Von der Kopfrasur zur Kopfakrobatik

CLT 2014

16. März 2014

Andreas Steil
Linux Consultant & Trainer
B1 Systems GmbH
steil@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source-Themen
- national & international tätig
- über 60 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- dezentrale Strukturen

Schwerpunkte

- Virtualisierung (XEN, KVM & RHEV)
- Systemmanagement (Spacewalk, Red Hat Satellite, SUSE Manager)
- Konfigurationsmanagement (Puppet & Chef)
- Monitoring (Nagios & Icinga)
- IaaS Cloud (OpenStack & SUSE Cloud)
- Hochverfügbarkeit (Pacemaker)
- Shared Storage (GPFS, OCFS2, DRBD & CEPH)
- Dateiaustausch (ownCloud)
- Paketierung (Open Build Service)
- Administratoren oder Entwickler zur Unterstützung des Teams vor Ort

Geheime Kommunikation – Überblick

- Steganographie
- Verschlüsselung
  - Klassische Verfahren:
    - Transpositionschiffre (z.B. Skytale)
    - Substitutionschiffre (z.B. Caesar-Chiffre)
    - Polyalphabetische Chiffre (z.B. Vigenère-Chiffre)
  - Computergestützte Verfahren:
    - Symmetrische Verschlüsselung:
      Stromchiffren, Blockchiffren, Mehrfachverschlüsselungen
      (z.B. RC4, DES, 3DES, IDEA, Twofish, Blowfish, AES)
    - Asymmetrische Verschlüsselung und Einwegfunktionen:
      Primzahlmultiplikation, diskreter Logarithmus
      (z.B. Diffie-Hellman, El Gamal, RSA, DSA, Elliptische Kurven)
    - Hashfunktionen (z.B. SHA-x, MD5)
- Anwendungen für kryptographische Verfahren
  (Digitale Signaturen, SSL/TLS, SSH, IPSec, S/MIME, PGP, . . .)

Agenda – Klassische Verfahren

Steganographie Nachrichten werden in unverfänglichen Informationen auf einem Trägermedium versteckt.

Transpositionsverfahren Buchstaben des Klartextes werden anders angeordnet.

- Stabchiffre/Skytale
- Fleißnersche Schablone
- ADFGX

Monoalphabetische Substitution Buchstaben des Klartextes werden durch jeweils gleiche Buchstaben ersetzt.

- Caesar-Verschlüsselung
- Atbasch

Polyalphabetische Substitution Buchstaben des Klartextes werden durch immer unterschiedliche Buchstaben ersetzt.

- Vigenère-Verschlüsselung
- Enigma

Agenda – Computergestützte Verfahren

- Symmetrische Verschlüsselung:
  - Stromchiffren
  - Blockchiffren
  - Mehrfachverschlüsselungen
- Einwegfunktionen und Asymmetrische Verschlüsselung:
  - Hash-Funktionen
  - Primzahlmultiplikation
  - Diskreter Logarithmus
- Anwendungsbeispiele für kryptographische Verfahren:
  - Digitale Signaturen
  - Secure Shell (SSH)
  - TLS
  - S/MIME
  - PGP/GnuPG
  - ...

Geheime Kommunikation – Prinzipien

Kerckhoffs'sches Prinzip (1883)

Sicherheit eines Systems darf nicht von der Geheimhaltung des Verschlüsselungsalgorithmus abhängen, nur von der Geheimhaltung eines Schlüssels.

Prinzipien von Shannon (1949)

Konfusion: Der funktionale Zusammenhang zwischen Klartext, Chiffretext und Schlüssel sollte komplex sein.
Diffusion: Jedes Chiffretextzeichen sollte von möglichst vielen Klartextzeichen und dem gesamten Schlüssel abhängen.

Security by Obscurity

Sicherheit durch Geheimhaltung der Funktionsweise.

