

Lecture 4

Cryptography



Mobile Business II (SS 2023)

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



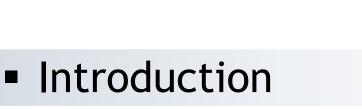


- Introduction
- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES
 - Advantages and Problems
- Public Key Cryptography



Symmetric Encryption Systems

- Classical cryptosystems are usually based on symmetric encryption systems.
- 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: Data 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

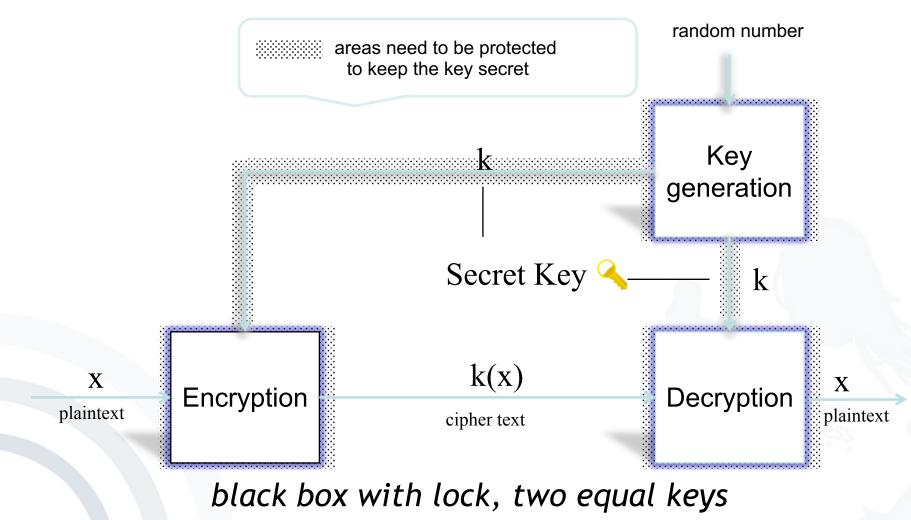


- Symmetric Cryptosystems
 - General Concept
 - Caesar Cipher
 - AES

- Advantages and Problems
- Public Key Cryptography

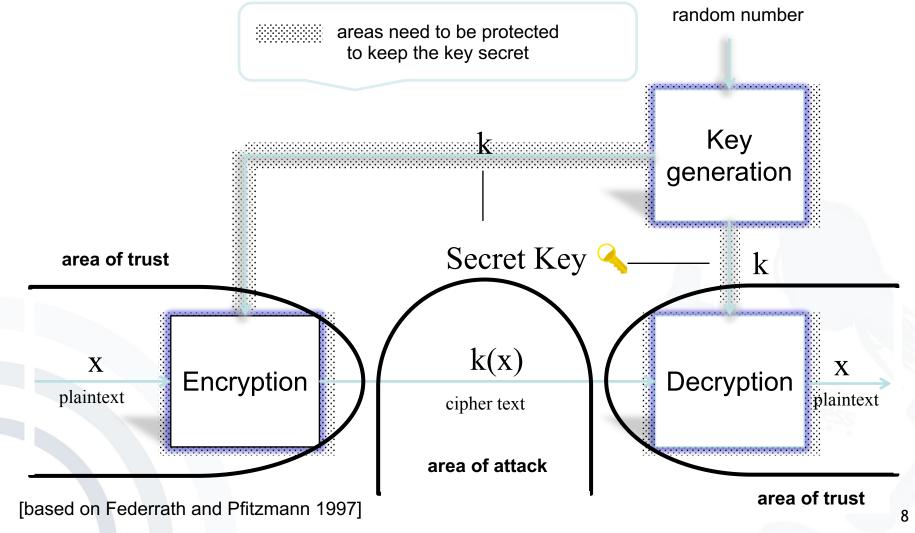


Symmetric Encryption Systems (1)



[based on Federrath and Pfitzmann 1997]

mobile Symmetric Encryption Systems (2)





- 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

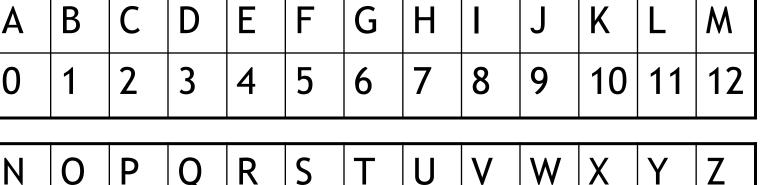
Introduction

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





Caesar Cipher



18 19 20 21 22 23 24 25

We assign a number for every character.

17

16

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

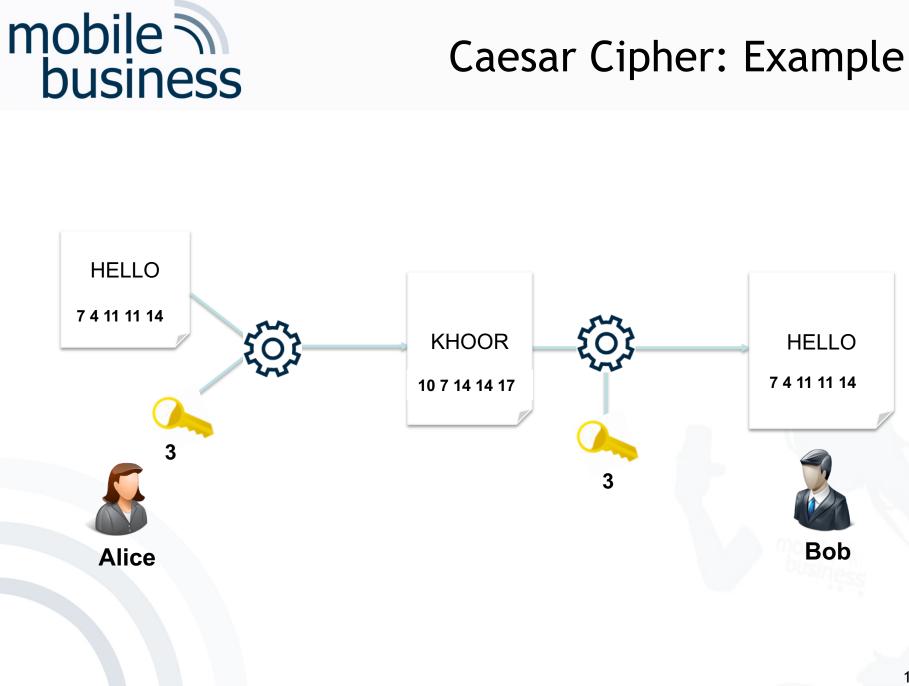
15

14

mobile

13









- 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

mobile business

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





Advanced Encryption Standard

- The Data Encryption Standard (DES) was designed to encipher sensitive but not classified data.
- The standard has been issued in 1977.
- In 1998, a design for a computer system and software that could break any DES-enciphered message within a few days was published.
- By 1999, it was clear that the DES no longer provided the same level of security it had 10 years earlier, and the search was on for a new, stronger cipher.
- AES Rijndael was a winner of U.S. National Institute of Standards and Technology bid for advanced encryptions.
- 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

mobile business

- Advantages and Problems
- Public Key Cryptography





Symmetric Encryption

Advantage: Algorithms are very fast

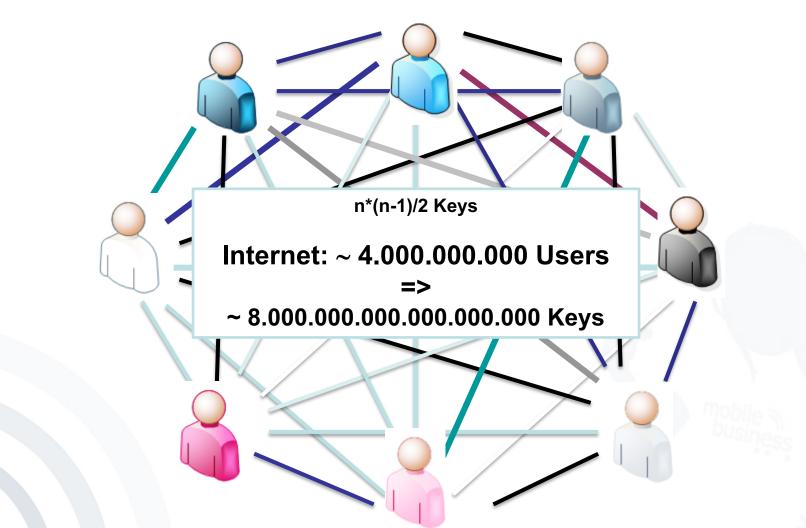
Algorithm	Performance*		
RC6	78 ms		
SERPENT	95 ms		
IDEA	170 ms		
MARS	80 ms		
TWOFISH	100 ms		
DES-ede	250 ms		
RIJNDEAL (AES)	65 ms		

