

#### Lecture 2

Cryptography



#### Mobile Business II (SS 2016)

#### Prof. Dr. Kai Rannenberg

Deutsche Telekom 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



# mobile business

# Symmetric Encryption Systems

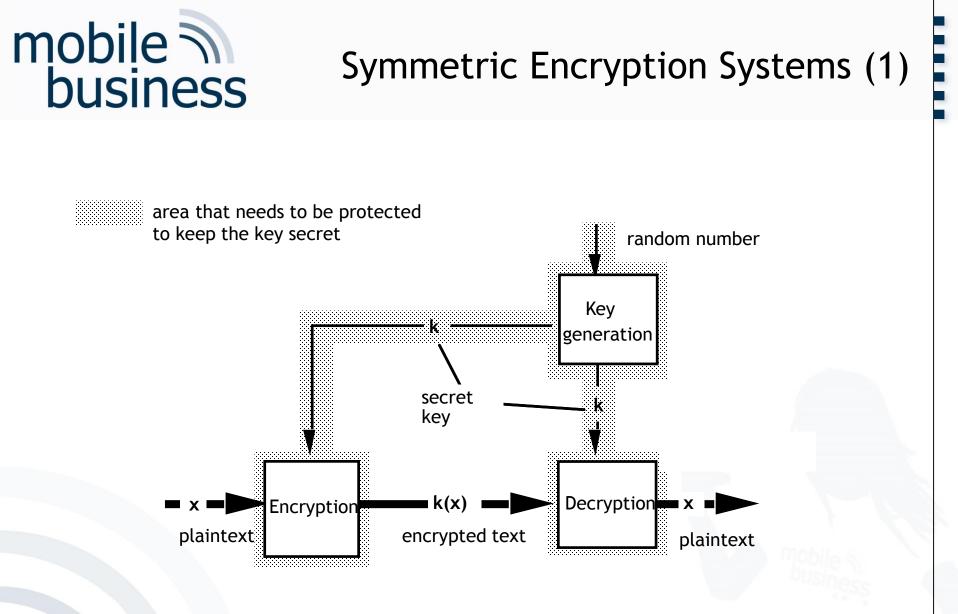
- Typical applications
  - confidential storage of user data
  - transfer of data between 2 users who negotiate a key via a secure channel
  - end-to-end channel encryption
- Examples
  - Vernam-Code (one-time pad, Gilbert Vernam)
    - key length = length of the plaintext (information theoretically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



## Introduction

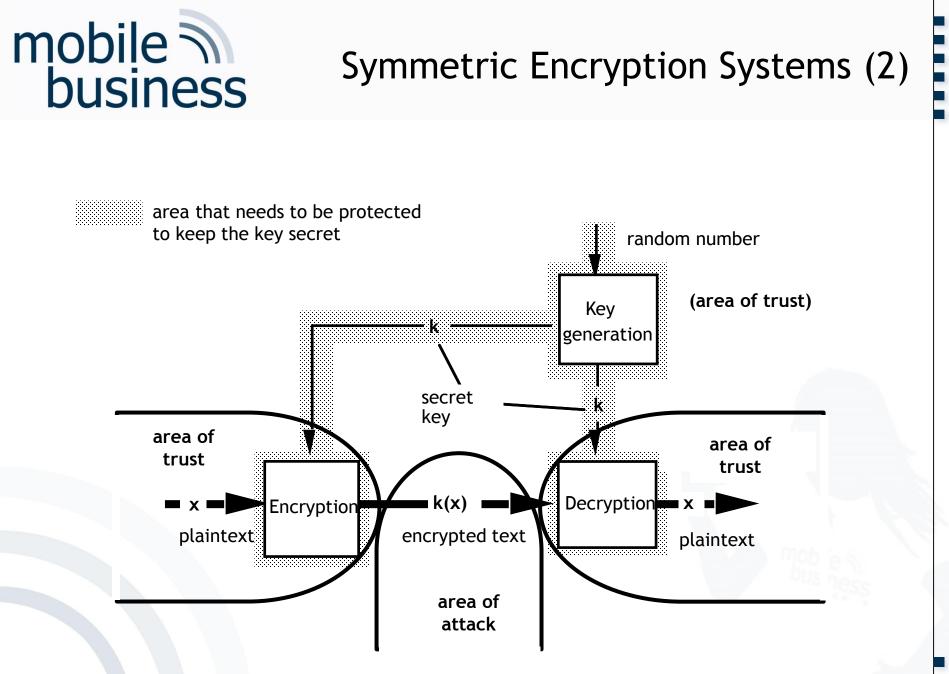
- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES
  - Advantages and Problems
- Public Key Cryptography





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.

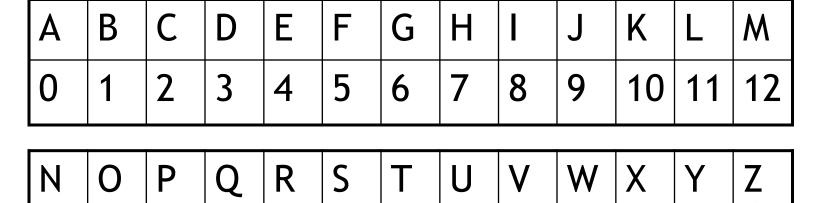




- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES

- Advantages and Problems
- Public Key Cryptography

#### Caesar Cipher



18 19 20 21 22 23 24 25

We assign a number for every character.

17

16

15

14

 This enables us to calculate with letters as if they were numbers.