Geschichte der Kryptographie – Überblick

- Transpositionsverfahren (bis 1. Weltkrieg)
  - Skytale
  - Fleißnersche Schablone
  - ADFGX
- Monoalphabetische Substitution (Zeitenwende)
  - Caesar-Verschlüsselung
  - Atbasch (kabbalistische Methode)
- Polyalphabetische Substitution (16. - 20. Jahrhundert)
  - Vigenère-Verschlüsselung
  - Enigma
- Einwegfunktionen (ab 1970er Jahre)
  - Primfaktorzerlegung
  - Diskrete Logarithmen

Steganographie

- Geheimtinte
  (z.B. Zitronensaft, Mischung aus Alaun und Essig auf Eierschale, . . .)
- Schmuggeltechniken
  (z.B. doppelter Boden in Paketen oder Briefumschlägen, hohle Absätze von Schuhen, . . .)
- Einbetten einer Nachricht in einer anderen unterhalb der Wahrnehmungsschwelle (z.B. jeweils erster Buchstabe eines Wortes, Satzes, Abschnitts, . . .)
- Schlüsselwörter in Texten
  (z.B. „three little birds - this is my message to you“)
- Zinken, Symbole, . . .
- Spezielle Bits in Bildern
- . . .

Transpositionsverfahren

Prinzip: Zeichen werden nicht ersetzt („substituiert“), sondern umsortiert („transponiert“).

Skytale
: Band wird um einen Stab („Skytale“) mit speziellem Durchmesser gewickelt

Gartenzaun
: geregelte Transposition, bei der Buchstaben z.B. abwechselnd auf zwei Zeilen geschrieben werden

Fleißnersche Schablone
: 1881 von Eduard Fleißner veröffentlicht; z.B. Schablone mit ausgeschnitten Quadraten, die gedreht wird

ADFGX
: 1918 von Fritz Nebel (!) erdacht; zweistufiges Verfahren (zuerst Substitution); 5x5-Matrix mit Kennwort

Monoalphabetische Substitution

- Prinzip:
  Nur ein einziges (festes) Alphabet zur Verschlüsselung zur Umwandlung des Klartextes in den Geheimtext.
- Beispiele:
  - Caesar-Verschlüsselung
    erste bekannte Verwendung durch Caesar (meist mit dem Schlüssel „C“ ;-) = Verschiebung um drei Buchstaben); nur 25 verschiedene Schlüssel möglich
  - Atbasch
    ursprünglich kabbalistische Methode; der erste Buchstabe wird mit dem letzten Buchstaben vertauscht, der zweite mit dem vorletzten, usw.
- Nachteil: leicht zu knacken . . .

Häufigkeitsverteilung der Buchstaben

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

Abbildung : Häufigkeitsverteilung der Buchstaben des deutschen Alphabets (Quelle: A. Beutelspacher, Kryptologie, 1993)

Polyalphabetische Substitution

Prinzip:
Jedes Zeichen wird jeweils durch ein anderes Zeichen ersetzt.

Caesar-Verschlüsselung mit fortschreitender Quelle
: wie Caesar-Verschlüsselung, nur dass das aktuelle Klartextzeichen je nach dessen Position im Klartextstrang im Alphabet verschoben wird.

Vigenère-Verschlüsselung
: ein Schlüsselwort bestimmt, wie viele und welche Alphabete genutzt werden. Die Alphabete leiten sich aus der Caesar-Substitution ab.

Rotor-Maschinen
: Walzen oder Räder, auf die die Buchstaben des Alphabets eingraviert sind, bestimmen die Zahl und Auswahl der Chiffrier-Alphabete.

Caesar-Verschlüsselung mit fortschreitender Quelle

Originaltext:	B	E	W	E	G	E	N	D
Position:	1	2	3	4	5	6	7	8
Geheimtext:	**C**	**G**	**Z**	**I**	**L**	**K**	**U**	**L**

Vigenère-Verschlüsselung (um 1780)

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	**R**	S	T	U	V	W	X
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	**A**	B
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
M	**M**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

Originaltext:	F	O	R	**N**	**S**	**A**	O	N	L	Y
Schlüssel:	G	E	H	**E**	**I**	**M**	G	E	H	E
Geheimtext:	G	S	Y	**R**	**A**	**M**	U	R	S	C