* 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

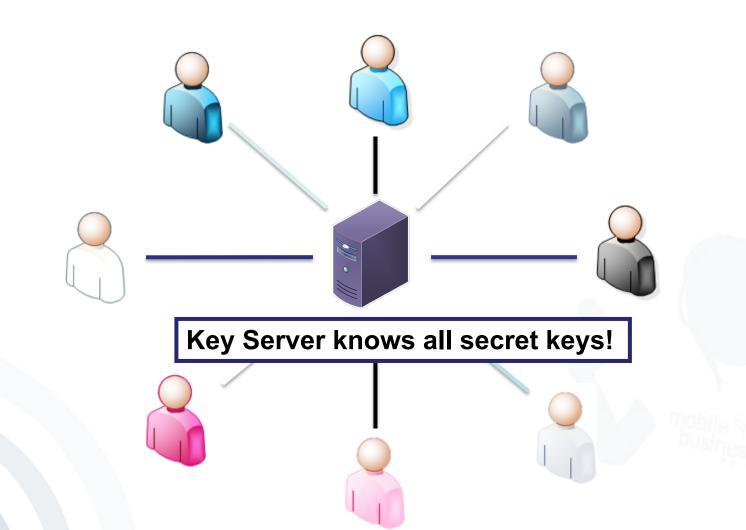




[adopted from J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Symmetric Encryption: A Possible Solution



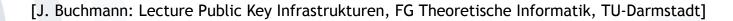


[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

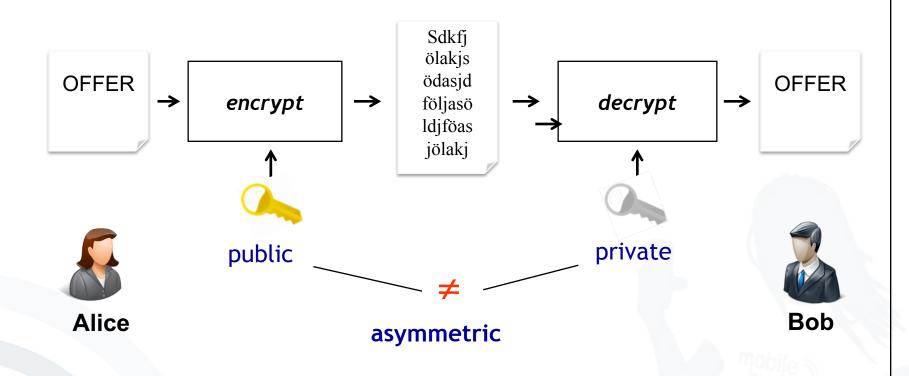


- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Digital Signature
 - Key Management
 - Example: PGP

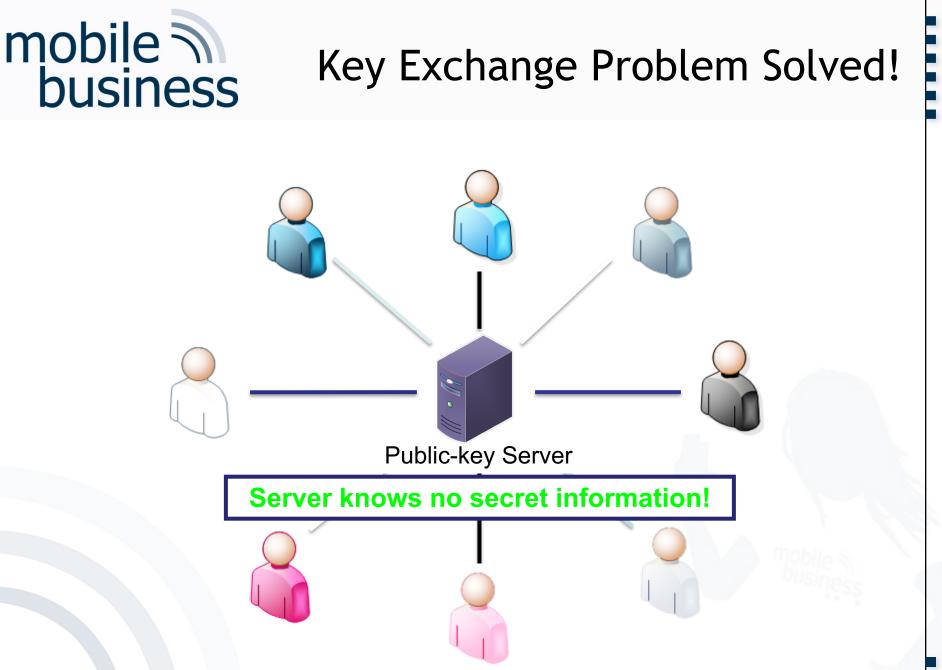




Public Key Encryption



mobile business



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



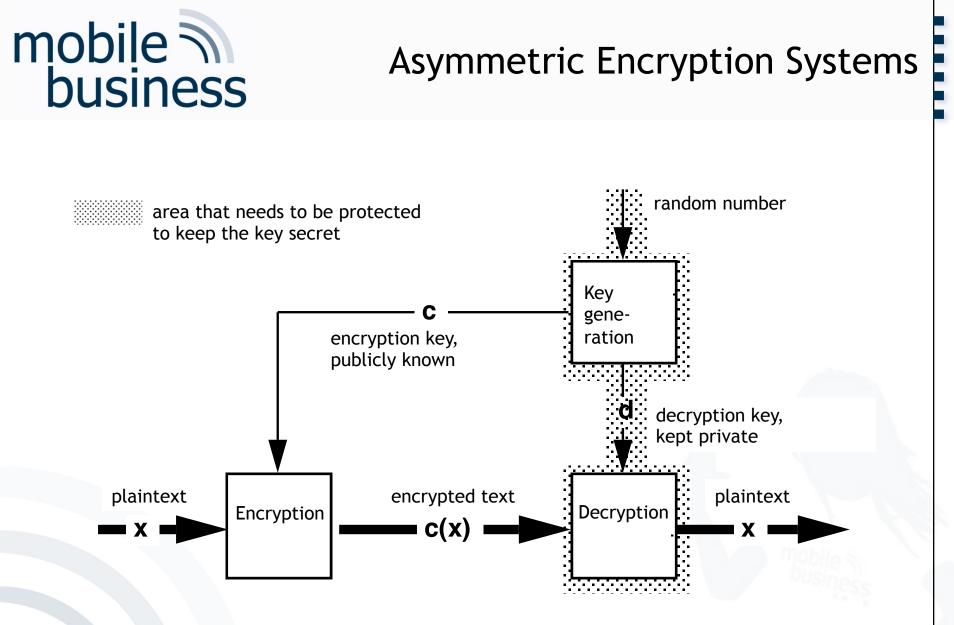
- Introduction
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Digital Signature
 - Key Management
 - Example: PGP





Concept of Asymmetric Encryption Systems

- Public key systems are based on asymmetric encryption.
- 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

mobile business

- 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

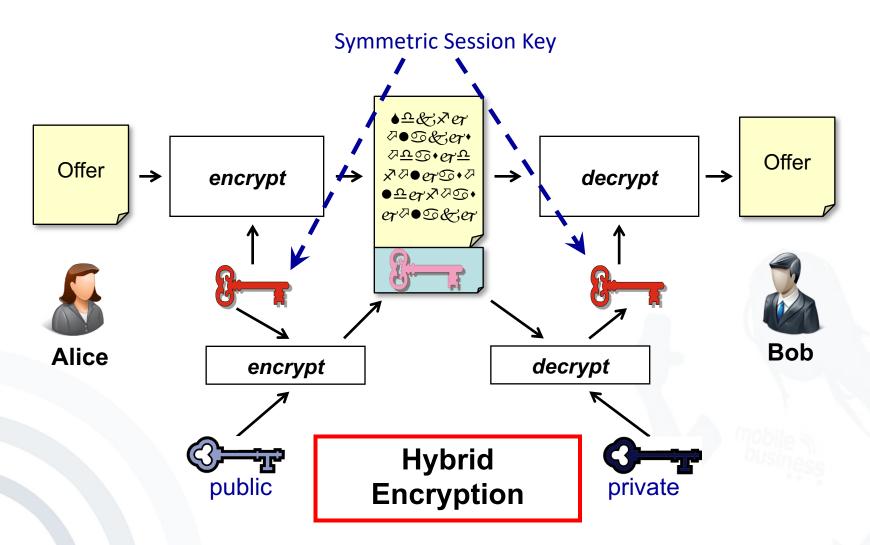
 \Rightarrow Algorithms are very slow.

