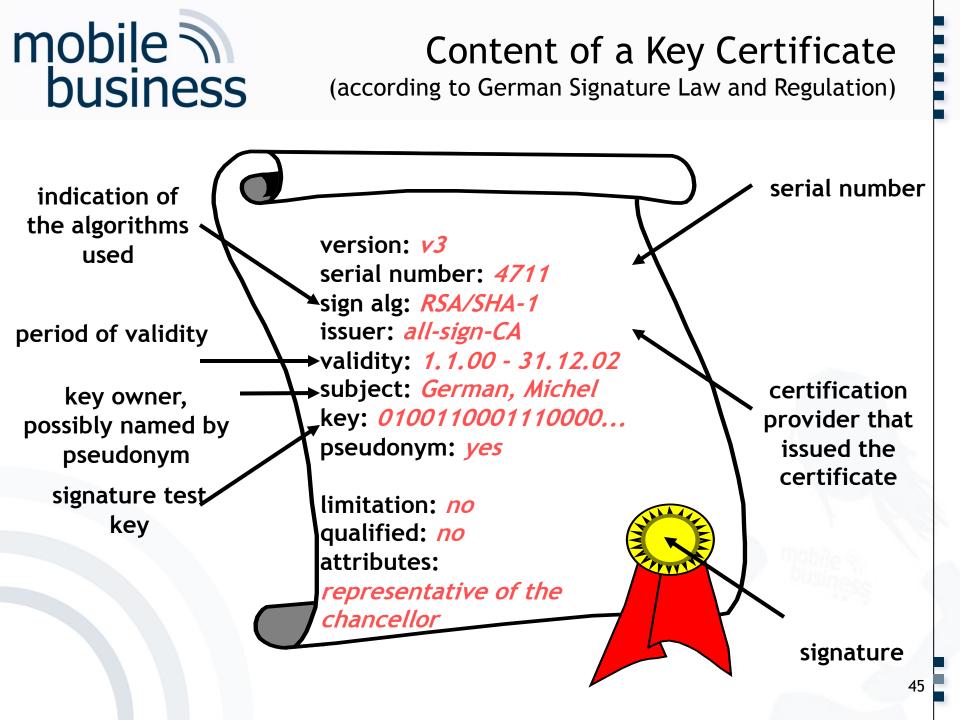


persons

organizations

TeleSec, D-Trust,

- 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.







- 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 by PIN)
- Publication of the certificate (if wanted)
- Barring of certificates
- If necessary issuing 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

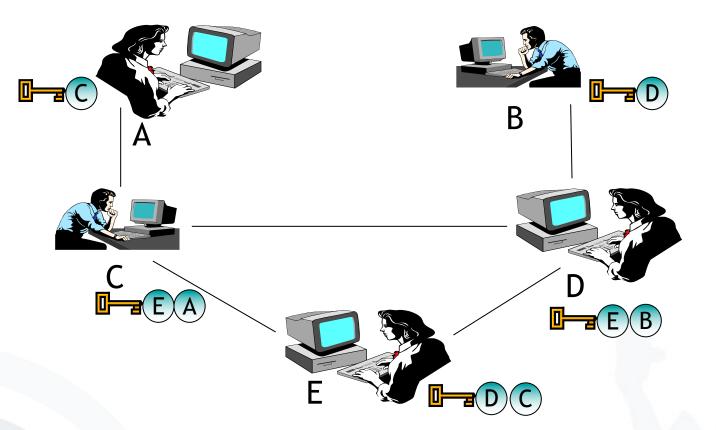
Possibly license of the regulation authority

mobile business Web of Trust "Introducer" David Bob knows David and has received David's public key by David himself Alice lets David sign her public key Bob can verify Alice' key Alice sends the signed on the basis of David's key to Bob signature Bob encrypts his message to Alice Bob Alice with the received key 5

- 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.