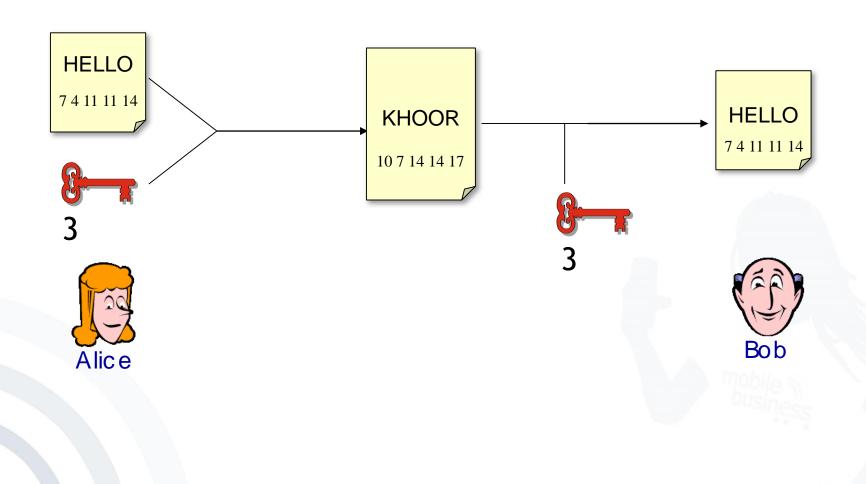




13



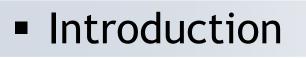
#### Caesar Cipher: Example





- 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]



- Introduction
- Symmetric Cryptosystems
  - General Concept
  - Caesar Cipher
  - AES

- Advantages and Problems
- Public Key Cryptography



# Symmetric Encryption



#### Advantage: Algorithms are very fast

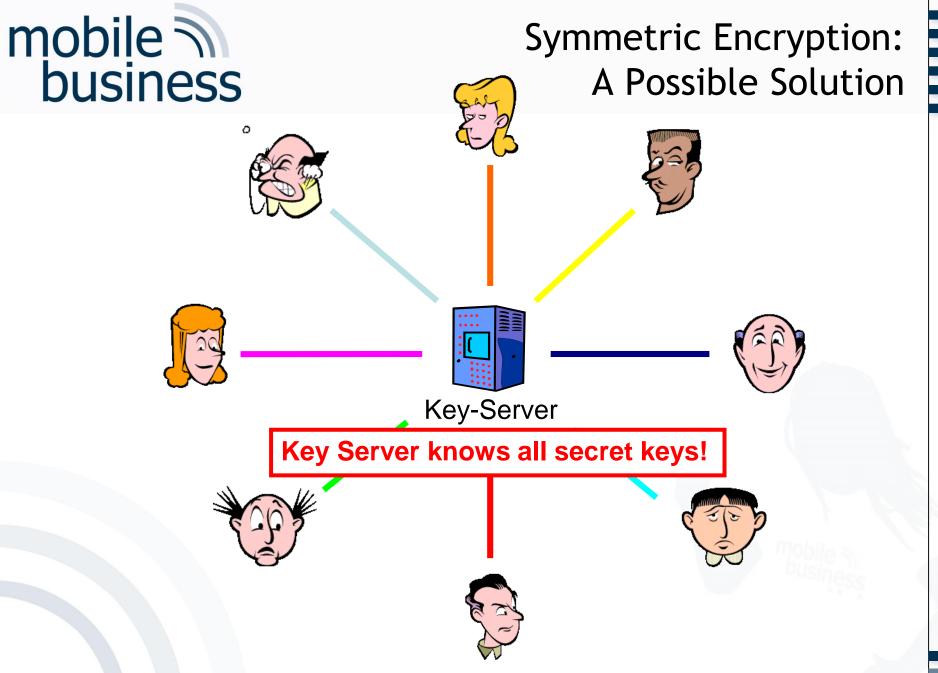
Algorithm	Performance*
RC6	78 ms
SERPENT	95 ms
IDEA	170 ms
MARS	80 ms
TWOFISH	100 ms
DES-ede	250 ms
RIJNDEAL (AES)	65 ms

\* 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

0 n\*(n-1)/2 Keys Internet: ~ 1.000.000.000 Users => ~ 500.000.000.000.000 Keys

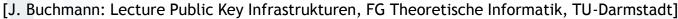


[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]