* 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



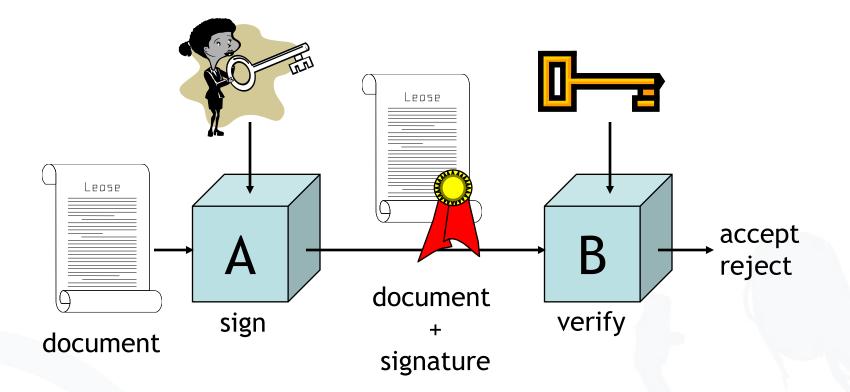
[based on: J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Introduction

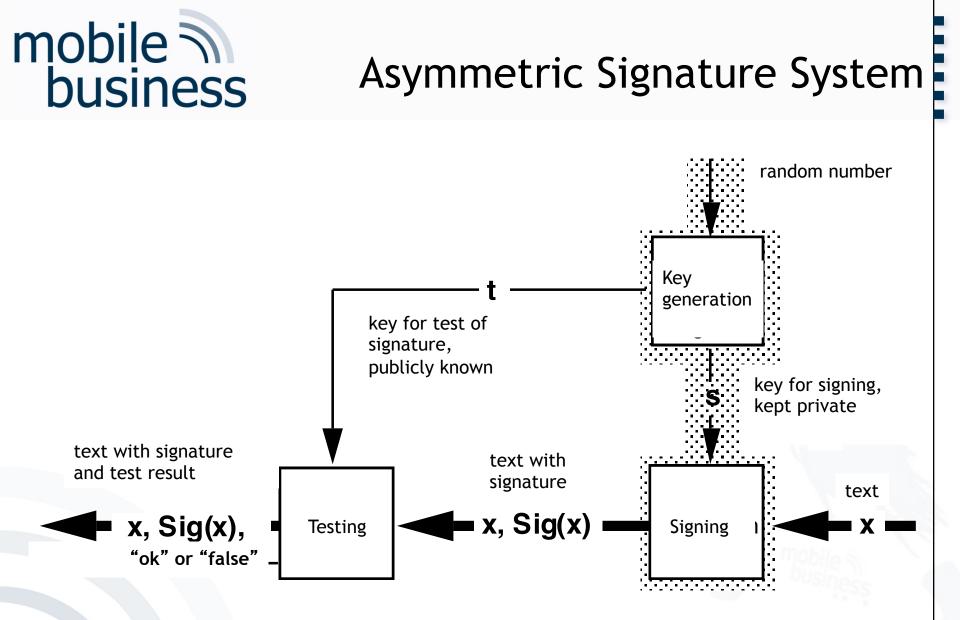
- Symmetric Cryptosystems
- Public Key Cryptography
 - General Concept
 - Algorithms
 - Hybrid Systems
 - Digital Signature
 - Key Management
 - Example: PGP



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

1	(lausur N	1C1 - Nachricht - Microsoft Word					
	9 - 19 7 9	arbeiten <u>A</u> nsicht Einfügen Forma <u>t</u> E <u>x</u> tras Tabelle <u>F</u> enster <u>?</u>		Frage hier eingeben	• ×		
f) 🚅	🗗 🔁 🖾 🖤 % 🖻 🛍 🚿 ∽ + ↔ - 🐁 🗗 🗔 💷 🐻 🖾					
4	Nur Tex	t → Courier New → 10 → F K 및 = = = ‡= + ‡= !=	∉∉∎• <u>∡</u> • <u>∧</u> •.				
En	dgültige V	ersion enthält Markups - Anzeigen - 🚳 🐨 - 🗞 - 🖄 - 🏠 -	월 PGPtray - Key Selection	n Dialog			<u>?</u> ×
I] <u>S</u> enden	Konten • 🖉 • 📴 🎭 🌻 🌲 💘 📰 Optionen • Nur-Text 🔹	Drag users from this list to th	ne Recipients list	Validity	Size	
E - 30		A set of characteristic fraction of the former set of the former s	📧 Andreas Albers <andreas.< td=""><td></td><td>•</td><td>2048/1024</td><td></td></andreas.<>		•	2048/1024	
1	An	Jan Muntermann;	Elvira Koch <elvira.koch@< td=""><td>)M-Lehrstuhl.de></td><td>•</td><td>3096/1024</td><td></td></elvira.koch@<>)M-Lehrstuhl.de>	•	3096/1024	
Œ	Cc		📧 fritsch		0	1024	
Be	reff:	Klausur MC1	📧 fritsch@dfki.uni-sb.de		0	1024	
			Fritsch@fsinfo.cs.uni-sb.de		•	1024	
	Hallo		Fritsch@pfsparc01.phil15.	uni-sb.de	0	1024	
	iviy ex	kercises for the "MC1" test are enclosed:	Fritsch@phil.uni-sb.de		9	1024	
	heiko	rossnagel heiko.rossnagel@m-lehrstuhl.de	Heiko Rossnagel <heiko.ro< td=""><td></td><td>•</td><td>1024/1024</td><td></td></heiko.ro<>		•	1024/1024	
			📧 Kai Rannenberg <kai.rannenberg@m-lehrstuhl.de></kai.rannenberg@m-lehrstuhl.de>			2048	-
		str. 78 fax: -25306 54 frankfurt www.m-lehrstuhl.de	Colling Rappenberg Kai Rapi	nenhera(a)m-lehrstuhl de >		2048/1024	
			Contract.		Validity	Size	
	PGF	Ptray - Enter Passphrase		ossnagel@m-lehrstuhl.de>		2048/1024	
70				ma@wiwi.uni-frankfurt.de>	•	1024	
Ze Se	S	igning key : Heiko Rossnagel <heiko.rossnagel@m-lehrst< td=""><td> (DSS/1024 💌</td><td></td><td></td><td></td><td></td></heiko.rossnagel@m-lehrst<>	(DSS/1024 💌				
	E	nter passphrase for above key:	🔽 Hide Typing	ОК	Car	ncel	Help
				n			
		OK	Cancel				
	100000000						34