Agenda

mobile business

Introduction

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



Protection of Email 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

| n Kahl < christian.kahl@m-le | Nicht gefundene Empfänger | | | | |
|--|---|---|---|--|--|
| | Empfänger für Verschlüsselung wählen | | | | |
| | | | | | |
| | Benutzer-ID | Vertrauen | Ablauf | Schlüssel-ID | Ę |
| | Christian Kahl < christian.kahl@m-lehrstuhl.de> | absolutes Ver | | 14E21EDA | |
| | Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um zu | | 02.09.2006 | 8D539C6E | ····· |
| MB II slides for lect | □ ■ Alexander Boettcher <ab764283@inf.tu-dresden.de></ab764283@inf.tu-dresden.de> | | | A63325B3 | |
| | Alexander Boettcher <ab764283@os.inf.tu-dresden.de></ab764283@os.inf.tu-dresden.de> | abgelaufen | 11.10.2005 | F26EE0CD | |
| | Andre Meixner <s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de> | - | | 7C433232 | |
| | | - | | 7E39E652 | |
| Bestätigung | ELEVANCE | 25 | | 52B1B05D | = |
| | | 2 | | A0D40924 | |
| VERSCHLUSSELTE INachricht an | rolgende Emptanger senden: | - | | 79B42C58 | |
| christian.kahl@m-lehrstuhl.de | | - | | B06F3816 | |
| | | 10 | | 0789B57F | |
| e> t: http:// Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt: | | | | | |
| | | 7. | | 9347DB3C | |
| , v.e., v.e. | | - | 20.02.2009 | 48CC64C2 | |
| | Ja <u>N</u> ein | 1 | | 8EF041F1 | |
| | | 3 | | 289E7DB2 | |
| | Katja Liesebach < katja.iiesebach@m-chair.net> | absolutes Ver | | C4495AF0 | |
| | E Katrin Borcea <kati@inf.tu-dresden.de></kati@inf.tu-dresden.de> | - | | F7C207CE | + |
| | christian.kahl@m-lehrstuhl.de Hinweis: Die Nachricht wurde m | Image: Alexander Boettcher < ab764283@os.inf.tu-dresden.de> Andre Meixmer <s4538672@inf.tu-dresden.de> Bestätigung VERSCHLÜSSELTE Nachricht an folgende Empfänger senden: christian.kahl@m-lehrstuhl.de Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt: Dx42B8B29914E21EDA, 0x23EE4D96C4495AF0 Ja Nein</s4538672@inf.tu-dresden.de> | Image: All attracts 101 Ltc. Alexander Boettcher < ab764283@os.inf.tu-dresden.de> abgelaufen Andre Meixner <s4538672@inf.tu-dresden.de> - Bestätigung Image: Comparison of the state of</s4538672@inf.tu-dresden.de> | Alexander Boettcher < ab764283@os.inf.tu-dresden.de> abgelaufen 11.10.2005 Andre Meixmer <s4538672@inf.tu-dresden.de> - Bestätigung Image: Second State S</s4538672@inf.tu-dresden.de> | Alexander Boetticher <ab764283@os.inf.tu-dresden.de> abgelaufen 11.10.2005 F26EEOCD Andre Meixner <s4538672@inf.tu-dresden.de> Andre Meixner <s4538672@inf.tu-dresden.de> Andre Meixner <s4538672@inf.tu-dresden.de> LEVANCE Andre Meixner <s4538672@inf.tu-dresden.de> LEVANCE LEVANCE LEVANCE LEVANCE AOD40924 AOD4</s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de></ab764283@os.inf.tu-dresden.de> |

OpenPGP: Decrypt Message

| Betreff: MB II Slides | |
|---|--|
| Von: Katja Liesebach <katja.liesebach@m-chair.net></katja.liesebach@m-chair.net> | |
| Datum: 19:18 | |
| An: Christian Kahl <christian.kahl@m-chair.net></christian.kahl@m-chair.net> | |
| Comment: Using GnuPG with Mozill | enPGP-Passphrase oder SmartCard-PIN ein Betreff: MB II Slides |
| 1LSWpm1xA11H1p12t1Kd9ecdjV10F001 V Erst nach 5 Minute 6xkXLtS6PkSb0k5nKkMZ1147F80IrvWi | Von: Katja Liesebach <katja.liesebach@m-chair.net></katja.liesebach@m-chair.net> |
| /Omd5jClR8N/NJeuSfsW6w1LUpTVHQQY zQAvcf2AvjqHHw4UldKW8ewB3GG4zqDl | Datum: 19:18 |
| XxkOviAC+ADTcPgF5FvYPpbEiKS9D8dgzZrBd07YIfdH0oMBgga9k | An: Christian Kahl <christian.kahl@m-chair.net></christian.kahl@m-chair.net> |
| JOKAYGJKXKQTILNGQIY39ITY20TOWIJAA+UPK2PQIA3IIDHEOQMSY cFJW5KxpqNFGvixp7wU6I+e7d6Df80== | Hi Christian, please find attached the MB II slides for lecture 7. |
| END PGP MESSAGE | |
| | DiplMedien-inf. Katja Liesebach |
| | Johann Wolfgang Goethe University Frankfurt a. M. Institute of Business <u>Informatics</u> <u>Chair</u> of Mobile Business and Multilateral <u>Security</u> <u>Graefstr</u> . 78, D-60486 Frankfurt a. M., <u>Germany</u> |
| | Internet: http://m-chair.net Fon: +49 (69) 798-25313 |
| | Fax: +49 (69) 798-25306 |



