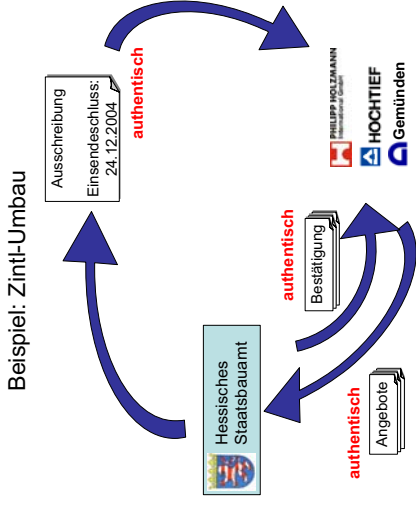


Public Key Infrastrukturen

V1. Public Key Techniken und Dienste

Prof. J. Buchmann
 FG Theoretische Informatik
 TU Darmstadt

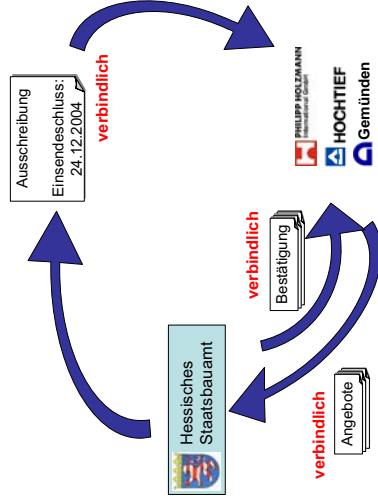
Beispiel: Zinti-Umbau



2

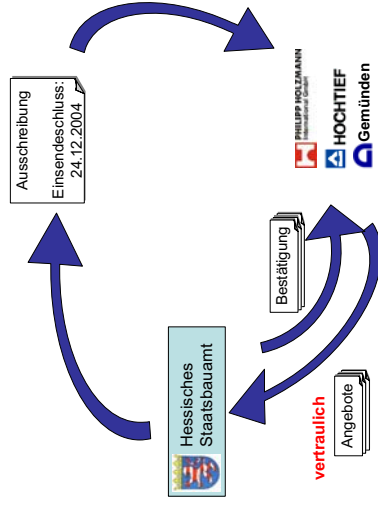
3

Beispiel: Zinti-Umbau



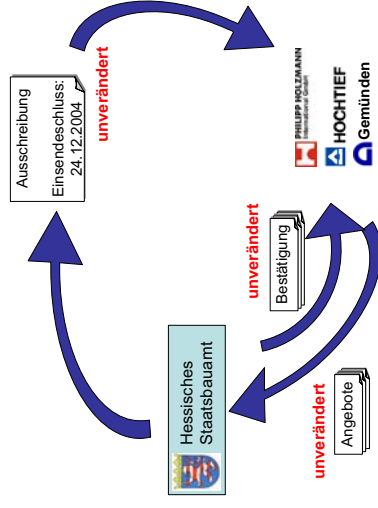
4

Beispiel: Zinti-Umbau



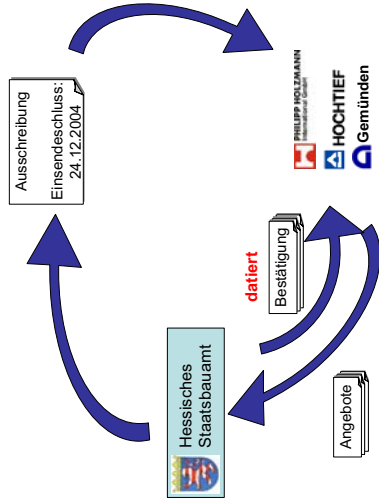
5

Beispiel: Zinti-Umbau



6

Beispiel: Zintl-Umbau



7

Sicherheitsziele

- authentisch**
- ▶ Urheber bekannt
- verbindlich**
- ▶ Urheber nachweisbar
- vertraulich**
- ▶ Nur für Berechtigte lesbar
- unverändert**
- datiert**
- ▶ Nachweisbar, dass das Dokument zu einem bestimmten Zeitpunkt existiert hat

8

TUDCard

elektronische Rückmeldung
Anmeldung zu Lehrveranstaltungen
Prüfungsmeldung
Drucken von Bescheinigungen
digitale Bibliotheken
sicheres Login
Gebäude Zugangsschutz
Mensa / Studentenwerk