Example PGP: Decrypt and Check a Message

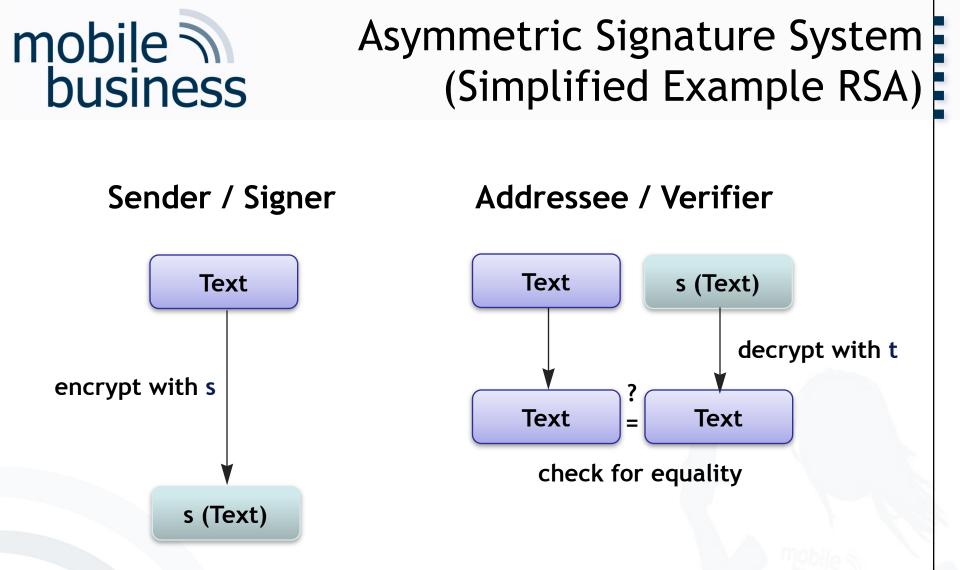
Von: Heiko Rossnagel	An: J	Jan Muntermann			
Betreff: Klausur MC1	Cc:	PGPtray -	Enter Passphrase		? ×
BEGIN PGP MESSAGE		Massage	was encrypted to the following	nublia kau(a) :	
Version: PGP 8.0 - not licensed for comm	ercial use: www.	pgp			
		20222	ssnagel <heiko.rossnagel@m-le< td=""><td></td><td></td></heiko.rossnagel@m-le<>		
hQCMA5/VPPIP3satAQP+LqxvxFSk4G/TAexpMLX4	36biwBp6xP8pa89R	7ro, Jan Munte	ermann <munterma@wiwi.uni-fr< td=""><td>ankfurt.de> (RSA/1024)</td><td></td></munterma@wiwi.uni-fr<>	ankfurt.de> (RSA/1024)	
uHEs07/tFrJFQJpPBcUWouy47p4sR2F0+IXqJuJy	Hp5ExMGIdmQCpGXE	osz:			
B5TXKtUB8YJdpPnck61as78RBP1sq8VDrA1YopEA	eqMMw2pkBuoxyo3K	CIR			
Ag4DIYlowhVX6ZwQCAD2L9WAA97xEUBWMET6kR9n	5+oafTBF+R01v6UO	22T			
Alkh23iQOlI9Drye/uygpcQpT2HhTtZY1AjjudLv	i+GsegOlWmBjY8q8	G1Y Enter pass	phrase for your private key :		Hide Typing
kDP3GEanyDiDU6R9F1XFOvxPNMk6Ek8hH6qZ37hh	DNDCXkxkSjM3nJ2V	'uuL			
uOuXNA9iAC96dhg7NpvzCJI2J7xRMtuBc9BUI8LX	ODrvGLwnLtaD5+Ev	gL1:			
dfvQ3NiGrUEQsOHVxwjQdMtr8C09kREYLuAdD7j/	O5WtsAdbAVMn72PY	FOI			
i77MitBfAbxXF0gFS7/b2LccbaK8fx6e1VNFnV07	B/9qpd0Gg5WZVP2e	QA5:			
h2oTOSjWCRp/v5s9Og1aUtcAxd1RAjQPHpVsFS2e	XXMnC9ZZvNIFMh6K	tom		ок	Cancel
m39jRjPE90b/HLjMwPAXUHyneh9QrCX1X5qHORNc	jIYVrnQyZGIk8t39	0591			Cancel
cr1rhf6ht7SwGgfgGW2aL8HyiFFWDC6mileTFwma	ifaali.fff00T~40	(PALINING)		· · ·	
E1IJGt9QLiwMmXormxcOg+WR2I: Text Viewer					
NjwtR+1SkqMCXs+PzcAHDsiuGz [,]		NTTON NYY			
pE3huhK5cfvu1Ug7+Oa9SUAy4J] *** Status:	Good Signat	ure from '	Valid Kev		
NZncI3vJgkZeZrlbh+pi4dRjs01 *** Signer:	Heiko Rossn		ko.rossnagel@m-l	ehrstuhl.de>	
=hCO9 (0x85964FC9					
END PGP MESSAGE **** Signed:	26.02.2004	11:40:49			
	d: 26.02.2004				
heiko rossnagel *** BEGIN P	<u>GP DECRYPTED/V</u>	/ERIFIED M	ESSAGE ***		
frankfurt direkt:					
-25306 D-60054 frankfurt Hallo Jan.					
My exercise	s for the "MC1"	test are encl	osed.		
IVIY EXCICISE			osed.		
AND DOD	DECOUDTED (UPP	TETER VEC			
*** END PGP	DECRYPTED/VER	(IFIED MES)	DAGE ***		
			1		1
			Copy to Clipboard	<u>o</u> k	

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.



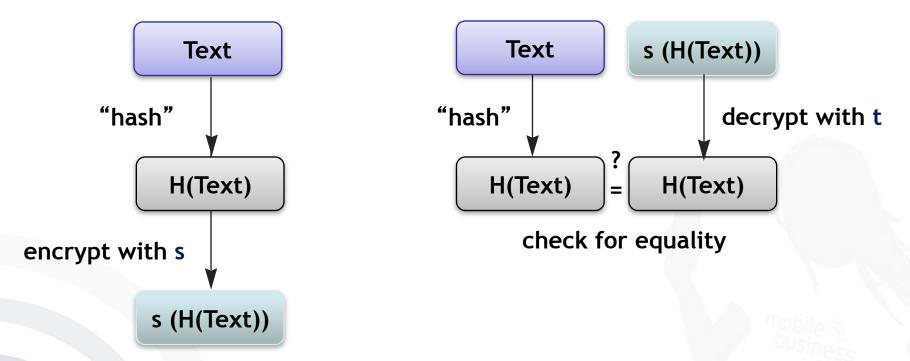
Signing key s only with the sender, test key t public
 Example is often mistakenly generalized.



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



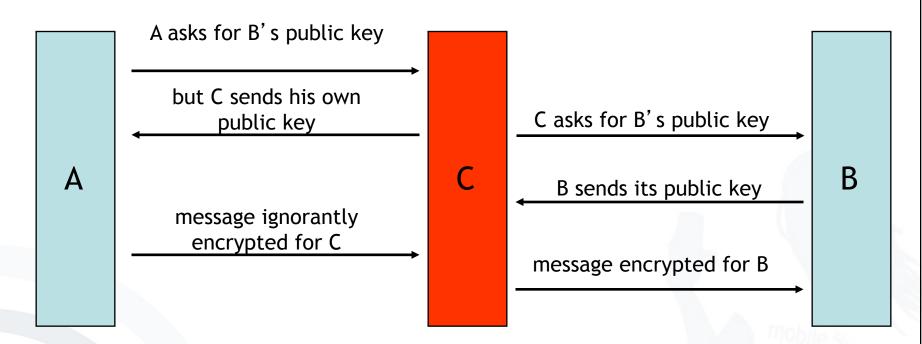
Introduction

- 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)

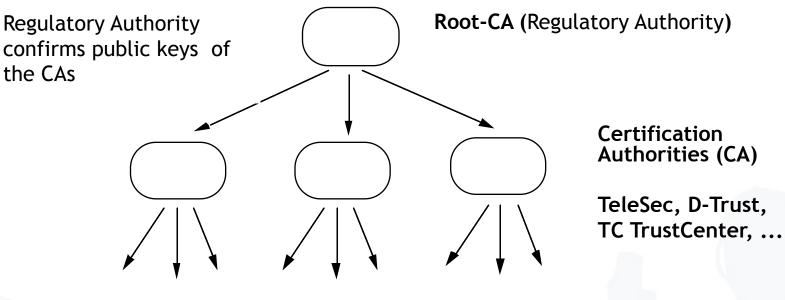
Three types of organization for certification systems (PKIs?):

- 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

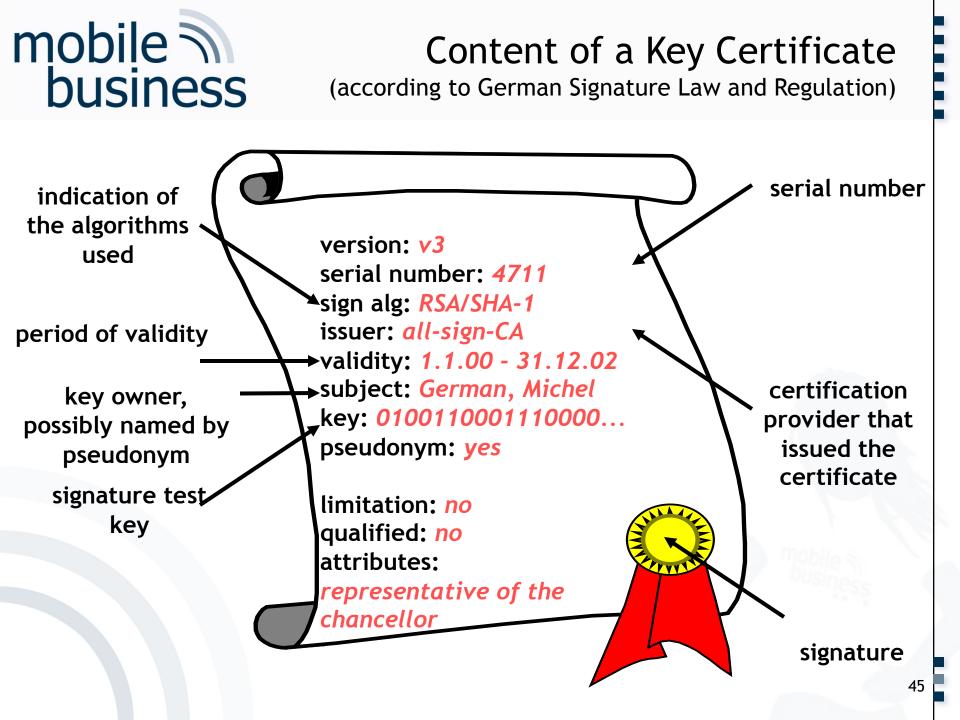
(Example: German Signature Law)



persons

organizations

- 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





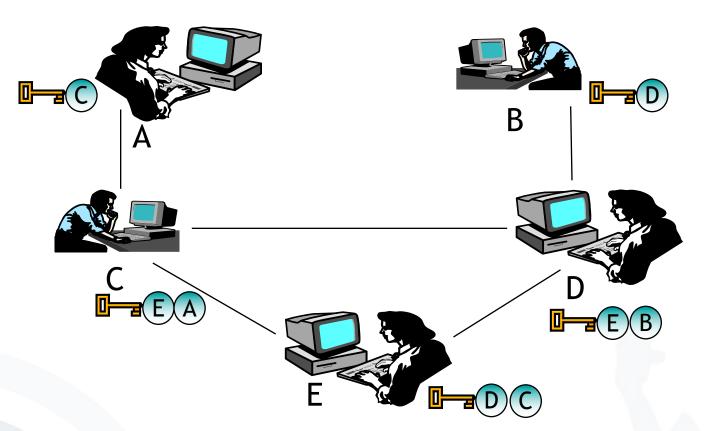
- Checking of the following items by certain confirmation centers (BSI, TÜVIT, ...)
 - Concept of operational security
 - Reliability of the executives and of the employees as well as of their know-how
 - Financial power for continuous operation
 - Exclusive usage of licensed technical components according 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