PGP-Certification of Keys

- 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: Key Management

| Benutzer-ID Vertrauen Ablauf-D Typ Alexander Boettcher ('Nur wenige wissen, wie viel man wissen muss, um z abgelaufen 02.09.2006 öffentlich Benutzer-ID OZ.09.2006 öffentlich Alexander Boettcher <ab764283@inf.tu-dresden.de> absolutes Vertrauen öffentlich Belavander Boettcher <ab764283@os.inf.tu-dresden.de> absolutes Vertrauen öffentlich Andreas Albers <abr></abr>absolutes Vertrauen öffentlich Andreas Albers <andreas.albers@m-lehrstuhl.de> absolutes Vertrauen öffentlich absolutes Vertrauen Andreas Pfitzmann <pritza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich absolutes Vertrauen Birgit Prescheck <birgit.pretscheck@gmx.net> - - - Christian Kahl <christian.kahl@m-lehrstuhl.de> absolutes Vertrauen Ochristian Kahl <christian.kahl@m-lehrstuhl.de> Bolites Vertrauen absolutes Vertrauen Ochristian Kahl <christian.kahl@m-lehrstuhl.de> - @ Denis Royer <me@myasterisk.de> absolutes Vertrauen Ox14E21EDA - @ Hagen Wahrig <wahrig@web.de> - - - - @ Hagen Wahrig <wahrig@m-lehrstuhl.de> absolutes Vertrauen absolutes Vertrauen absolutes</wahrig@m-lehrstuhl.de></wahrig@web.de></me@myasterisk.de></christian.kahl@m-lehrstuhl.de></christian.kahl@m-lehrstuhl.de></christian.kahl@m-lehrstuhl.de></birgit.pretscheck@gmx.net></pritza@inf.tu-dresden.de></andreas.albers@m-lehrstuhl.de></ab764283@os.inf.tu-dresden.de></ab764283@inf.tu-dresden.de> | Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten: | | | Alle zeig | en | | | |
|--|---|-----------------|------------------------------|-----------|---|------------|------------|-------------------|
| Alexander Boettcher < ab764283@inf.tu-dresden.de> absolutes Vertrauen öffentlich Alexander Boettcher < ab764283@os.inf.tu-dresden.de> obgelaufen 11.10.2005 öffentlich Andre Meixner < s4538672@inf.tu-dresden.de> - öffentlich offentlich 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 Vertrauen offentlich André Solutes - Schlüsseleigenschaften Birgit Pretscheck < birgit.pretscheck@gmx.net> - - Christian Kahl < christian.kahl@m-lehrstuhl.de> absolutes Vertrauen Ortistian Kahl < christian.kahl@m-lehrstuhl.de> B Denis Royer < me@myasterisk.de> absolutes Vertrauen offentlich - B' Hagen Wahrig@web.de> - - - - B' Hagen Wahrig@wahrig@web.de> - - - - B' Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Vertrauen absolutes Vertrauen absolutes Vertrauen Besitzer-Vertrauen absolutes Vertrauen absolutes Vert</zibuschka@m-lehrstuhl.de> | nutzer-ID | Vertrauen | Ablauf-D | Тур | E. | | | |
| Alexander Boettcher < ab 764283@os.inf.tu-dresden.de> ab gelaufen 11.10.2005 öffentlich absolutes Vertrauen öffentlich öffentlich absolutes Vertrauen öffentlich öffentlich öffentlich öxtlüssel-ID öxtlässel-ID | lexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um z | abgelaufen | 02.09.2006 | öffentlid | th 🔺 | | | |