9

TUDCard

elektronische Rückmeldung
Anmeldung zu Lehrveranstaltungen
Prüfungsmeldung
Drucken von Bescheinigungen
digitale Bibliotheken
sicheres Login
Gebäude Zugangsschutz
Mensa / Studentenwerk



10

TUDCard

authentisch	✓
verbindlich	✗
vertraulich	✗
unverändert	✓
datiert	✗
sicheres Login	



11

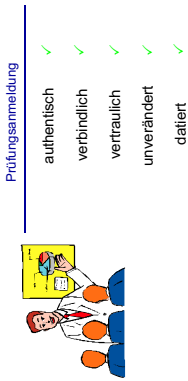
TUDCard

elektronische Rückmeldung
Anmeldung zu Lehrveranstaltungen
Prüfungsmeldung
Drucken von Bescheinigungen
digitale Bibliotheken
sicheres Login
Gebäude Zugangsschutz
Mensa / Studentenwerk



12

TUDCard

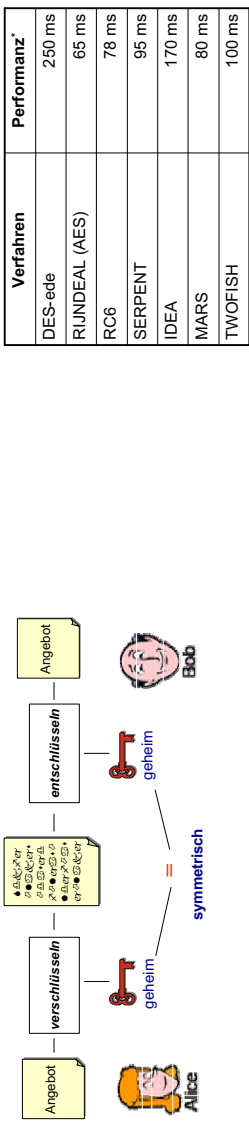


13

Verschlüsselung

symmetrische Verschlüsselungsverfahren

Vorteil: Verfahren sind sehr schnell

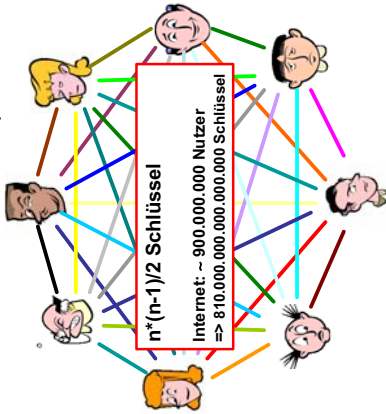


Verfahren	Performanz*
DES-ede	250 ms
RUNDEAL (AES)	65 ms
RC6	78 ms
SERPENT	95 ms
IDEA	170 ms
MARS	80 ms
TWOFISH	100 ms

*) Verschlüsselung von 1 MB-Blöcken auf einem Pentium 2.8 GHz, mit dem FlexProvider (Java)

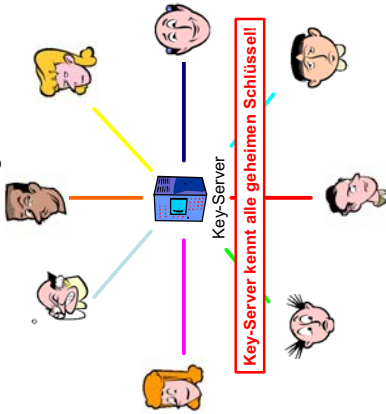
14

ABER: Schlüsselaustauschproblem



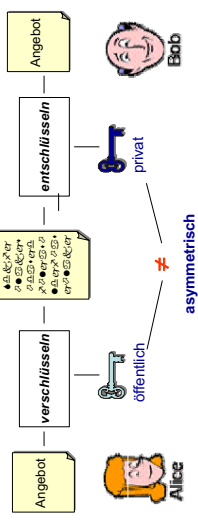
16

Eine Lösung:



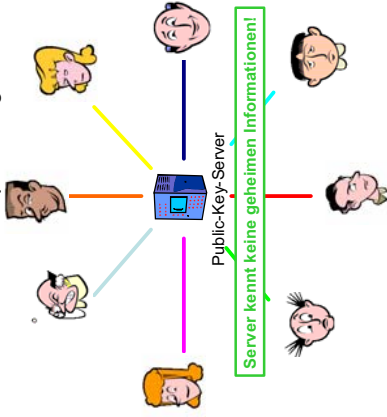
17

Verschlüsselung



18

Schlüsselaustauschproblem gelöst!