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

enden Kontakte			S/MIME Speichern				
on: Katja Liesebach	h <katja.liesebach@m-chair.net> - ka</katja.liesebach@m-chair.net>	OpenP(iP-Schlüssel auswählen	100			
- An: E	Christian Kahl < christian.kahl@m-le		ht gefundene Empfänger				
		⊂ Em	ofänger für Verschlüsselung wählen				
etreff: MB II Slides			Benutzer-ID	Vertrauen	Ablauf	Schlüssel-ID	C,
			Christian Kahl <christian.kahl@m-lehrstuhl.de></christian.kahl@m-lehrstuhl.de>	absolutes Ver		14E21EDA	
i Christian,			Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um zu.		02.09.2006	8D539C6E	i
assa find atta	ched the MR II slides for lest		Alexander Boettcher <ab764283@inf.tu-dresden.de></ab764283@inf.tu-dresden.de>	-		A63325B3	
lease find attached the MB II slides for lect			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	
plMedien-inf	OpenPGP-Bestätigung			-		52B1B05D	Ξ
No. 16.				-		A0D40924	
hann Wolfgang Stitute of Bus	VERSCHLÜSSELTE Nachricht ar	in folgend	e Empfänger senden:	-		79B42C58	
hair of Mobile	christian.kahl@m-lehrstuhl.de			-		B06F3816	
raefstr. 78, D-				-		0789B57F	
			e>	-	11.04.2011	165A5F90	
ternet: http:/	Hinweis: Die Nachricht wurde n 0x42B8B29914E21EDA, 0x23EE4E		nden Benutzer-IDs / Schlüsseln verschlüsselt:	-		9347DB3C	
on: +49 (69) 79	0x42b6b29914E21EDA, 0x25EE4L	0900449.	Aro	-	20.02.2009	48CC64C2	
ax: +49 (69) 79		Ja	Nein	-		8EF041F1	
		<u>.</u>		-		289E7DB2	
	1		Katja Liesebach < katja.iiesebach@m-chair.net>	absolutes Ver		C4495AF0	
			🗉 Katrin Borcea <kati@inf.tu-dresden.de></kati@inf.tu-dresden.de>	-		F7C207CE	-

OpenPGP: Decrypt Message



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

ige Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten:		[Alle <u>z</u> eig	en			
Benutzer-ID Alexander Boettcher ("Nur wenige wissen, wie viel man wissen muss, um z	Vertrauen abgelaufen	Ablauf-D	Typ öffentlig	t,			
Alexander Boettcher (Nor Wenge Wissen, We vier nor Wissen mass, um 2 Alexander Boettcher							

Schlü

OpenPGP-Schlüssel herunterladen

	Schlüssel gefunden - Auswählen zum Importieren			
	Benutzer-ID	Erstellt	Schlüssel-ID	Ę
	□	1997-03-09	8EF041F1	
		1997-09-18	AF1FDF70	
		1997-03-09	6623E0DD	
lüssel-Server auswählen uche nach Schlüssel Kai Rannenber				
chlüssel-Server subkeys.pgp.n	et Abbrechen			
		0	K Abbr	rechei