| Andre Meixner <\$4538672@inf.tu-dresden.de> - offentlich Andreas Albers < andreas.albers@m-lehrstuhl.de> absolutes Vertrauen öffentlich Andreas Pfitzmann < pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich Andréas Pfitzmann < pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich André Deuker < andre.deuker@m-lehrstuhl.de> absolutes Vertrauen öffentlich Birgit Pretscheck < birgit.pretscheck@gmx.net> - - Christian Kahl < christian.kahl@m-lehrstuhl.de> absolutes Vertrauen öffentlich Bonis Royer < me@myasterisk.de> absolutes Vertrauen Christian Kahl < christian.kahl@m-lehrstuhl.de> Elvira Koch < Elvira.Koch@m-lehrstuhl.de> volles Vertrauen Ox14E21EDA Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> - Typ öffentlich # Hagen Wahrig < wahrig@web.de> - - Typ öffentlich # Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Vertrauen absolutes Vertrauen absolutes Vertrauen # Kaija Liesebach <katja.liesebach@mir.tu-dresden.de> - - absolutes Vertrauen absolutes Vertrauen # Katja Liesebach <katja.liesebach@m-chair.net> <</katja.liesebach@m-chair.net></katja.liesebach@mir.tu-dresden.de></zibuschka@m-lehrstuhl.de></fg798936@inf.tu-dresden.de> | lexander Boettcher <ab764283@inf.tu-dresden.de></ab764283@inf.tu-dresden.de> | absolutes Vertr | rauen | öffentli | ch 🗌 | | | |
| Andreas Albers < andreas.albers@m-lehrstuhl.de> absolutes Vertrauen öffentlich Andreas Pfitzmann < pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich Andreas Pfitzmann < pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich Andreas Pfitzmann < pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich Andreas Albers < andre.deuker@m-lehrstuhl.de> absolutes Vertrauen öffentlich Birgit Pretscheck < birgit.pretscheck@gmx.net> - Christian Kahl@m-lehrstuhl.de> Schlüsseleigenschaften © Denis Royer <me@myasterisk.de> absolutes Vertrauen Schlüssel-ID Ox14E21EDA © Livia Koch <elvira.koch@m-lehrstuhl.de> - - Typ öffentlich # Hagen Wahrig <wahrig@web.de> - - Typ öffentlich # Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ver absolutes Ver absolutes Ver # Kaia leisebach <katja.liesebach@minf.tu-dresden.de> - Besitzer-Vertrauen absolutes Vertrauen absolutes Ver - - - absolutes Ver absolutes Vertrauen</katja.liesebach@minf.tu-dresden.de></zibuschka@m-lehrstuhl.de></wahrig@web.de></elvira.koch@m-lehrstuhl.de></me@myasterisk.de> | lexander Boettcher <ab764283@os.inf.tu-dresden.de></ab764283@os.inf.tu-dresden.de> | abgelaufen | 11.10.2005 | öffentlid | th 🛛 | | | |
| Andreas Pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE absolutes Vertrauen öffentlich André Deuker < andre.deuker@m-lehrstuhl.de> absolutes Vertrauen öffentlich Birgit Pretscheck < birgit.pretscheck@gmx.net> - Schlüsseleigenschaften Christian Kahl < christian.kahl@m-lehrstuhl.de> absolutes Vertrauen Ortimäre Benutzer-ID Christian Kahl < christian.kahl@m-lehrstuhl.de | ndre Meixner <s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de> | - | | öffentli | ch 🛛 | | | |
| André Deuker < andre. deuker@m-lehrstuhl.de> absolutes Ve Birgit Pretscheck < birgit.pretscheck@gmx.net> absolutes Ve Christian Kahl < christian.kahl@m-lehrstuhl.de> absolutes Ve Denis Royer < me@myasterisk.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 @wab.de> - Hagen Wahrig @wab.de> - Jan Zibuschka < zibuschka@m-lehrstuhl.de> absolutes Ve Kai Rannenberg < Kai.Rannenberg@m-lehrstuhl.de> - Katja Liesebach <katja.liesebach@m-chair.net> absolutes Ve Besitzer-Vertrauen absolutes Vertrauen absolutes Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net> | ndreas Albers <andreas.albers@m-lehrstuhl.de></andreas.albers@m-lehrstuhl.de> | absolutes Vertr | rauen | öffentli | ch 👘 | | | |