Fleißnersche Schablone (1881)

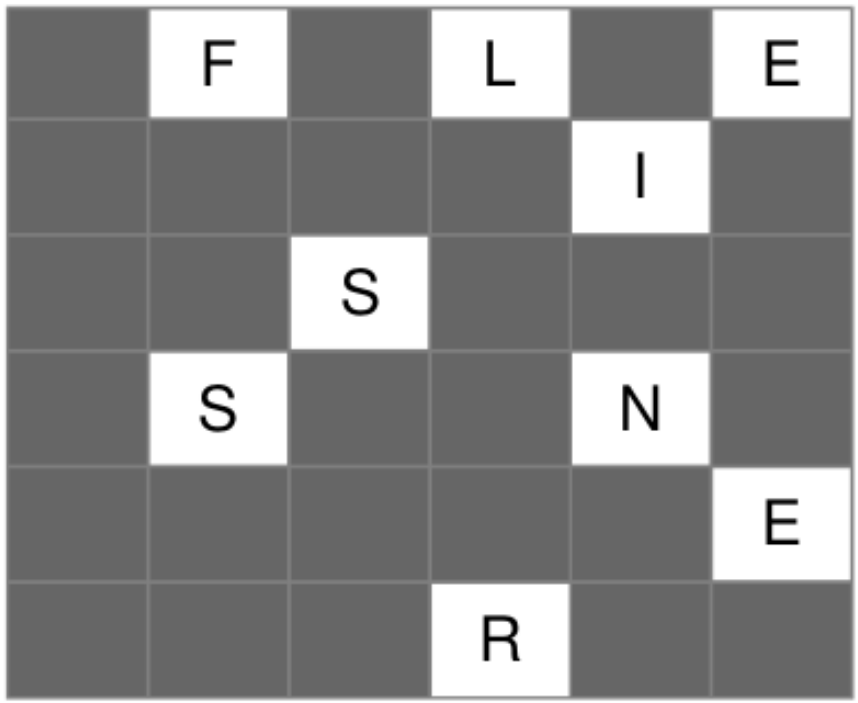


Abbildung : Transposition mit Fleißner-Schablone

ADFGX-Verschlüsselung (Fritz Nebel, 1918)

1. Substitution mit Polybios-Quadrat:

	A	**D**	**F**	**G**	**X**
A	O	Z	A	P	F
D	T	I	S	B	C
F	D	E	G	H	K
G	L	M	N	Q	R
X	U	V	W	X	Y

Originaltext:	W	E	I	S	S	B	I	E	R
Schlüssel 1:	O	Z	A	P	F	T	I	S	
Chiffrat 1:	**XF**	**FD**	**DD**	**DF**	**DF**	**DG**	**DD**	**FD**	**GX**

2. Transposition mit Matrix:

P	R	O	S	I	T
15	17	14	18	9	19
X	**F**	**F**	**D**	**D**	**D**
F	**D**	**F**	**D**	**G**	**D**
D	**F**	**D**	**G**	**X**	

Chiffrat 1:	XF	FD	DD	DF	DF	DG	DD	FD	GX
Schlüssel 2:	P	R	O	S	I	T			
Geheimtext:	**DGXF FDXF DFDF DDGD D**								

Enigma (Arthur Scherbius, 1923)

Enigma

Komplexität der Verschlüsselung (= Größe des Schlüsselraumes):

Ringstellung

26 verschiedene Ringstellungen (01 bis 26) für die mittlere und die rechte Walze $\Rightarrow 26^2 = 676$ Ringstellungen

Walzenlage

3 von 5 Walzen (I bis V) und 1 von 2 Umkehrwalzen (B oder C) $\Rightarrow 2 \cdot (5 \cdot 4 \cdot 3) = 120$ mögliche Walzenlagen

Walzenstellung

für jede der drei rotierenden Walzen 26 Möglichkeiten (A bis Z) $\Rightarrow 26^3 = 17.576$ Walzenstellungen

Steckerverbindungen

maximal 13 Steckerverbindungen zwischen 26 Buchstaben $\Rightarrow$ $26 \cdot 25/2 = 325$ Möglichkeiten für die erste Verbindung; $24 \cdot 23/2 = 276$ Möglichkeiten für die zweite Verbindung, ...