Key-Server



X

PGP: Public Key Catalogs

le Edt ywe Ravortes Iool Heb Back + + · · · · · · · · · · · · · · · · ·	Public Key Server Ver	bose Index ``Kai Rannenberg " - Microsoft Internet Explorer
if http://blackhole.pca.din.de:11371/pls/hookup?op=windex&search=Kai+Rannenberg Image: Content of the state of the		
Public Key Server Verbose Index ``Kai Rannenberg '' Type bits/keyID Date User ID Dub 1024/AFIFDF70 1997/09/18 kara <kara@iig.uni-freiburg.de> Dig 0E6375FD Mathias Schunter <schunter@acm.org> Dig 0502003 Herbert Damker <damker@iig.uni-freiburg.de> Dig 05020041 Birgit Pfitzmann 1 <pre>/// fitzb@informatik.uni-hildesheim.de> No LEGAL RELEVANCE Dig 079AC041 Birgit Pfitzmann 1 <pre>// fitzb@informatik.uni-freiburg.de> Dig 0279D5039 Kai R. Rannenberg 2040 Kara@iig.uni-freiburg.de> Dig 279D5039 Kai Martius <kai@imib.med.tu-dresden.de> Dig 49F104 Hannes Federrath <federrath@inf.tu-dresden.de> Dig 0E6375FD Mathias Schunter <schunter@acm.org> Mathias Schunter <schunter@acm.org> Dig 0E6663F Martin Reichenback <marel@iig.uni-freiburg.de> Mig 0E6675FD Mathias Schunter <schunter@acm.org> Mati Reichenback <marel@iig.uni-freiburg.de> Mig 0E6663F Martin Reichenback <marel@iig.uni-freiburg.de> <</marel@iig.uni-freiburg.de></marel@iig.uni-freiburg.de></schunter@acm.org></marel@iig.uni-freiburg.de></schunter@acm.org></schunter@acm.org></federrath@inf.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></pre></pre></damker@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de>	🖙 Back 🔹 🔿 🗸 🙆 💋	🔐 🔞 Search 📾 Favorites 🛞 Media 🧭 🛃 + 🎒 🔕 + 📃 🖓
Public Key Server Verbose Index ``Kai Rannenberg '' Type bits/keyID Date User ID Dub 1024/AFIFDF70 1997/09/18 kara <kara@iig.uni-freiburg.de> Dig 0E6375FD Mathias Schunter <schunter@acm.org> Dig 0502003 Herbert Damker <damker@iig.uni-freiburg.de> Dig 05020041 Birgit Pfitzmann 1 <pre>/// fitzb@informatik.uni-hildesheim.de> No LEGAL RELEVANCE Dig 079AC041 Birgit Pfitzmann 1 <pre>// fitzb@informatik.uni-freiburg.de> Dig 0279D5039 Kai R. Rannenberg 2040 Kara@iig.uni-freiburg.de> Dig 279D5039 Kai Martius <kai@imib.med.tu-dresden.de> Dig 49F104 Hannes Federrath <federrath@inf.tu-dresden.de> Dig 0E6375FD Mathias Schunter <schunter@acm.org> Mathias Schunter <schunter@acm.org> Dig 0E6663F Martin Reichenback <marel@iig.uni-freiburg.de> Mig 0E6675FD Mathias Schunter <schunter@acm.org> Mati Reichenback <marel@iig.uni-freiburg.de> Mig 0E6663F Martin Reichenback <marel@iig.uni-freiburg.de> <</marel@iig.uni-freiburg.de></marel@iig.uni-freiburg.de></schunter@acm.org></marel@iig.uni-freiburg.de></schunter@acm.org></schunter@acm.org></federrath@inf.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></pre></pre></damker@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de>	Address 🖉 http://blackhole.i	oca.dfn.de:11371/pks/lookup?op=vindex&search=Kai+Rannenberg
Type bits/keyID Date User ID Dub 1024/ <u>AFIFDF70</u> 1997/09/18 kara < <u>kara@iig.uni-freiburg.de></u> Big DB6375FD Matthias Schunter < <u>schunter@acm.org></u> Dig D5CDE033 Herbert Damker < <u>diamker@iig.uni-freiburg.de></u> Dig 879AC041 Birgit Pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE Big 879AC041 Birgit Pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE Big 8128DC75 Gerhard Weck < <u>73064.2271@compuserve.com></u> Big 8128DC75 Gerhard Weck < <u>43064.2271@compuserve.com></u> Big 8128DC75 Gerhard Weck < <u>43064.2271@compuserve.com></u> Big SC3C4FE4 Holger Reif < <u>teif@prakinf.tu-ilmenau.de></u> Matthias Schunter <schunter@acm.org> Kai R. Rannenberg <<u>kai@microsoft.com></u> Big 0B6375FD Matthias Schunter <<u>schunter@acm.org></u> Big 0F4584B5 Douglas Swiggum <<u>Swiggum@Waisman.Wisc.Edu></u> Big 0F4584B5 Douglas Swiggum <<u>Swiggum@Waisman.Wisc.Edu></u> Big 0F45863FFD Kara <<u>kara@iig.uni-freiburg.de></u> Mattina Schunter <<u>schunter@acm.org></u> Kara <<u>kara@iig.uni-freiburg.de></u> Mig AF1FDF70 Kara <<u>kara@iig.uni-freiburg.d</u></schunter@acm.org>		
<pre>1024/AFIFDF70 1997/09/18 kara <kara@iig.uni-freiburg.de> 10g D86375FD Matthias Schunter <schunter@acm.org> 10g D5CDEC083 Herbert Dawker <damker@iig.uni-freiburg.de> 10g 879AC041 Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE 10g 8128DC75 Gerhard Weck <73064.2271@compuserve.com> 10g 8EF041F1 Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de> 10g 2F6D5039 Kai Martius <kai@imib.med.tu-dresden.de> 10g 45EF1064 Hannes Federrath <federrath@inf.tu-ilmenau.de> 10g 45EF1064 Hannes Federrath <federrath@inf.tu-dresden.de> 10g 065375FD Matthias Schunter <schunter@acm.org> 10g 0458485 Douglas Swiggum@Waisman.Wisc.Edu> 10g 04458485 Douglas Swiggum@Waisman.Wisc.Edu> 10g 0286537FD Martin Reichenbach <mare@iig.uni-freiburg.de> 10g 0286537FD Martin Reichenbach <mare@iig.uni-freiburg.de> 10g 0286537FD Martin Reichenbach <mare@iig.uni-freiburg.de> 10g 0445845 Douglas Swiggum@Waisman.Wisc.Edu> 10g 045657FD Martin Reichenbach <mare@iig.uni-freiburg.de> 10g 0456575FD Martin Reichenbach <mare@iig.uni-freiburg.de> 10g 045675FD Martinas Schunter <schunter@acm.org> 10g 045675FFD Martinas Schunter <schunter@acm.org> 10g 045675FFD Mathias Schunter <schunter@acm.org> 10g 0456375FD Mathias Schunter <schunter@acm.org> 10g 0456375FFD Mathias Schunte</schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></mare@iig.uni-freiburg.de></schunter@acm.org></federrath@inf.tu-dresden.de></federrath@inf.tu-ilmenau.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></kara@iig.uni-freiburg.de></pfitzb@informatik.uni-hildesheim.de></damker@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de></pre>	Public Ke	y Server Verbose Index ``Kai Rannenberg ''
<pre>sig 0B6375FD Matthlas Schunter <schunter@acm.org> sig 05CDE083 Herbert Damker <damker@ig.uni-freiburg.de> sig 079AC041 Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE sig 8120DC75 Gerhard Weck <73064.2271@compuserve.com> sig 8EF041F1 Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de> sig 2F05039 Kai Martius <kai@imib.med.tu-dresden.de> sig 5C3C4FE4 Holger Reif <reif@prakinf.uu-ilmenau.de> Kai R. Rannenberg <kai@imif.uu-ilmenau.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai Rannenberg <kaa@iig.uni-freiburg.de> Kai R. Rannenberg <kaa@iig.uni-freiburg< td=""><td>Type bits/keyID</td><td>Date User ID</td></kaa@iig.uni-freiburg<></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kai@uni-freiburg.de></kai@uni-freiburg.de></kai@uni-freiburg.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></reif@prakinf.uu-ilmenau.de></kai@imib.med.tu-dresden.de></kara@iig.uni-freiburg.de></pfitzb@informatik.uni-hildesheim.de></damker@ig.uni-freiburg.de></schunter@acm.org></pre>	Type bits/keyID	Date User ID
<pre>sig 0B6375FD Matthlas Schunter <schunter@acm.org> sig 05CDE083 Herbert Damker <damker@ig.uni-freiburg.de> sig 079AC041 Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE sig 8120DC75 Gerhard Weck <73064.2271@compuserve.com> sig 8EF041F1 Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de> sig 2F05039 Kai Martius <kai@imib.med.tu-dresden.de> sig 5C3C4FE4 Holger Reif <reif@prakinf.uu-ilmenau.de> Kai R. Rannenberg <kai@imif.uu-ilmenau.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai R. Rannenberg <kai@uni-freiburg.de> Kai Rannenberg <kaa@iig.uni-freiburg.de> Kai R. Rannenberg <kaa@iig.uni-freiburg< td=""><td>pub 1024/AF1FDF70</td><td>1997/09/18 kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></td></kaa@iig.uni-freiburg<></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kaa@iig.uni-freiburg.de></kai@uni-freiburg.de></kai@uni-freiburg.de></kai@uni-freiburg.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></kai@imif.uu-ilmenau.de></reif@prakinf.uu-ilmenau.de></kai@imib.med.tu-dresden.de></kara@iig.uni-freiburg.de></pfitzb@informatik.uni-hildesheim.de></damker@ig.uni-freiburg.de></schunter@acm.org></pre>	pub 1024/AF1FDF70	1997/09/18 kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
<pre>sig S79AC041 Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE sig S128DC75 Gerhard Weck <73064.2271@compuserve.com> sig SEF041F1 Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de> sig 2F05039 Kai Martius <kai@imb.med.tu-dreaden.de> sig SC3C4FE4 Holger Reif <reif@prakinf.tu-ilmenau.de> kai A. Rannenberg <kai@imic.rosoft.com> Kai R. Rannenberg <kai@microsoft.com> Kai R. Rannenberg <kai@imicrosoft.com> kara <kara@iig.uni-freiburg.de> sig AEB4BCDD fap2_AEB4BCD_HSK <fapp2@can.ac.ub> kai Rannenberg <kara@iig.uni-freiburg.de> sig 0C65E63F Martin Reichenbach <marei@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></fapp2@can.ac.ub></kara@iig.uni-freiburg.de></kai@imicrosoft.com></kai@microsoft.com></kai@imic.rosoft.com></reif@prakinf.tu-ilmenau.de></kai@imb.med.tu-dreaden.de></kara@iig.uni-freiburg.de></pfitzb@informatik.uni-hildesheim.de></pre>	sig OB6375FI	Matthias Schunter <schunter@acm.org></schunter@acm.org>
<pre>sig 8128DC75 Gerhard Weck <73064.22718compuserve.com> sig 8FF04IF1 Kai R. Ranenberg 2048 <kara@iig.uni-freiburg.de> sig 2F8D5039 Kai Martius <kai@imbb.med.tu-dresden.de> sig 5C3C4FE4 Holger Reif <reif@prakinf.tu-ilmenau.de> kai AFIFDF70 kara <kara@iig.uni-freiburg.de> Kai R. Ranenberg <kai@info.com> Kai R. Ranenberg <kai@info.com> Kai R. Ranenberg <kai@info.com> Kai R. Ranenberg <kai@info.com> Kai Ranenberg <kai@iig.uni-freiburg.de> sig 0E6375FD Matthias Schunter <schunter@acm.org> Kai Ranenberg <kara@iig.uni-freiburg.de> Kara <kara@iig.uni-freiburg.de> Kara@iig.uni-freiburg.de> Kara <kara@iig.uni-freiburg.de> Kara@iig.uni-freiburg.de> Kara@iig.uni-freiburg.d</kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></kai@iig.uni-freiburg.de></kai@info.com></kai@info.com></kai@info.com></kai@info.com></kara@iig.uni-freiburg.de></reif@prakinf.tu-ilmenau.de></kai@imbb.med.tu-dresden.de></kara@iig.uni-freiburg.de></pre>	sig D5CDE083	Herbert Damker <damker@iig.uni-freiburg.de></damker@iig.uni-freiburg.de>
<pre>sig SEF041F1 Kai R. Rannenberg 2048 <kara@iig.uni-freiburg.de> sig 2F055039 Kai Martius <kai@imb.med.tu-dresden.de> sig 2F055039 Kai Martius <kai@imb.med.tu-dresden.de> sig AFIFDF70 kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kair@microsoft.com> Kai Ranenberg <kair@mi< td=""><td>sig 879AC041</td><td>Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE</pfitzb@informatik.uni-hildesheim.de></td></kair@mi<></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kara@iig.uni-freiburg.de></kai@imb.med.tu-dresden.de></kai@imb.med.tu-dresden.de></kara@iig.uni-freiburg.de></pre>	sig 879AC041	Birgit Pfitzmann 1 <pfitzb@informatik.uni-hildesheim.de> NO LEGAL RELEVANCE</pfitzb@informatik.uni-hildesheim.de>