19

Public-Key-Server

Zuordnung: Namen ? öffentliche Schlüssel

Öffentliches Verzeichnis	
Buchmann	13121311235912753192375134123
Karatsiolis	8422834964509823610263135768
...	...

20

Asymmetrische Verschlüsselungsverfahren

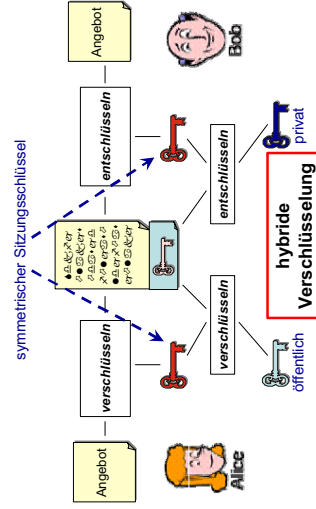
Verfahren	Performanz*
RSA (1024 bits)	6,6 s
RSA (2048 bits)	11,8 s

Nachteil: Komplexe Operationen mit sehr großen Zahlen
 ⇒ **Verfahren sind sehr langsam**

*) Verschlüsselung von 1 MB-Blöcken auf einem Pentium 2,8 GHz, mit dem FlexProvider (Java)

21

Lösung:



22

Geheimnis

$n = 109417386415705274218097073220403576120037$
 $329454492059909138421314763499842889347847$
 $179972578912673324976257528997818337970765$
 $7244027146743531593354333897$

Im August 1999 faktorisiert:

$p = 1026395928297411057720541966573991675900716$
 $567808038066803341933521790711307779$
 $q = 106603488380168454820927220360012878679207$
 $958575989291522270608237193062808643$

23

Schwieriges Berechnungsproblem: Faktorisieren

Fermat – Zahlen (Pierre de Fermat, 1601-1665)

$$F_m = 2^{2^m} + 1$$

$$F_0 = 3$$

$$F_1 = 5$$

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

$$F_5 = 4294967297$$

 $= 64 \cdot 1^*67004 \cdot 17$

24

Schwieriges Berechnungsproblem: Faktorisieren

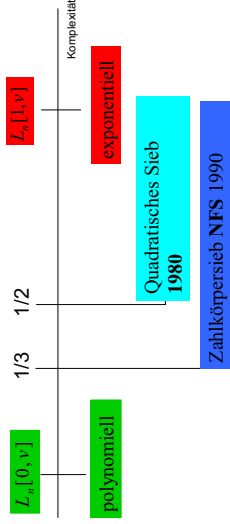
Vollständig faktorisierte Fermat – Zahlen

m	Dezimalstellen	Jahr	Entdecker
5	10	1732	Euler
6	20	1880	Landry, Le Lasseur
7	39	1970	Morrison, Brillhart
8	78	1980	Brent, Pollard
9	155	1990	Western, Lenstra, Manasse, u.a.
10	309	1995	Selfridge, Brillhart, Brent
11	617	1988	Cunningham, Brent, Morain

25

Berechnungsaufwand

$$L_n[u, v] = e^{v(\log n)^u (\log \log n)^{(1-u)}}$$



26

Gelöste RSA - Challenges

Jahr	n	Algorithmus	MIPS-Jahr
Apr. 1991	RSA-100	QS	7
Apr. 1992	RSA-110	QS	75
Jun. 1993	RSA-120	QS	830
Apr. 1994	RSA-129	QS	5000
Apr. 1996	RSA-130	NFS	500
Feb. 1999	RSA-140	NFS	2000
Apr. 1999	RSA-155	NFS	8000
Apr. 2003	RSA-160		
Dec. 2003	RSA-576 (174 Digits)		

27

Schwieriges Berechnungsproblem: DLP

Diskrete-Logarithmen-Problem (DLP):

G Gruppe

$$\text{Löse } g^x = a$$

$$x = \log_g a$$

G Punktgruppe einer **elliptischen Kurve**:

Exponentielle Komplexität

Erlaubt kleine Schlüssel

28

Gelöste Elliptische-Kurven-Challenges

Jahr	Schlüssellänge	Algorithmus	MIPS-Jahre
1997	79	Pollard	k.A.
1998	89	Pollard	k.A.
1998	97	Pollard	k.A.
1999	97	Pollard	16.000
2000	108	Pollard	400.000