Enigma – Schlüsselraum

Größe des Schlüsselraumes einer Enigma I :
Produkt aus 676 Ringstellungen, 120 Walzenlagen, 16.900 Walzenstellungen und 150.738.274.937.250 Steckermöglichkeiten
$\Rightarrow$
$676 \cdot 120 \cdot 16.900 \cdot 150.738.274.937.250 =$
$206.651.321.783.174.268.000.000$ Möglichkeiten $=$
$2 \cdot 10^{23}$ Möglichkeiten

($\Rightarrow$ entspricht einer Schlüssellänge von 77 Bit)

Enigma – Walze

Abbildung : Linke Seite einer Walze mit Übertragskerbe

Enigma und die Turing-Bombe

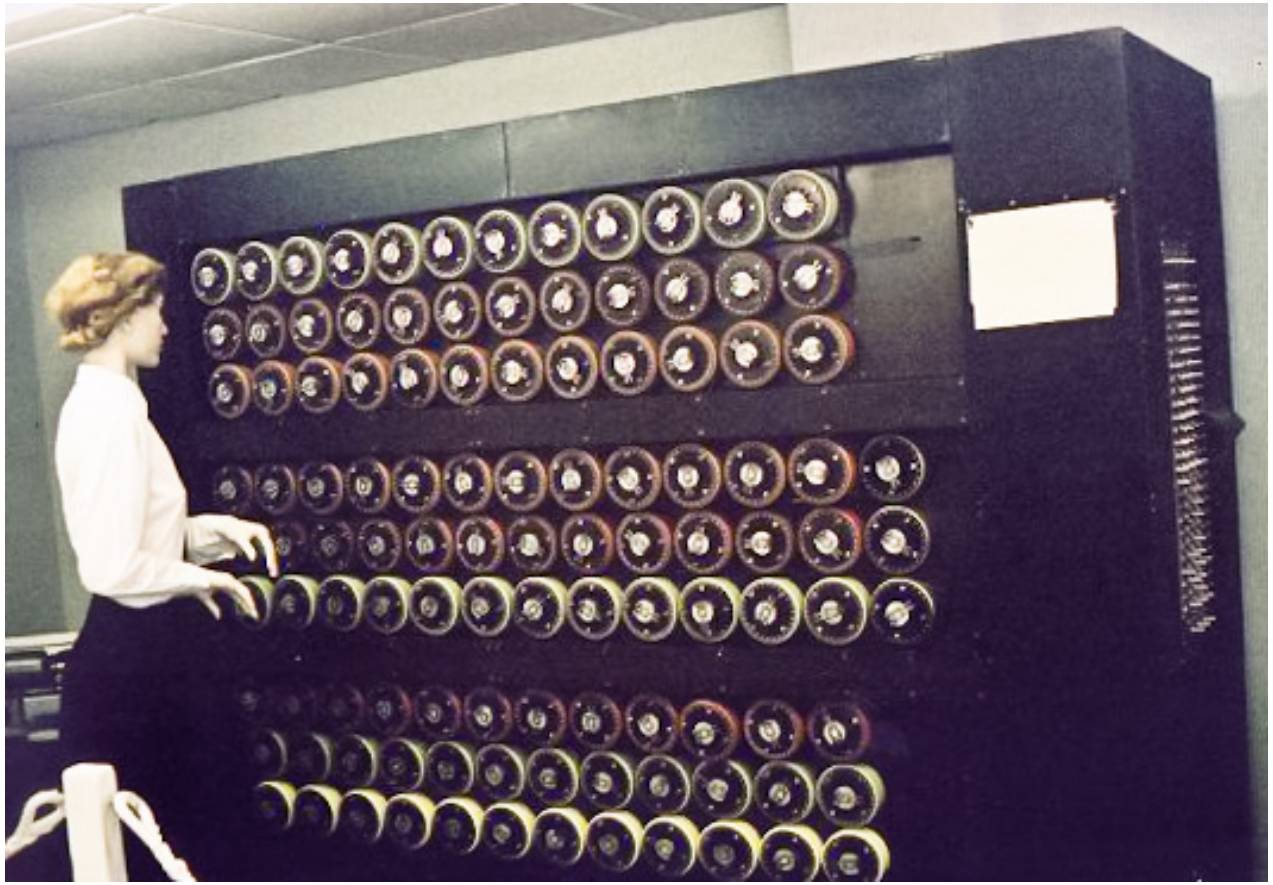


Abbildung : Turing-Bombe

Moderne Verschlüsselung

Blockchiffren (*Block Cipher*)
: deterministisches Verschlüsselungsverfahren, bei dem ein Klartext fester Länge auf ein Chiffrat fester Länge abgebildet wird (z.B. AES bei WLAN, IP-Telefonie in offenen Protokollen wie SRTP oder proprietären Systemen wie Skype; IPsec, SSH; Twofish bei Festplattenverschlüsselung).

Stromchiffren (*Stream Cipher*)
: kryptographischer Algorithmus zur symmetrischen Verschlüsselung, bei dem Zeichen des Klartextes mit den Zeichen eines Schlüsselstroms einzeln verknüpft werden (z.B. GSM bei Sprachübertragung).

Blockchiffren – Designziele

Allgemein: Verschlüsselungsfunktion soll sich möglichst zufällig zeigen.

Konfusion
: Zusammenhang zwischen Klartext und Chiffretext verschleiern.

Diffusion
: Information über den Chiffretext verteilen.

Lawineneffekt
: Jedes Bit im Chiffretext soll von jedem Bit des Klartexts und des Schlüssels abhängen. Änderungen im Klartext sollen möglichst großen Einfluss auf den Chiffretext haben. (Idealfall: Änderung eines Bits des Klartextblockes ändert jedes Bit des Geheimtextblockes.)