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



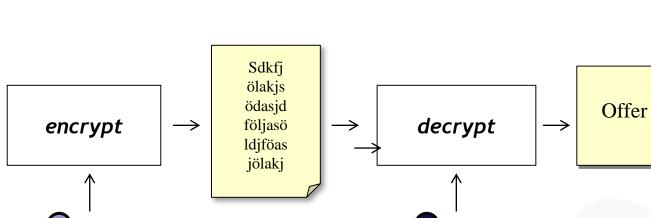
7

asymmetric

Bob

#### Public Key Encryption

private



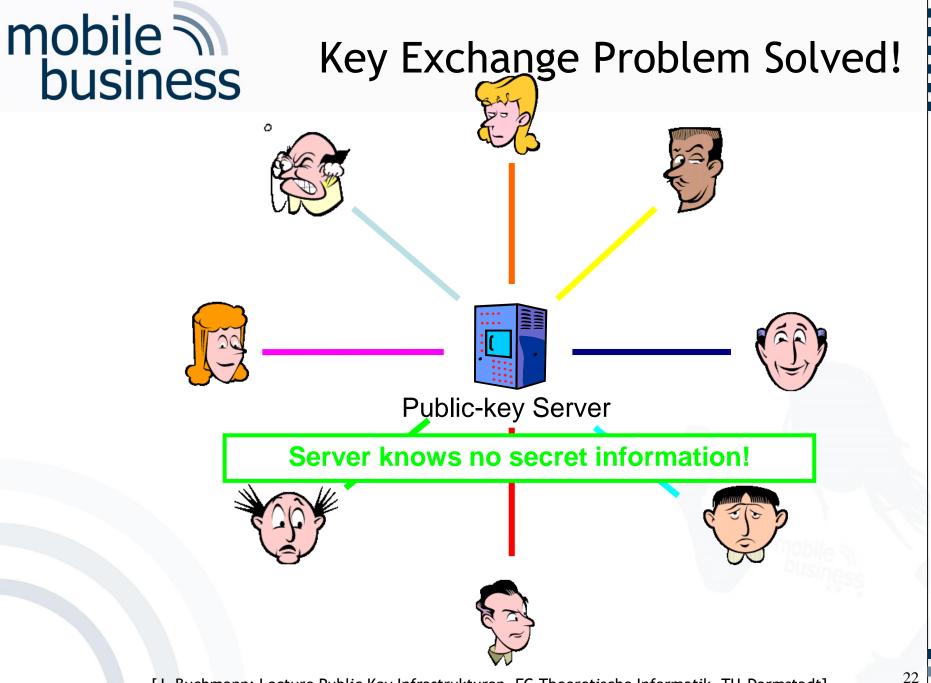
# mobile business

Offer

Alice

ann: Locturo Public Koy Infrastrukturon - EG Theoretische Inf

public



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



Introduction

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



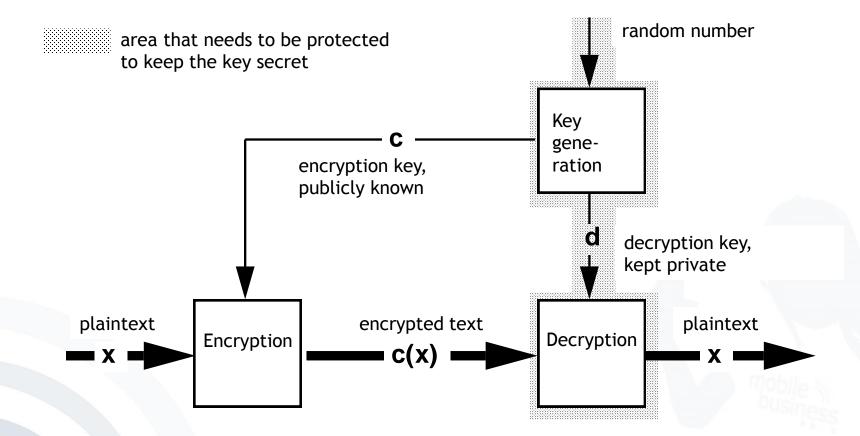


## Concept of Asymmetric Encryption Systems

- 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).

# mobile business

#### 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

# mobile business

#### 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
  - 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

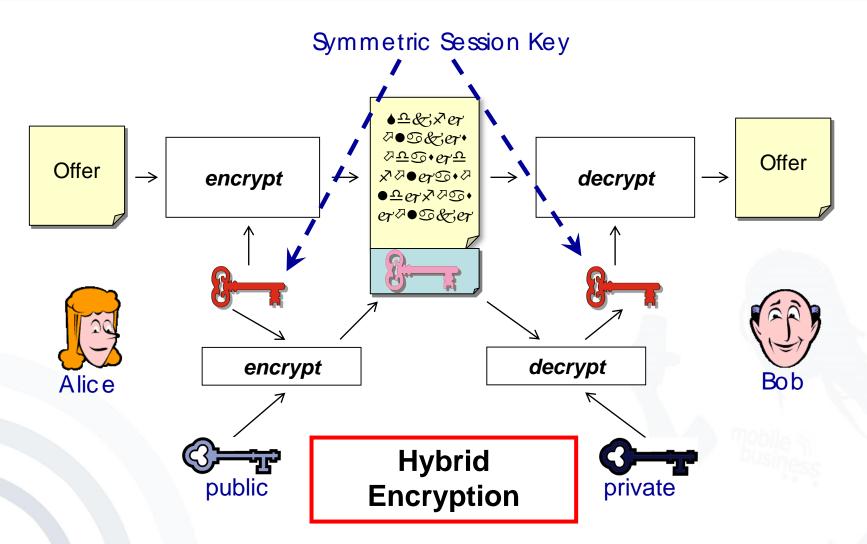
 $\Rightarrow$  Algorithms are very slow.

\* 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]

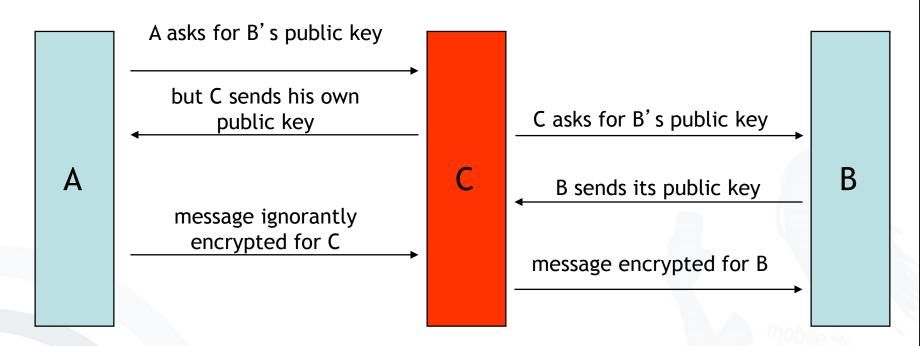




- Symmetric Cryptosystems
- Public Key Cryptography
  - General Concept
  - Algorithms
  - Hybrid Systems
  - Key Management
  - Example: PGP



# "Man in the middle attack"



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

# mobile business

# 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)

# mobile business

# 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

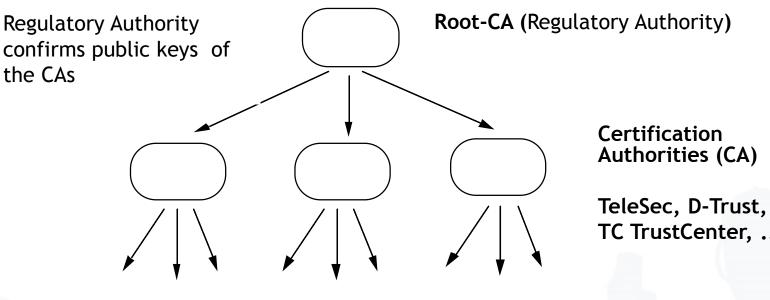
Web of Trust

- 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)