<pre>sig 2F8D5039 Kai Martius <kai@imib.med.tu-dresden.de> sig 5C3C4FE4 Holger Reif <reif@prakinf.tu-ilmenau.de> sig AFIFDF70 kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kair@microsoft.com> Kai Rannenberg <kair@microsoft.com> Kair@microsoft.com> Kai R. Rannenberg <kair@microsoft.com> Kair@microsoft.com> Kai R. Rannenberg <kair@microsoft.com> Kair@microsoft.com> Kai R. Rannenber</kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kair@microsoft.com></kara@iig.uni-freiburg.de></reif@prakinf.tu-ilmenau.de></kai@imib.med.tu-dresden.de></pre>	sig 8128DC75	Gerhard Weck <73064.22710compuserve.com>
<pre>sig SC3C4FE4 Holger Reif <reif@prakinf.tu-ilmenau.de> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kair@microsoft.com> Kai R. Rannenberg <kair@microsoft.com> sig AEB4BCDD fapp2_AEB4BCDD_HSK <fapp2@cam.ac.uk> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> Kai Rannenberg <kair@uig.uni-freiburg.de> Kai Rannenberg <kair@lig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> Kai Rana@iig.uni-freiburg.de> Kai Rana@iig.uni-freiburg.de> Kara <kara@iig.uni-freiburg.de> Kara &kara@iig.uni-freiburg.de> Kara <kara@iig.uni-freiburg.de> Kara &kara@iig.uni-freiburg.de> Kara &kara@i</kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kair@lig.uni-freiburg.de></kair@uig.uni-freiburg.de></kara@iig.uni-freiburg.de></fapp2@cam.ac.uk></kair@microsoft.com></kair@microsoft.com></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></reif@prakinf.tu-ilmenau.de></pre>	sig 8EF041F1	Kai R. Rannenberg 2048 < <u>kara@iig.uni-freiburg.de</u> >
sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig 49EF1D84 Hannes Federrath <federrath@inf.tu-dresden.de> Kai R. Rannenberg <kair@microsoft.com> sig 0B6375FD Matthias Schunter <schunter@acm.org> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig 044584B5 Douglas Swiggum <swiggum@waisman.wisc.edu> sig 0CB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> sig 0CB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> sig 0B6375FD kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> sig 0B6375FD kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> sig 0B6375FD Matthias Schunter <schunter@acm.org> kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> sig 0B6375FD Matthias Schunter <schunter@acm.org> sig 0B6375FD Matthias Schunter <schunter@acm.org> sig 0B6375FD Matthias Schunter <schunter@acm.org> sig 0B6375FD Matthias Schunter <schunter@acm.org> <td>sig 2F8D5039</td><td>Kai Martius <kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de></td></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></swiggum@waisman.wisc.edu></kara@iig.uni-freiburg.de></schunter@acm.org></kair@microsoft.com></federrath@inf.tu-dresden.de></kara@iig.uni-freiburg.de>	sig 2F8D5039	Kai Martius <kai@imib.med.tu-dresden.de></kai@imib.med.tu-dresden.de>
sig 49EF1D84 Hannes Federrath <federrath@inf.tu-dresden.de> Kai R. Rannenberg <kair@microsoft.com> sig 0B6375FD Matthias Schunter <schunter@acm.org> sig AEB4BCDD fapp2_AEB4BCDD_HSK <fapp2@cam.ac.uk> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig 04584B5 Douglas Swiggum@Waisman.Wisc.Edu> kara <kara@iig.uni-freiburg.de> Kai Rannenberg <kara@iig.uni-freiburg.de> sig 0CB6E63F Martin Reichenbach <marel@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> sig 0B6375FD Mathias Schunter <schunter@acm.org> kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> sig 0B6375FD Mathias Schunter <schunter@acm.org> sig 0B6375FD Mathias Schunter <schunter@acm.org> kai R. Rannenberg <kara@iig.uni-freiburg.de> sig 0B6375FD Mathias Schunter <schunter@acm.org> <td< td=""><td>sig <u>5C3C4FE4</u></td><td>Holger Reif <<u>reif@prakinf.tu-ilmenau.de</u>></td></td<></schunter@acm.org></kara@iig.uni-freiburg.de></schunter@acm.org></schunter@acm.org></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></schunter@acm.org></schunter@acm.org></schunter@acm.org></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marel@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></fapp2@cam.ac.uk></schunter@acm.org></kair@microsoft.com></federrath@inf.tu-dresden.de>	sig <u>5C3C4FE4</u>	Holger Reif < <u>reif@prakinf.tu-ilmenau.de</u> >
Kai R. Rannenberg <kair@microsoft.com> Sig OB6375FD Matthias Schunter <schunter@acm.org> Sig AEB4BCDD fapp2_AEB4BCDD_HSK <fapp2@cam.ac.uk> Sig AF1FDF70 kara <kara@ig.uni-freiburg.de> Sig OCB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> Sig OCB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> kara <kara@tig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> kara <kara@tig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kara@tig.uni-freiburg.de> Kai R. Raa@tig.uni-freiburg.de> Kai R. Raa@tig.uni-freiburg.de> Kai R. Raa@tig.uni-freiburg.de> Kai R.</kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></kara@ig.uni-freiburg.de></fapp2@cam.ac.uk></schunter@acm.org></kair@microsoft.com>	sig AF1FDF70	kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
<pre>sig OB6375FD Matthias Schunter <schunter@acm.org> sig AEB4BCDD fapp2_AEB4BCDD_HSK <fapp2@cam.ac.uk> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig O44584B5 Douglas Swiggum <swiggum@waisman.wisc.edu> Kai Rannenberg <kara@iig.uni-freiburg.de> sig OCB6E63F Martin Reichenbach <marel@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> sig OB6375FD Matthias Schunter <schunter@acm.org> kai R. Rannenberg <kara@iig.uni-freiburg.de> Kai R. Ran@iig.uni-freiburg.de> Kai R. Ran@iig.</kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></kara@telematik.iig.uni-freiburg.de></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marel@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></swiggum@waisman.wisc.edu></kara@iig.uni-freiburg.de></fapp2@cam.ac.uk></schunter@acm.org></pre>	sig <u>49EF1D84</u>	Hannes Federrath < <u>federrath@inf.tu-dresden.de</u> >
<pre>sig AEB4BCDD fapp2_AEB4BCDD_HSK <fapp2@cam.ac.uk> sig AF1FDF70 kara <kara@iig.uni-freiburg.de> sig 044584B5 Douglas Swiggum <<u>Swiggum@Waisman.Wisc.Edu> Kai Rannenberg <kara@iig.uni-freiburg.de> sig 0CB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> sig 0B6375FD Matthias Schunter <<u>schunter@acm.org</u>> kai R. Rannenberg <<u>kara@iig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> sig 0B6375FD Matthias Schunter <<u>schunter@acm.org</u>> sig 0A5175FD Matthias Schunter <<u>schunter@acm.org</u>> sig 0A5175</kara@iig.uni-freiburg.de></u></kara@telematik.iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></u></kara@iig.uni-freiburg.de></fapp2@cam.ac.uk></pre>		Kai R. Rannenberg < <u>kair@microsoft.com</u> >
sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > sig <u>044584B5</u> Douglas Swiggum < <u>Swiggum@Waisman.Wisc.Edu</u> > Kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> > sig <u>0CB6E63F</u> Martin Reichenbach < <u>marei@iig.uni-freiburg.de</u> > kara < <u>kara@telematik.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 <u>0B6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > Matthias Schunter < <u>schunter@acm.org</u> > sig <u>0B6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>0B6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>0B6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >	sig <u>086375FI</u>	Matthias Schunter < <u>schunter@acm.org</u> >
sig 044584B5 Douglas Swiggum < <u>Swiggum</u> @Waisman.Wisc.Edu> Kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> > kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> > kara < <u>kara@telematik.iig.uni-freiburg.de</u> > kara < <u>kara@telematik.iig.uni-freiburg.de</u> > kara < <u>kara@telematik.iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > Sig 0B6375FD Matthias Schunter < <u>schunter@acm.org</u> > Sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> >	sig <u>AEB4BCDI</u>	fapp2_AEB4BCDD_HSK < <u>fapp2@cam.ac.uk</u> >
Kai Rannenberg <kara@iig.uni-freiburg.de> Sig OCB6E63F Martin Reichenbach <marei@iig.uni-freiburg.de> kara <kara@iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@telematik.iig.uni-freiburg.de> kara <kara@tig.uni-freiburg.de> kara <kara@tig.uni-freiburg.de> Kai R. Rannenberg <kara@tig.uni-freiburg.de> Kai Af1FDF70 kara <kara@tig.uni-freiburg.de> Kai R. Rannenberg <kara@tig.uni-freiburg.de> Kai Af1FDF70 kara <kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@tig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@telematik.iig.uni-freiburg.de></kara@iig.uni-freiburg.de></marei@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>	sig <u>AF1FDF70</u>	kara < <u>kara@iig.uni-freiburg.de</u> >
sig <u>OCB6E63F</u> Martin Reichenbach < <u>marei@iig.uni-freiburg.de</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > kara < <u>kara@telematik.iig.uni-freiburg.de</u> > sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > kara < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > Sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >	sig <u>044584B5</u>	Douglas Swiggum < <u>Swiggum@Waisman.Wisc.Edu</u> >
sig AF1FDF70 kara < <u>kara@iig.uni-freiburg.de</u> > kara < <u>kara@telematik.iig.uni-freiburg.de</u> > sig OB6375FD 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 OB6375FD Matthias Schunter < <u>schunter@acm.org</u> > sig AF1FDF70 kara < <u>kara@iig.uni-freiburg.de</u> >		Kai Rannenberg < <u>kara@iig.uni-freiburg.de</u> >
kara <kara@telematik.iig.uni-freiburg.de> Big OB6375FD Matthias Schunter <schunter@acm.org> Big AF1FDF70 kara <kara@iig.uni-freiburg.de> Kai R. Rannenberg <kara@iig.uni-freiburg.de> Big OB6375FD Matthias Schunter <schunter@acm.org> Big AF1FDF70 kara <kara@iig.uni-freiburg.de> Sig OB6375FD Matthias Schunter <schunter@acm.org> Sig AF1FDF70 kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de></schunter@acm.org></kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de></schunter@acm.org></kara@telematik.iig.uni-freiburg.de>	sig <u>OCB6E63E</u>	Martin Reichenbach < <u>marei@iig.uni-freiburg.de</u> >
sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >	sig <u>AF1FDF70</u>	kara < <u>kara@iig.uni-freiburg.de</u> >
sig AF1FDF70 kara < <u>kara@iig.uni-freiburg.de</u> > Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >		
Kai R. Rannenberg < <u>kara@iig.uni-freiburg.de</u> > sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >	sig <u>0B6375FI</u>	
sig <u>OB6375FD</u> Matthias Schunter < <u>schunter@acm.org</u> > sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >	sig <u>AF1FDF70</u>	
sig <u>AF1FDF70</u> kara < <u>kara@iig.uni-freiburg.de</u> >		
	-	
	sig <u>AF1FDF70</u>	kara <kara@iig.uni-freiburg.de></kara@iig.uni-freiburg.de>
	•	
	 8)	🚺 👔 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)