| 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> - Katja Liesebach <katja.liesebach@m-chair.net> - Ataja Liesebach <katja.liesebach@m-chair.net> absolutes Ve Besitzer-Vertrauen absolutes Vertrauen absolutes Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></katja.liesebach@m-chair.net></kai.rannenberg@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de></wahrig@web.de> | ndreas Pfitzmann <pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE</pfitza@inf.tu-dresden.de> | | | | ch | | | |
| 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> - Hagen Wahrig <wahrig@web.de> - Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ve Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de> - Katja Liesebach <katja.liesebach@m-chair.net> - Besitzer-Vertrauen absolutes Vertrauen absolutes Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></kai.rannenberg@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de></wahrig@web.de></wahrig@web.de> | ndré Deuker <andre.deuker@m-lehrstuhl.de></andre.deuker@m-lehrstuhl.de> | absolutes Ve | Schlüsseleigensc | haften | | | | _ |
| Denis Royer <me@myasterisk.de> absolutes Ve Primare Benutzer-ID Christian Kahl <christian.kahl@m-lehrstuhl.de< th=""> Elvira Koch <elvira.koch@m-lehrstuhl.de> volles Vertra Schlüssel-ID 0x14E21EDA Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> - Typ öffentlich Hagen Wahrig <wahrig@web.de> - Typ öffentlich Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ve Vertrauen absolutes Ve Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de> - Besitzer-Vertrauen absolutes Vertrauen Katja Liesebach <katja.liesebach@m-chair.net> absolutes V Besitzer-Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></kai.rannenberg@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de></wahrig@web.de></fg798936@inf.tu-dresden.de></elvira.koch@m-lehrstuhl.de></christian.kahl@m-lehrstuhl.de<></me@myasterisk.de> | irgit Pretscheck kirgit.pretscheck@gmx.net> | - | j | | | | | |
| Denis Royer <me@myasterisk.de> absolutes Ve</me@myasterisk.de> Elvira Koch <elvira.koch@m-lehrstuhl.de> volles Vertra</elvira.koch@m-lehrstuhl.de> Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> -</fg798936@inf.tu-dresden.de> Hagen Wahrig <wahrig@web.de> -</wahrig@web.de> Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ve</zibuschka@m-lehrstuhl.de> Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de> absolutes Ve</kai.rannenberg@m-lehrstuhl.de> Kaia Liesebach <katja.liesebach@inf.tu-dresden.de> -</katja.liesebach@inf.tu-dresden.de> Katja Liesebach <katja.liesebach@m-chair.net> absolutes Ve</katja.liesebach@m-chair.net> Besitzer-Vertrauen absolutes Vertrauen | hristian Kahl <christian.kahl@m-lehrstuhl.de></christian.kahl@m-lehrstuhl.de> | absolutes Ve | Primäre Benut | zer-ID | Chainting Kabler | - La tatan | | |
| Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> - 5Childsser10 0x14E21EDA Hagen Wahrig@web.de> - Typ öffentlich Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ve Vertrauen absolutes Ver Katja Liesebach <katja.liesebach@m-chair.net> - Besitzer-Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></zibuschka@m-lehrstuhl.de></fg798936@inf.tu-dresden.de> | enis Royer <me@myasterisk.de></me@myasterisk.de> | absolutes Ve | r minore Denae | | Christian Kani < | christian. | kani@m-ien | irstuni.de> |