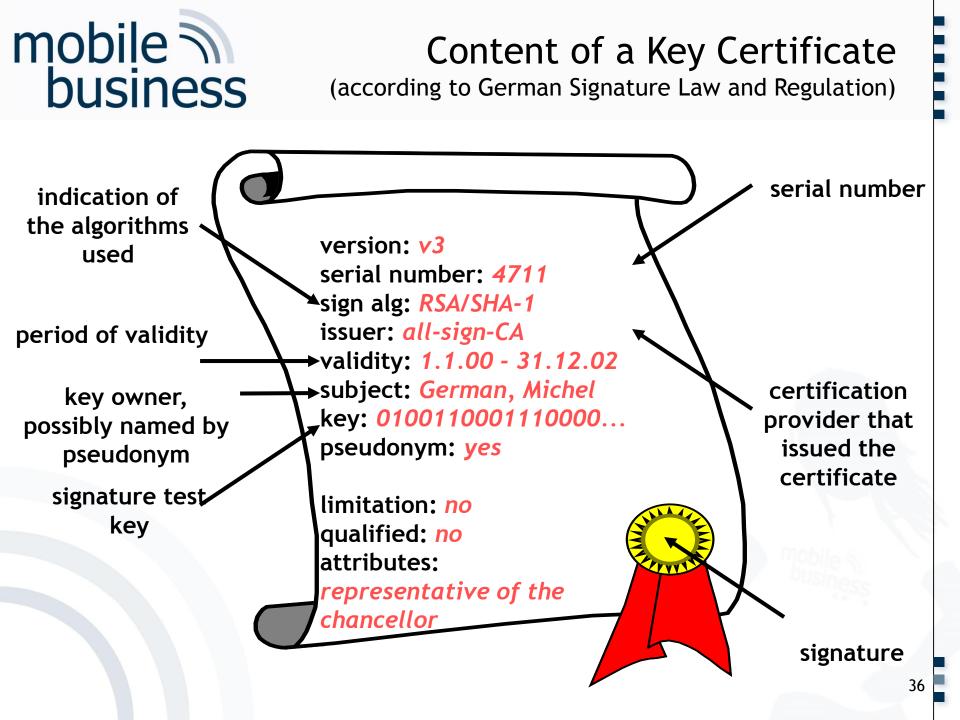


persons

organizations

TC TrustCenter, ...

- 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

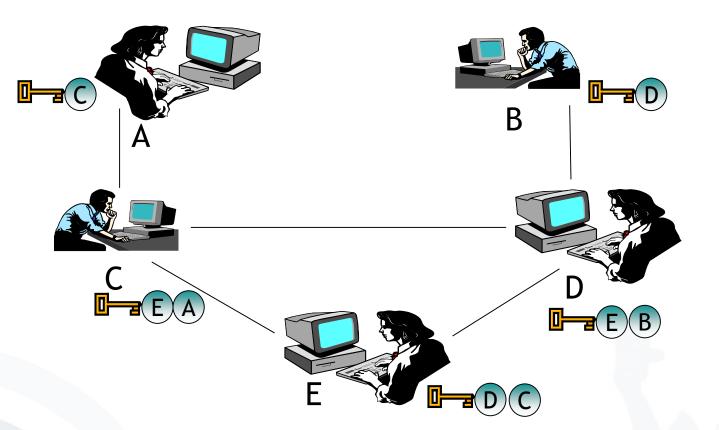
Possibly license of the regulation authority

#### 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 3 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

- Symmetric Cryptosystems
- Public Key Cryptography
  - General Concept
  - Algorithms
  - Hybrid Systems
  - 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

Verfassen: MB II Slice	des Ansicht Einstellungen OpenPGP abc U G Rechtschr, Anhang Open	Extras Hilfe		
Von: Katja Liesebach	n <katja.liesebach@m-chair.net> - ka Christian Kahl <christian.kahl@m-le< th=""><th></th><th></th><th></th></christian.kahl@m-le<></katja.liesebach@m-chair.net>			
Betreff: MB II Slides				
		Benutzer-ID Vertrauen	Ablauf	Schlüssel-ID
Hi Christian, please find attac	ched the MB II slides for lect	✓       Christian Kahl < christian.kahl@m-lehrstuhl.de>       absolutes V         △       Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um zu abgelaufen         □       Alexander Boettcher < ab764283@inf.tu-dresden.de>       -         □       Alexander Boettcher < ab764283@os.inf.tu-dresden.de>       -         □       Alexander Boettcher < ab764283@os.inf.tu-dresden.de>       -         □       Alexander Boettcher < ab764283@os.inf.tu-dresden.de>       -         □       Andre Meixner < s4538672@inf.tu-dresden.de>       -	02.09.2006 11.10.2005	14E21EDA ▲ 8D539C6E A63325B3 F26EE0CD 7C433232
	OpenPGP-Bestätigung	ELEVANCE -		7E39E652 52B1B05D A0D40924
Johann Wolfgang Institute of Bus <u>Chair</u> of Mobile <u>Graefstr</u> . 78, D-	VERSCHLÜSSELTE Nachricht a christian.kahl@m-lehrstuhl.de	folgende Empfänger senden:		79B42C58 B06F3816 0789B57F
Internet: http:/ Fon: +49 (69) 79 Fax: +49 (69) 79	Hinweis: Die Nachricht wurde 0x4288B29914E21EDA, 0x23EE4	nit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:	20.02.2009	165A5F90 9347DB3C 48CC64C2 8EF041F1
		- absolutes V □ € Katrin Borcea <kati@inf.tu-dresden.de> -</kati@inf.tu-dresden.de>	er	289E7DB2 C4495AF0 F7C207CE ←
		<ul> <li>Nachricht unverschlüsselt und nicht unterschrieben senden</li> <li>Diesen Dialog nicht mehr anzeigen, wenn Verschlüsselung unmöglich ist</li> <li>Liste aktualisieren</li> <li><u>F</u>ehlende Schlüssel herunterladen</li> </ul>	ОК	Abbrechen