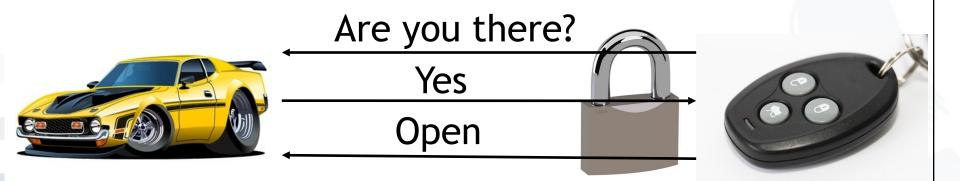
[Marshall Symposium 1998] [Randell 2004]







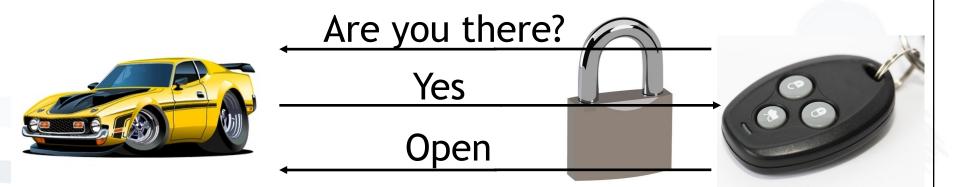
- Solution: Protect communication with crypto?
- e.g. symmetric cryptography + hash/signature

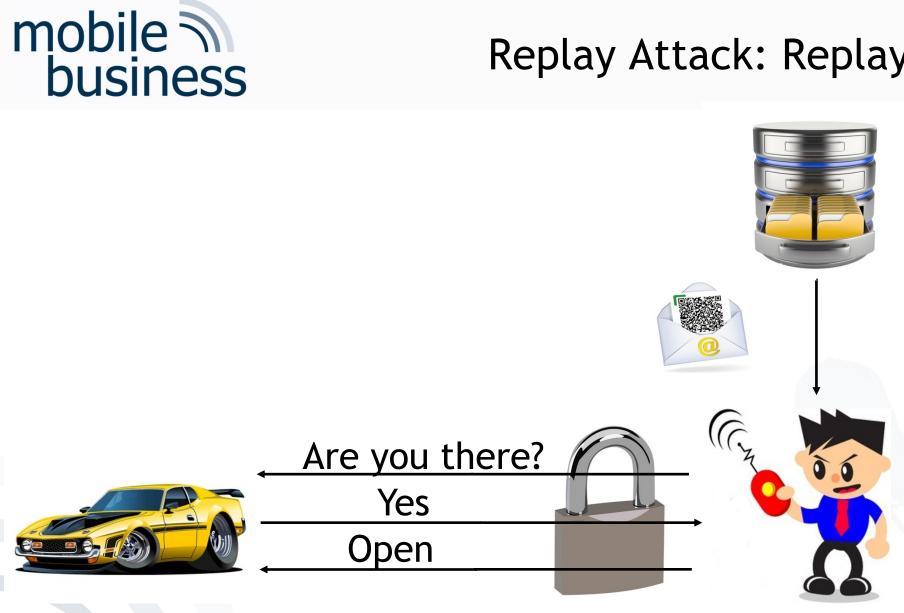


Replay Attack: Eavesdrop

mobile business





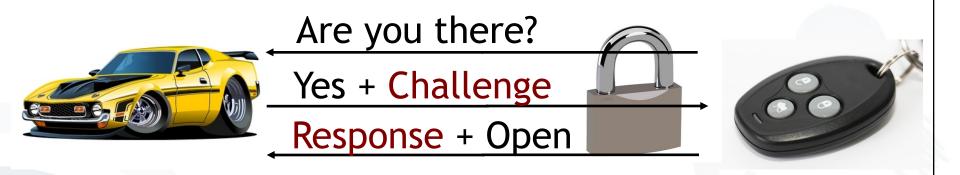


Replay Attack: Replay



Replay Attack: Solution

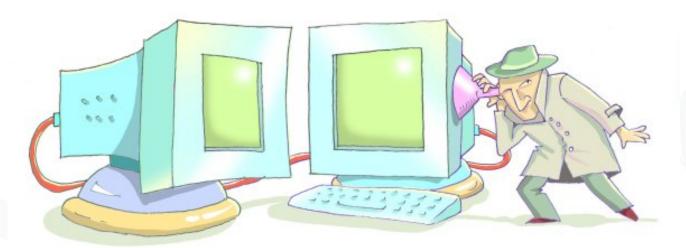
e.g. Challenge-Response helps





Side-Channel Attacks I

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

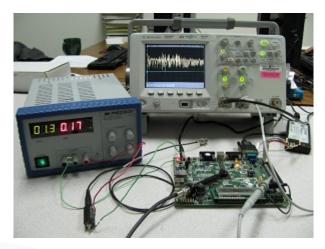


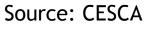
Source: Eran Tromer

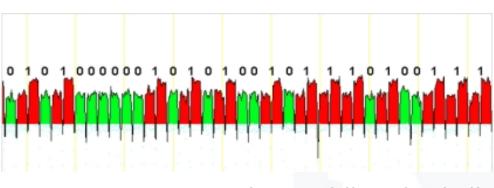


Side-Channel Attacks II

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





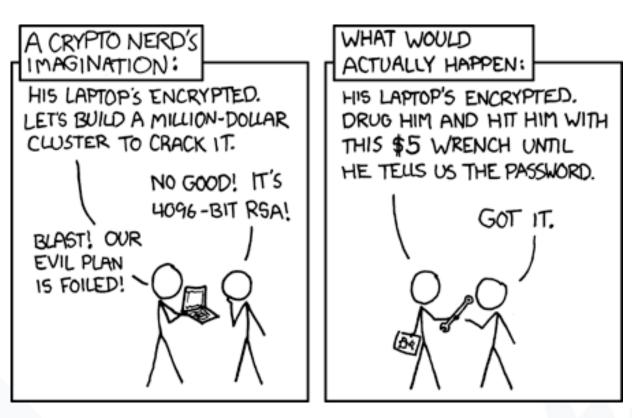


Source: Gilbert Goodwill

- 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

- 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