| Felix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de> - Typ Öffentlich Hagen Wahrig «wahrig@web.de> - Typ Öffentlich Jan Zibuschka <zibuschka@m-lehrstuhl.de> absolutes Ve Vertrauen absolutes Ve Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de> - Besitzer-Vertrauen absolutes Vertrauen Katja Liesebach <katja.liesebach@m-chair.net> absolutes Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></kai.rannenberg@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de></fg798936@inf.tu-dresden.de> | lvira Koch <elvira.koch@m-lehrstuhl.de></elvira.koch@m-lehrstuhl.de> | volles Vertra | Schlüssel-ID | [| 0x14E21EDA | | | |
| Jan Zibuschka <zibuschka@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de> Mai Rannenberg <kai.rannenberg@m-lehrstuhl.de></kai.rannenberg@m-lehrstuhl.de> absolutes Ve Katja Liesebach <katja.liesebach@inf.tu-dresden.de></katja.liesebach@inf.tu-dresden.de> Katja Liesebach <katja.liesebach@m-chair.net></katja.liesebach@m-chair.net> absolutes Ve Besitzer-Vertrauen absolutes Vertrauen | elix Göpfert (keine Passphrase) <fg798936@inf.tu-dresden.de></fg798936@inf.tu-dresden.de> | - | | | VALAEZIEDA | | | |
| • Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de> absolutes Ve Vertrauen absolutes Ve Vertrauen Katja Liesebach <katja.liesebach@m-chair.net> absolutes Ve Besitzer-Vertrauen absolutes Vertrauen</katja.liesebach@m-chair.net></kai.rannenberg@m-lehrstuhl.de> | lagen Wahrig <wahrig@web.de></wahrig@web.de> | - | Тур | | öffentlich | | | |
| Kai Kannenberg «Kai Kannenberg@m-ienrstuni.de» absolutes vertrauen Katja Liesebach «katja.liesebach@inf.tu-dresden.de» - Katja Liesebach «katja.liesebach@m-chair.net> absolutes Vertrauen | an Zibuschka <zibuschka@m-lehrstuhl.de></zibuschka@m-lehrstuhl.de> | absolutes Ve | Vertrauen | | | | | |
| Katja Liesebach <katja.liesebach@m-chair.net> absolutes V</katja.liesebach@m-chair.net> | ai Rannenberg <kai.rannenberg@m-lehrstuhl.de></kai.rannenberg@m-lehrstuhl.de> | absolutes Ve | Vertrauen absolutes Vertraue | | uen | | | |
| Katja Liesebach <katja.liesebach@m-chair.net> absolutes V</katja.liesebach@m-chair.net> | atja Liesebach <katja.liesebach@inf.tu-dresden.de></katja.liesebach@inf.tu-dresden.de> | - | Recitzer-Vertra | uen | abcolutor Vortrauon | | | |
| | atja Liesebach <katja.liesebach@m-chair.net></katja.liesebach@m-chair.net> | absolutes V | Desitzer-vertia | uen | absolutes Vertra | uen | | |
| # Katrin Borcea < kati@inf.tu-dresden.de> - Fingerabdruck E1 CC 2A AS PCP2 452A 65C2 DDD2 42P8 P200 | atrin Borcea <kati@inf.tu-dresden.de></kati@inf.tu-dresden.de> | - | Fingerabdruck | - F | E1CC 3AA5 BCB2 452A 65C2 DDD3 42B8 B299 | | | D9 D200 14E2 1ED/ |
| Marco Lehmann <m99@gmx.li></m99@gmx.li> | | - | | | EICC SAAD BCB | 2 4JZA UJ | CZ DDD5 42 | DO D299 14EZ IEDA |
| Mathias Staab <mathias.staab@arcor.de> Typ ID Algo Stär Erzeugt Ablau</mathias.staab@arcor.de> | 1athias Staab <mathias.staab@arcor.de></mathias.staab@arcor.de> | - | Typ | ID | Algo | Stär | Frzeuat | Ablauf-Datum |
| Mike Bergmann (dienstlich, TU Dresden, unbeschrnkt gltig) <mb41@inf.t.,< td=""><td>/ike Beramann (dienstlich. TU Dresden. unbeschrnkt altia) <mb41@inf.t< td=""><td>-</td><td></td><td></td><td>-</td><td></td><td>-</td><td></td></mb41@inf.t<></td></mb41@inf.t.,<> | /ike Beramann (dienstlich. TU Dresden. unbeschrnkt altia) <mb41@inf.t< td=""><td>-</td><td></td><td></td><td>-</td><td></td><td>-</td><td></td></mb41@inf.t<> | - | | | - | | - | |
| Unterschlüssel 0x98F0 ELG 2048 07.09.2007 nie | | | Unterschlüs | sel 0x | BEFU ELG | 2048 (| 17.09.2007 | nie |