# OpenPGP: Decrypt Message

Von:       Katja Liesebach < katja.liesebach@m-chair.net>         Datum:       19:18         An:       Christian Kahl <christian.kahl@m-chair.net>         Charset:       ISO-8859-15         Version:       GnuPG v1.4.7 (MingW32)         Comment:       Using GnuPG with Mozil         hQEOAzxc3rss71RREAQAoa4NK8beV0v;       Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein         hQEOAzxc3rss71RREAQAoa4NK8beV0v;       Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein         hQEOAzxc3rss71RREAQAoa4NK8beV0v;       Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein         hQEOAzxc3rss71RREAQAoa4NK8beV0v;       Erst nach 5 Minut         foxXkLts6FkSbok5nKkM21147FB01rvWQ       Erst nach 5 Minut         //Omd5jC1R8N/NJeuSfsW6w1LUpTVHQQ       Erst nach 5 Minut         //Omd5jC1R8N/NJeuSfsW6w1LUpTVHQQ       Erst nach 5 Minut         //Mn2/s+Mn6AqNVnAdFJub8Vag2ZrEBd07YIfdH0oMBgga9X       Minut         //Mn2/s+Mn6AqNVnAdFJub8Vag2TumSd3v4PE021VBS4ag       Am: Christian Kahl <christian.kahl@m-chair.net>         //Mn2/s+Mn6AqNVnAdFJub8Vag2TumSd3v4PE021VBS4ag       Hi Christian,         //FJW5KXpqNFGyixn7wU61+e7d6Df8Q==       =        </christian.kahl@m-chair.net></christian.kahl@m-chair.net>	Datum: 19:18         An: Christian Kahl <christian.kahl@m-chair.net>        BEGIN PGP MESSAGE         Charset: ISO-8859-15         Version: GnuPG v1.4.7 (MingW32)         Comment: Using GnuPG with Mozil         hQEOAzxc3rSs71RREAQAoa4NK8beV0V;         IESWpm1xA11HIpTZ1K49ecdjV10F0J         6xtXLt56PK3b0K5nKtW21147F801rvM;         //md5jC1ReN/Nousf5%%w1L0pTVHQQ         2QAvcf2AvjqHHw401dKW8ewB3G642q0         Xxk0v1Ac+ADTcPgr5FvYPbpE1KS9D8dgzZEEBd07YIfdH00MEgga9;         JMwn2/s+Mn6AqNVhdFJuh8VaFvLW+up3G2+msGd3v4P8021VB54sc;         jCkaydXkKgr1INqr(391ty20tuolJaa+uPK2pq1A311DHEoqm8);         cFJW5KxpqNFGyixn7wU61+e7d6Df8Q==         ==Ekh        END FGP MESSAGE</christian.kahl@m-chair.net>	Betreff: MB II Slides	
Datum: 19:18         Am: Christian Kahl <christian.kahl@m-chair.net>        BEGIN PGP MESSAGE         Charset: ISO-8859-15         Version: GnuPG v1.4.7 (MingW32)         Comment: Using GnuPG with Mozil         hQEOAzxc3rSs71RREAQAoa4NK8beVOV         IESWpm1xA11HIpT2tIKd9ecdjV10F0J         6xtXtts6Pksb0k5nKMx21147F801rwn         /Omd5jCLR8M/NJeuSfsWeilLUpTVHQQ         QAvcf2AvjqHHw4UldKW8ewB3G64zqD         Xxk0viAc+ADTc9gF5FvYPbbEiKS9D8dgzZrEd07YIfdH00MEgga94         JMm2/s+Mn6AqNVhdPJuh8VaFvLW+up3G2+msGd3v4P8021VBS4sg         j0kaydJkxKqriLNqiY391ty2UtowJJaa+uPK2pqlA311DHEogm8         cFJW5KxpqNFGyixn7wU61+e7d6Df8Q==         =         =         DiplMedien-inf. Katja Liesebach</christian.kahl@m-chair.net>	Datum: 19:18         An: Christian Kahl <         Christian Kahl          Christian Kahl          Christian Kahl          Christian Kahl          OpenPGP-Engabe         Image: Status         OpenPGP-Engabe         Image: Status         OpenPGP-Engabe         Image: Status         Image: St	Von: Katja Liesebach <katja.liesebach@m-chair.net></katja.liesebach@m-chair.net>	
BEGIN FGP MESSAGE Charset: ISO-8859-15 Version: GnuFG v1.4.7 (MingW32) Comment: Using GnuPG with Mozill hQEOAzxc3rSs7IREEAQAoa4NK8beVOV iEsWpm1xA11HIpTZtIKd9ecdjV10F0J 6xkXLtS6PkSb0k5nKkM21147F80IrVWQ /Omd5jC1R8N/NJeuSfsW6w1LUpTVHQQ 2QAvcf2AvjqHHw4U1dKW8ewB3G64zqD XxkOviAC+ADTcPgF5FvYPbEiKS9D8dgzZrBd07YIfdH0oMBgga9x XxkOviAC+ADTcPgF5FvYPbEiKS9D8dgzZrBd07YIfdH0oMBgga9x JWWn2/s+Mn6AqNVhdPJuh6VaFvLW+up3C2+msGd3v4P802IVB54sq JOkaydJkxKqriLNgqiY39ltyZUtowlJaa+uPK2pqlA311DHEoqm8y cFJWSKxpqNFGyixn7wU6I+e7d6Df8Q== =eEkh END PGP MESSAGE DiplMedien-inf. Katja Liesebach	BEGIN PGP MESSAGE         Charset: ISO-8859-15         Version: GnuPG v1.4.7 (MingW32)         Comment: Using GnuPG with Mozil         hQEOAzxc3rS971RREAQAoa4NK8beVOV         iEsWpmixAllHIp7ZtIKd9ecdyVL0703         6xxXtL56Pk5b0k5nKkM21147F80IrvW         @ Est nach 5 Minut         @ Wort2AvjdHRH4U1dKW8ewB3G64zq01         XxkvolAC+ADTcPgFFvYPbEIKS9D8dgzZZFBd07YIfdH0oMEgga34         Min2/s+Mn6AqUVnAPUnBVaFVLH-up3C2+mseGd3v4P8021VB54sq         JOKaydJxxKgriLNgqiY391tyZUtovLJaa+uPK2pqL311DHEogm82         FUWSKXpqNFGyixn7wU6I+e7d6Df8Q==         eEEkh        END PGP MESSAGE         Dip1Medien-inf. Katja Liesebach         Johann Wolfgang Goethe University Frankfurt a. M.         Institute of Business Informatics         Chainers of Multile Business and Multilateral Security         Graefstr. 78, D-60486 Frankfurt a. M., Germany         Internet: http://m-chair.net		
Charset: ISO-8859-15 Version: GnuPG v1.4.7 (MingW32) Comment: Using GnuPG with Mozill hQEOAzxc3rSs7lRREAQAoa4NK8beVOV iEsWpm1xA11HIpT2tIKd9ecdjVlOFOJ 6xkXLc56PkSb0k5nKkM21147F80IrvWi //md5jClR8N/NJeuSfsW6w1L0pTVHQQ 2QAvcf2AvjqHHw4UldKW8ewB3GG4zqD Xxk0viAC+ADTcPgF5FvYPbEiKS9D8dgzZrBd07YIfdH00MEgga9 JMWn2/s+Mn6AqNVhdPJuh8VaFvLW+up3G2+msGd3v4P8021VBS4sd jOkaydJkxKqriLNgqiY391tyZUtow1Jaa+uPK2pqlA311DHEoqm8 cFJW5KxpqNFGyixn7wUGI+e7d6Df8Q== =eEkh END PGP MESSAGE DiplMedien-inf. Katja Liesebach	Charset: ISO-8859-15 Version: GnuPG v1.4.7 (MingW32) Comment: Using GnuPG with Mozil hQEOAzxc3rSs71RREAQAoa4NK8beVOV; iEsWpnixAlHHIpTZIKK9ecdjVlOFOJ; WErstnach 5 Minut Werstnach	An: Christian Kahl <christian.kahl@m-chair.net></christian.kahl@m-chair.net>	
	Internet: http://m-chair.net Fon: +49 (69) 798-25313	Charset: ISO-8859-15 Version: GnuPG v1.4.7 (MingW32) Comment: Using GnuPG with Mozill hQEOAzxc3rSs71RREAQAoa4NK8beVOV: iEsWpm1xA11HIpTZtIKd9ecdjV10F0J; 6xkXLtS6PkSb0k5nKkMZ1147F80IrvWH /Omd5jC1R8N/NJeuSfsW6w1LUpTVHQQ zQAvcf2AvjqHHw4UldKW8ewB3GG4zqDl XxkOviAC+ADTcPgF5FvYPpbEiKS9D8dgzZrBd07YIfdH0oMBgga9k JMWn2/s+Mn6AqNVhdPJuh8VaFvLW+up3GZ+msGd3v4P80Z1VBS4sq jOkaydJkxKqriLNgqiY391tyZUtowlJaa+uPK2pqlA311DHEoqm8y cFJW5KxpqNFGyixn7wU6I+e7d6Df8Q== =eEkh	DenPGP-Passphrase oder SmartCard-PIN ein          Betreff: MB II Slides         Von: Katja Liesebach <katja.liesebach@m-chair.net>         Datum: 19:18         An: Christian Kahl <christian.kahl@m-chair.net>         Hi Christian,         please find attached the MB II slides for lecture 7.         DiplMedien-inf. Katja Liesebach         Johann Wolfgang Goethe University Frankfurt a. M.         Institute of Business Informatics</christian.kahl@m-chair.net></katja.liesebach@m-chair.net>
			Fon: +49 (69) 798-25313