29

Quantencomputer

machen

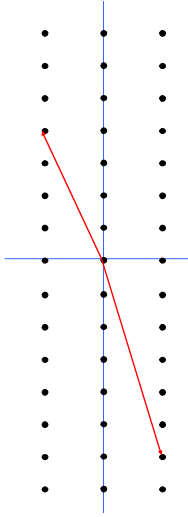
Faktorisieren **leicht**

ECDLP **leicht**

Alle gängigen Kryptosysteme **unsicher**

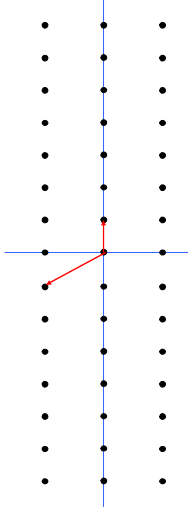
30

Alternative: Kurze Gittervektoren



31

Alternative: Kurze Gittervektoren



32

Kurze Vektoren

Dimension	Laufzeit LLL	Länge SV
100	8 min	$3 \cdot 10^3$
200	2 h	$2 \cdot 10^5$
300	9 h	$4 \cdot 10^6$
400	27.7 h	$1 \cdot 10^8$
450	2 d	$4 \cdot 10^8$

Architektur: SunBlade 100 (C++)

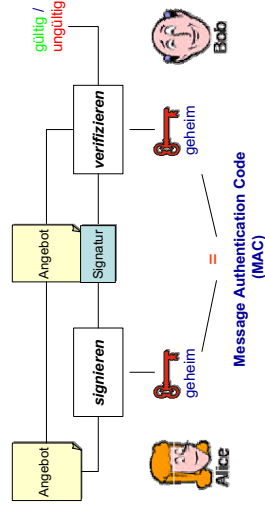
33

Herausforderungen für die Wissenschaft

- Finde schwierige Berechnungsprobleme
- Finde die richtigen Sicherheitsmodelle
- Finde beweisbar sichere Kryptoverfahren

34

Signatur



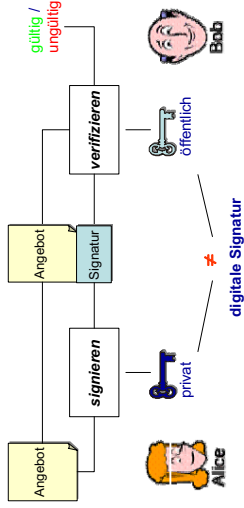
35

Message Authentication Code

- Symmetrisches Verfahren
- ⇒ **schnell**
- ⇒ **Schlüsselaustauschproblem**

36

Signatur



37

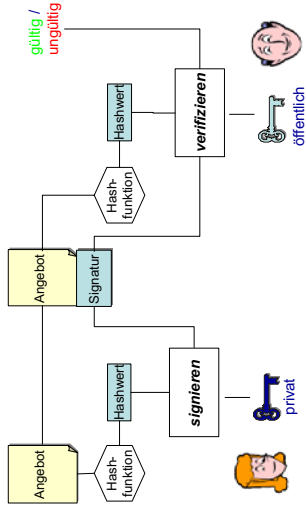
Digital Signature

Asymmetrisches Verfahren

⇒ **langsam**

⇒ **Schlüsselaustauschproblem gelöst**

Lösung



38

Asymmetrische Signatur-Verfahren

Verfahren	Performanz*
RSA (1024)	35 msec
DSA (1024)	32 msec
ECDSA (160)	38 msec

*) Erstellung einer Signatur auf einem Pentium 2,8GHz mit dem FlexProvider (Java)

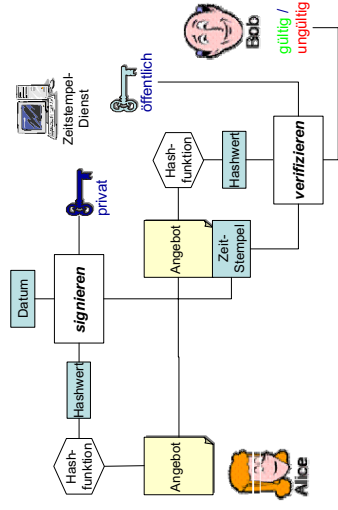
40

Erreichen der Sicherheitsziele

- Authentizität → MAC, digitale Signatur
- Verbindlichkeit → digitale Signatur
- Vertraulichkeit → sym. und asym. Verschlüsselung
- Unverändertheit → MAC, digitale Signatur
- Datiert → Zeitstempel

41

Zeitstempel



42

Vielen Dank für Ihre
Aufmerksamkeit!