60

Key-Server

| | Benutzer-ID | Erstellt | Schlüssel-ID | |
|--------------------------|--------------|--------------------|--------------|--|
| | □ | 1997-03-09 | | |
| | □ | 1997-09-18 | | |
| | □ | 1997-03-09 6623E0D | | |
| | | | | |
| | Y | | | |
| sel-Server auswählen | | | | |
| | | | | |
| he nach Schlüssel Kai Ra | nnenberg | | | |
| | /s.pgp.net | | | |
| Subre | spyphiet | | | |
| | | | | |
| | | | | |
| | OK Abbrechen | | | |
| | OK Abbrechen | | | |
| | OK Abbrechen | | | |
| C | OK Abbrechen | | | |
| C | OK Abbrechen | | | |
| | OK Abbrechen | | | |
| | OK Abbrechen | 0 | K Abbrec | |

mobile business

PGP: Public Key Catalogs

| <u>-</u> jie <u>E</u> di | it <u>V</u> iew F <u>a</u> vorites | <u>T</u> ools <u>H</u> elp | |
|--------------------------|------------------------------------|--|---------|
| Þ Back | • • • 🕲 😰 🖞 | 🖞 🔯 Search 🔝 Favorites 🛞 Media 🍏 🛃 - 🎒 🔯 - 📃 📿 | |
| ddress | http://blackhole.pd | ca.dfn.de:11371/pks/lookup?op=vindex&search=Kai+Rannenberg 🖉 🄗 😡 | Links ' |
| | | | - |
| D | hlia Var | Sower Venhage Index "Kei Dannenhaug !! | |
| r u | опс кеу | ' Server Verbose Index ``Kai Rannenberg '' | |
| | | | |
| Type k | bits/keyID | Date User ID | |
| pub : | 1024/ <u>AF1FDF70</u> | 1997/09/18 kara < <u>kara@iig.uni-freiburg.de</u> > | |
| sig | 0B6375FD | Matthias Schunter < <u>schunter@acm.org</u> > | |
| sig | D5CDE083 | Herbert Damker < <u>damker@iig.uni-freiburg.de</u> > | |
| зig | 879AC041 | Birgit Pfitzmann 1 < <u>pfitzb@informatik.uni-hildesheim.de</u> > NO LEGAL RELEVANCE | |
| sig | 8128DC75 | Gerhard Weck <73064.22710compuserve.com> | |
| sig | 8EF041F1 | Kai R. Rannenberg 2048 < <u>kara0iig.uni-freiburg.de</u> > | |
| sig | 2F8D5039 | Kai Martius < <u>Kai@imib.med.tu-dresden.de</u> > | |
| sig | 5C3C4FE4 | Holger Reif < <u>reif@prakinf.tu-ilmenau.de</u> > | |
| sig | AF1FDF70 | kara < <u>kara@iig.uni-freiburg.de</u> > | |
| sig | 49EF1D84 | Hannes Federrath < <u>federrath@inf.tu-dresden.de</u> > | |
| | | Kai R. Rannenberg < <u>kair@microsoft.com</u> > | |
| sig | <u>0B6375FD</u> | Matthias Schunter < <u>schunter@acm.org</u> > | |
| sig | AEB4BCDD | fapp2_AEB4BCDD_HSK < <u>fapp2@cam.ac.uk</u> > | |
| sig | AF1FDF70 | kara < <u>kara@iig.uni-freiburg.de</u> > | |
| зig | <u>044584B5</u> | Douglas Swiggum < <u>Swiggum@Waisman.Wisc.Edu</u> > | |
| | | Kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> > | |
| зig | OCB6E63F | Martin Reichenbach < <u>marei@iig.uni-freiburg.de</u> > | |
| sig | AF1FDF70 | kara < <u>kara@iig.uni-freiburg.de</u> > | |
| | | kara < <u>kara@telematik.iig.uni-freiburg.de</u> > | |
| sig | <u>0B6375FD</u> | Matthias Schunter < <u>schunter@acm.org</u> > | |
| sig | AF1FDF70 | kara < <u>kara@iig.uni-freiburg.de</u> > | |
| | | Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > | |
| sig | <u>0B6375FD</u> | Matthias Schunter < <u>schunter@acm.org</u> > | |
| sig | AF1FDF70 | kara < <u>kara@iig.uni-freiburg.de</u> > | ĺ |
| | | | Þ |
| | | Internet | |

- Network of public-key servers:
 - www.cam.ac.uk.pgp.net/pgpnet/email-key-server-info.html
 - http://pgp.mit.edu/





PGP: Practical Attacks and Weaknesses

- 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]

Remark

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

(Roger Needham / Butler Lampson)

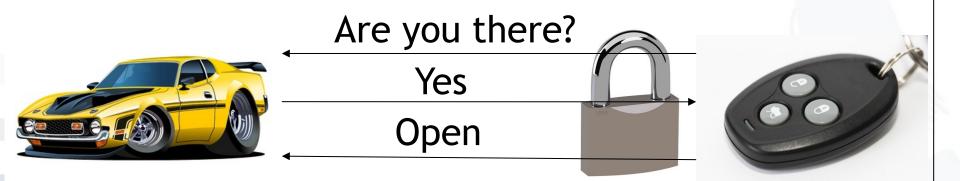
[Marshall Symposium 1998] [Randell 2004]







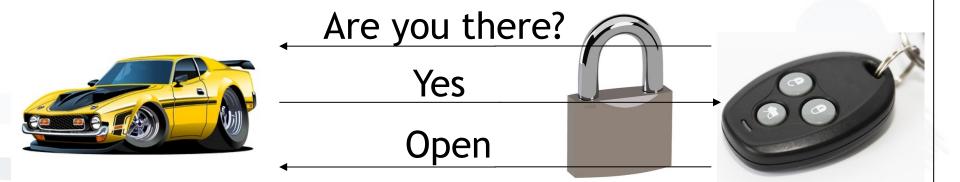
- Solution: Protect communication with crypto?
- e.g. symmetric cryptography + hash/signature