#### 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

ge Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten:			Alle <u>z</u> eig	en						
Benutzer-ID	Vertrauen	Ablauf-D.	Тур	Ę						
Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um z	abgelaufen	02.09.2006	öffentli	ch 🔺						
Alexander Boettcher <ab764283@inf.tu-dresden.de></ab764283@inf.tu-dresden.de>	absolutes Vert	trauen	öffentli	ch 🗐						
Alexander Boettcher <ab764283@os.inf.tu-dresden.de></ab764283@os.inf.tu-dresden.de>	abgelaufen	11.10.2005	öffentli	ch 🛛						
Andre Meixner <s4538672@inf.tu-dresden.de></s4538672@inf.tu-dresden.de>	-		öffentli	ch						
Andreas Albers <andreas.albers@m-lehrstuhl.de></andreas.albers@m-lehrstuhl.de>	absolutes Vert	trauen	öffentli	ch						
Andreas Pfitzmann <pfitza@inf.tu-dresden.de> NO LEGAL RELEVANCE</pfitza@inf.tu-dresden.de>	absolutes Vert	trauen	öffentli	ch 📃						
André Deuker <andre.deuker@m-lehrstuhl.de></andre.deuker@m-lehrstuhl.de>	absolutes Ve	Schlüsseleigen	chaften							
Birgit Pretscheck <birgit.pretscheck@gmx.net></birgit.pretscheck@gmx.net>	-									
Christian Kahl < christian.kahl@m-lehrstuhl.de>	absolutes Ve	Primäre Beni	ıtzer-ID	Christian Kahl <	e a la sila tina.	a habl@ea lab	unturbal alles			
⊞ Denis Royer < me@myasterisk.de>		Fillingle Deligizer-1D		Christian Kani «	christia	n.kani@m-ien	rstuni.de>			
ra Koch <elvira.koch@m-lehrstuhl.de> volles Vertra Schlüssel-ID</elvira.koch@m-lehrstuhl.de>		[	0x14E21EDA							
<ul> <li></li></ul>			l							
		Тур		öffentlich						
		e Vertrauen Besitzer-Vertrauen		absolutes Vertrauen						
							absolutes Vertra	auen		
							Fingerabdru	k [	FICC 3445 BCF	R2 4524 P
				Marco Lehmann <m99@gmx.li></m99@gmx.li>	-			Lice shirts bei		502 0005 42
		Mathias Staab <mathias.staab@arcor.de></mathias.staab@arcor.de>	-	Тур	ID	Algo	Stär	Erzeugt	Ablauf-Datum	
Mike Beramann (dienstlich. TU Dresden, unbeschrnkt altia) <mb41@inf.t< td=""><td>-</td><td>Unterschlü</td><td></td><td>98F0 ELG</td><td>2048</td><td>07.09.2007</td><td>-:-</td></mb41@inf.t<>	-	Unterschlü		98F0 ELG	2048	07.09.2007	-:-			
		Unterschil	issei 0x	OFU ELU	2048	07.09.2007	nie			

	Op	enPGP-Schlüssel herunterladen		_
	ſ	Schlüssel gefunden - Auswählen zum Importieren		
		Benutzer-ID	Erstellt	Schlüssel-ID
		<ul> <li>➡ Kai R. Rannenberg &lt; kair@microsoft.com&gt;</li> <li>➡ kara &lt; kara@iig.uni-freiburg.de&gt;</li> <li>➡ kara &lt; kara@telematik.iig.uni-freiburg.de&gt;</li> </ul>	1997-03-09 1997-09-18 1997-03-09	
Schlüssel-Server auswähle Suche nach Schlüssel	en Kai Rannenber			
Schlüssel-Server	subkeys.pgp.nd	et 🔹 Abbrechen		
			0	K Abbrecher



23

# PGP: Public Key Catalogs

Public	Key Server Verb	ose Index ``Kai Rannenberg " - Microsoft Internet Explorer 📃 🔲
<u>File E</u> dil	t <u>V</u> iew F <u>a</u> vorites	Iools Help
🕁 Back 🕓	• • • 🙆 😰 🖞	🖞 🔞 Search 📷 Favorites 🎯 Media 🧭 🖏 - 🚔 🔯 - 🗐 🖓
Address 🥉	http://blackhole.pd	:a.dfn.de:11371/pks/lookup?op=vindex&search=Kai+Rannenberg
- 1.		
Pul	blic Key	Server Verbose Index ``Kai Rannenberg ''
Type k	oits/keyID	Date User ID
	-	1997/09/18 kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
sig	0B6375FD	Matthias Schunter <schunter@acm.org></schunter@acm.org>
sig	D5CDE083	Herbert Damker <damker@iig.uni-freiburg.de></damker@iig.uni-freiburg.de>
sig	879AC041	Birgit Pfitzmann 1 < <u>pfitzb@informatik.uni-hildesheim.de</u> > NO LEGAL RELEVANCE
sig	8128DC75	Gerhard Weck <73064.2271@compuserve.com>
sig	8EF041F1	Kai R. Rannenberg 2048 < <u>kara@iig.uni-freiburg.d</u> e>
sig	2F8D5039	Kai Martius <kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de>
sig	5C3C4FE4	Holger Reif <reif@prakinf.tu-ilmenau.de></reif@prakinf.tu-ilmenau.de>
sig	AF1FDF70	kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
sig	49EF1D84	Hannes Federrath < <u>federrath@inf.tu-dresden.de</u> >
		Kai R. Rannenberg < <u>kair@microsoft.com</u> >
sig	0B6375FD	Matthias Schunter < <u>schunter@acm.org</u> >
sig	AEB4BCDD	fapp2_AEB4BCDD_HSK < <u>fapp2@cam.ac.uk</u> >
sig	AF1FDF70	kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
sig	<u>044584B5</u>	Douglas Swiggum < <u>Swiggum@Waisman.Wisc.Edu</u> >
		Kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> >
sig	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> >
(		<b>   &gt;</b>

- 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)

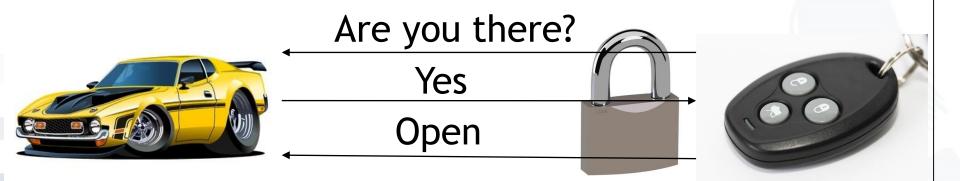
[Marshall Symposium 1998] [Randell 2004]







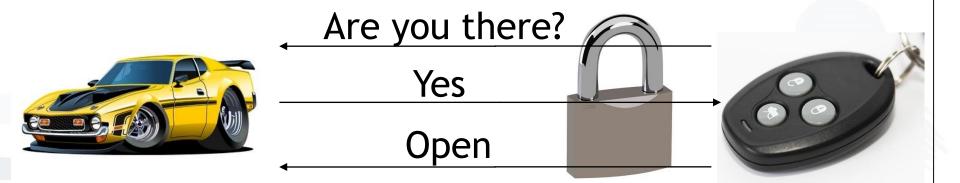
- Solution: Protect communication with crypto?
- e.g. symmetric cryptography + hash/signature