Replay Attack: Eavesdrop

mobile business





(h Are you there? Yes

Open

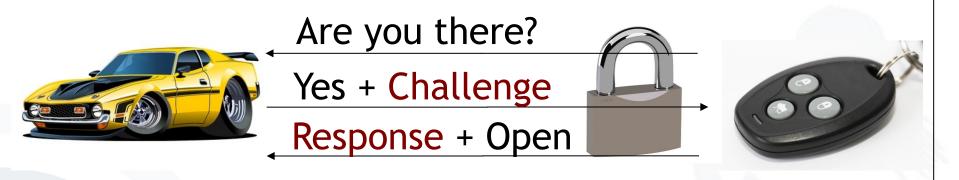


Replay Attack: Replay



Replay Attack: Solution

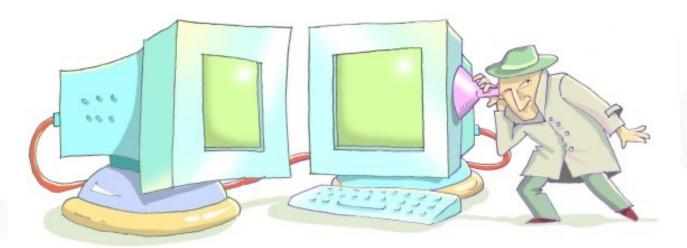
e.g. Challenge-Response helps





Side-Channel Attacks I

 A secure cryptoalgorithm does not imply that the implementation is also secure

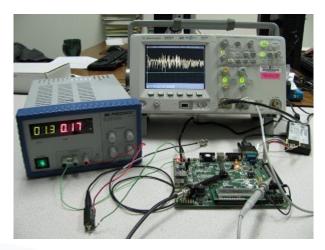


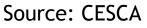
Source: Eran Tromer

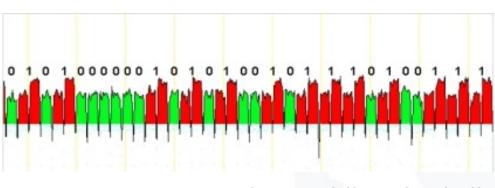


Side-Channel Attacks II

Side-Channels: Time, Power, Noise, Radiation, ...





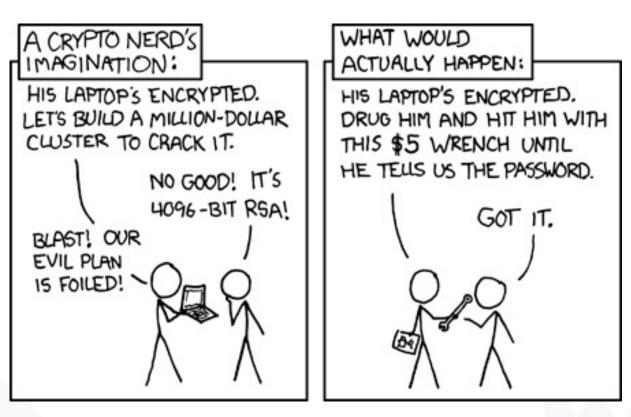


Source: Gilbert Goodwill

- Other data (side-channel) leaks information
- Conclusion on processed bits possible



The Human Element



Source: https://xkcd.com/538/

Human Element: Behavior and Passwords

- Florencio, D. & Herley, C., 2007. A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web - WWW '07*, p.657. Available at: http://portal.acm.org/citation.cfm?doid=1242572.12426 61.
- Florêncio, D., Herley, C. & Coskun, B., 2007. Do strong web passwords accomplish anything? *Proceedings of the* 2nd USENIX workshop on Hot topics in security (HOTSEC'07), p.10. Available at: http://portal.acm.org/citation.cfm?id=1361419.1361429.
- 3. Norberg, P.A., Horne, D.R. & Horne, D.A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), pp.100-126.



Literature

mobile business

- Bishop, M. (2005) Introduction to Computer Security, Addison Wesley, Boston, pp. 97-116.
- Cremers, Cas, et al. "Distance hijacking attacks on distance bounding protocols." 2012 IEEE Symposium on Security and Privacy. IEEE, 2012.
- 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.
- The Marshall Symposium: Address Roger Needham, May 29, 1998, Rackham School of Graduate Studies, University of Michigan web.archive.org/web/20081201182254/http://www.si.umich.edu/marshall/doc s/p201.htm, accessed 2015-04-15.
- Randell, B. (2004) Brief Encounters; Pp. 229-235 in: Andrew Herbert, Karen Spärck Jones: Computer Systems: Theory, Technology, and Applications; New York, Springer 2004
- 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