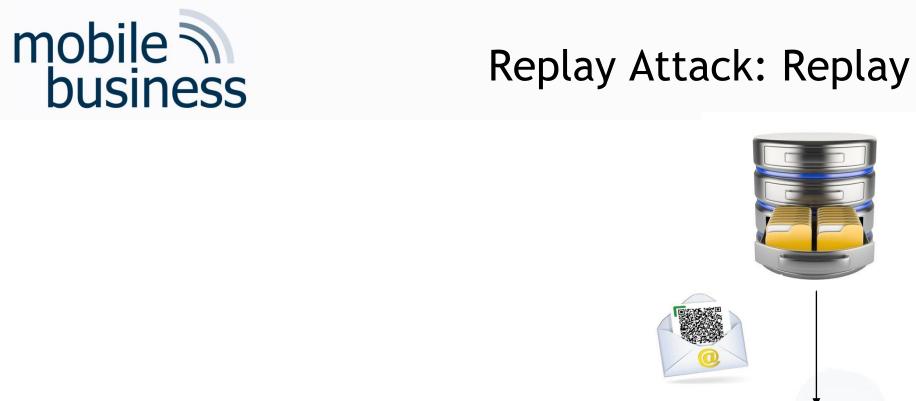


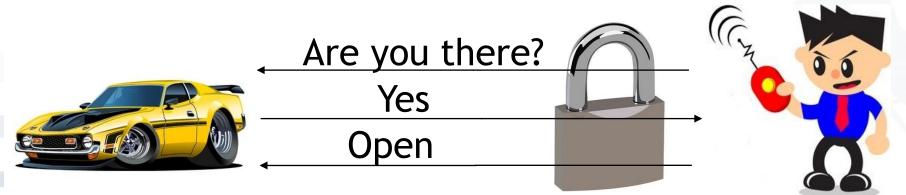
# Replay Attack: Eavesdrop

# mobile business





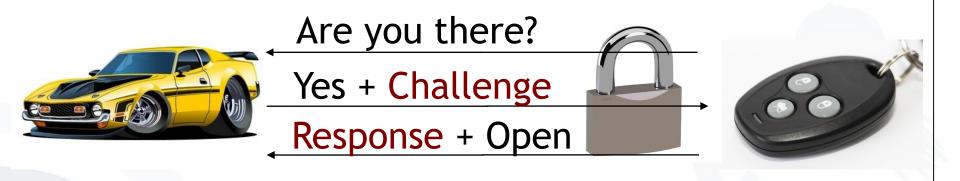


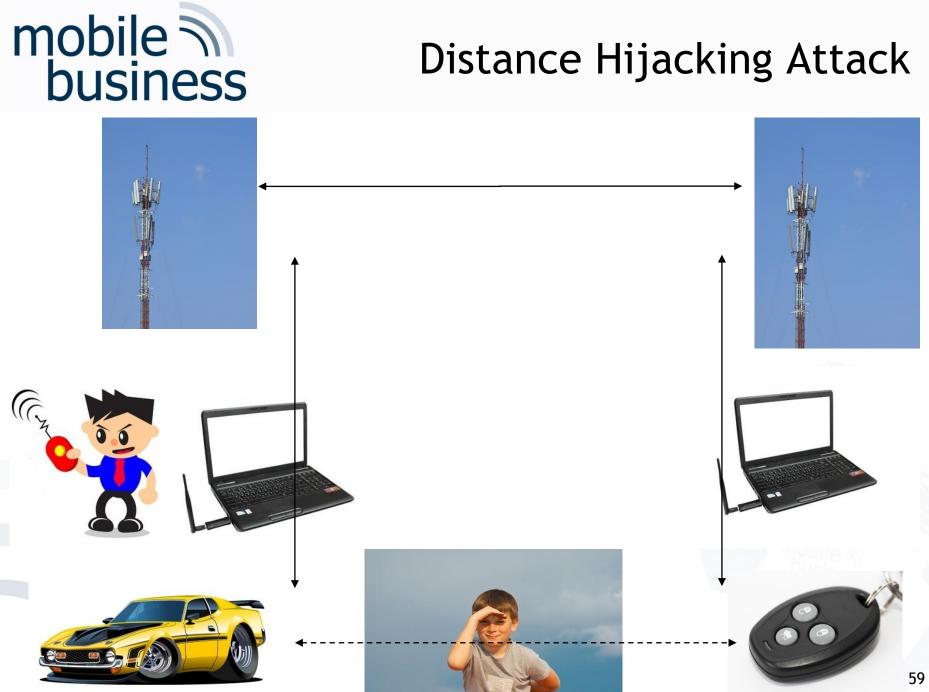




# Replay Attack: Solution

e.g. Challenge-Response helps



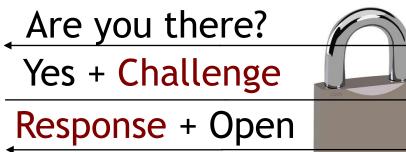




# Distance Hijacking Attack: Solution

Distance-Bounding Protocol



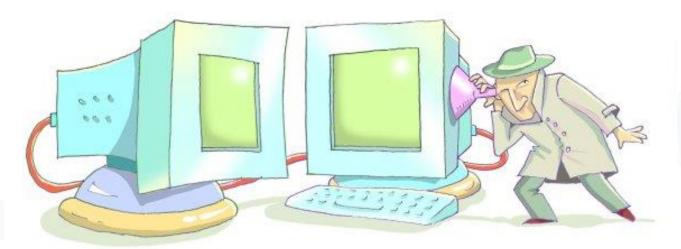






## Side-Channel Attacks I

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

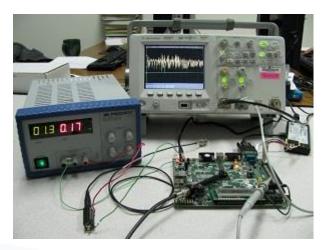


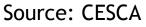
Source: Eran Tromer

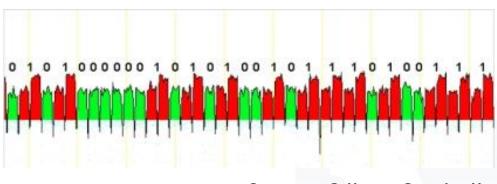


# Side-Channel Attacks II

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





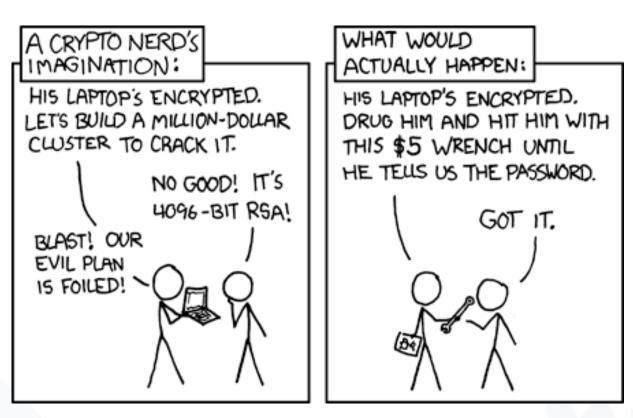


Source: Gilbert Goodwill

- 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



- 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.
- 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