Moderne Verschlüsselungsalgorithmen – Beispiele I

Data Encryption Standard (DES/3DES)

1974; Schlüssellänge nur 56 Bit ⇒ Erweiterung: Triple DES (3DES) mit drei voneinander unabhängigen 56-Bit-Schlüsseln.

Blowfish

1993; variable Schlüssellängen bis 448 Bit; schnell; Sicherheit bislang noch nicht mathematisch bewiesen.

Advanced Encryption Standard (AES)

1998; Nachfolger von DES/3DES; auch Rijndael-Algorithmus; Ergebnis einer öffentlichen Ausschreibung; Schlüssellängen bis 256 Bit; wird u.a. von US-Behörden, bei WLAN, IP-Telefonie, IPsec, SSH eingesetzt.

Moderne Verschlüsselungsalgorithmen – Beispiele II

IDEA (International Data Encryption Algorithm)
: 1990; an der ETH Zürich entwickeltes Blockverschlüsselungsverfahren; Anwendung u.a. in PGP

Twofish
: 1998; Blockverschlüsselungsverfahren vom Counterpane Team; u.a. bei GNU PG, TrueCrypt, dm-crypt und Microsoft Windows eingesetzt.

RC2, RC4, RC5, RC6
: mehrere Verschlüsselungsverfahren von Ronald L. Rivest („Rivest Cipher“).

Moderne Verschlüsselungsalgorithmen – Beispiele III

CAST-128, CAST-256
: 1996; Blockverschlüsselungsverfahren von Carlisle Adams und Stafford Tavares (⇒ CAST); unpatentiert.

QUISCI (Quick Stream Cipher)
: 2001; sehr schnelles Stromverschlüsselungsverfahren von Stefan Müller; unpatentiert.

...

Symmetrische Verschlüsselung – Probleme

Bisher vorgestellte Verfahren sind sog. „symmetrische Verfahren“, d.h. Sender und Empfänger nutzen den gleichen Schlüssel.
Zwei Probleme bei der symmetrischen Verschlüsselung:

- Schlüsselübertagung
- Anzahl der benötigten Schlüssel

Schlüsselanzahl

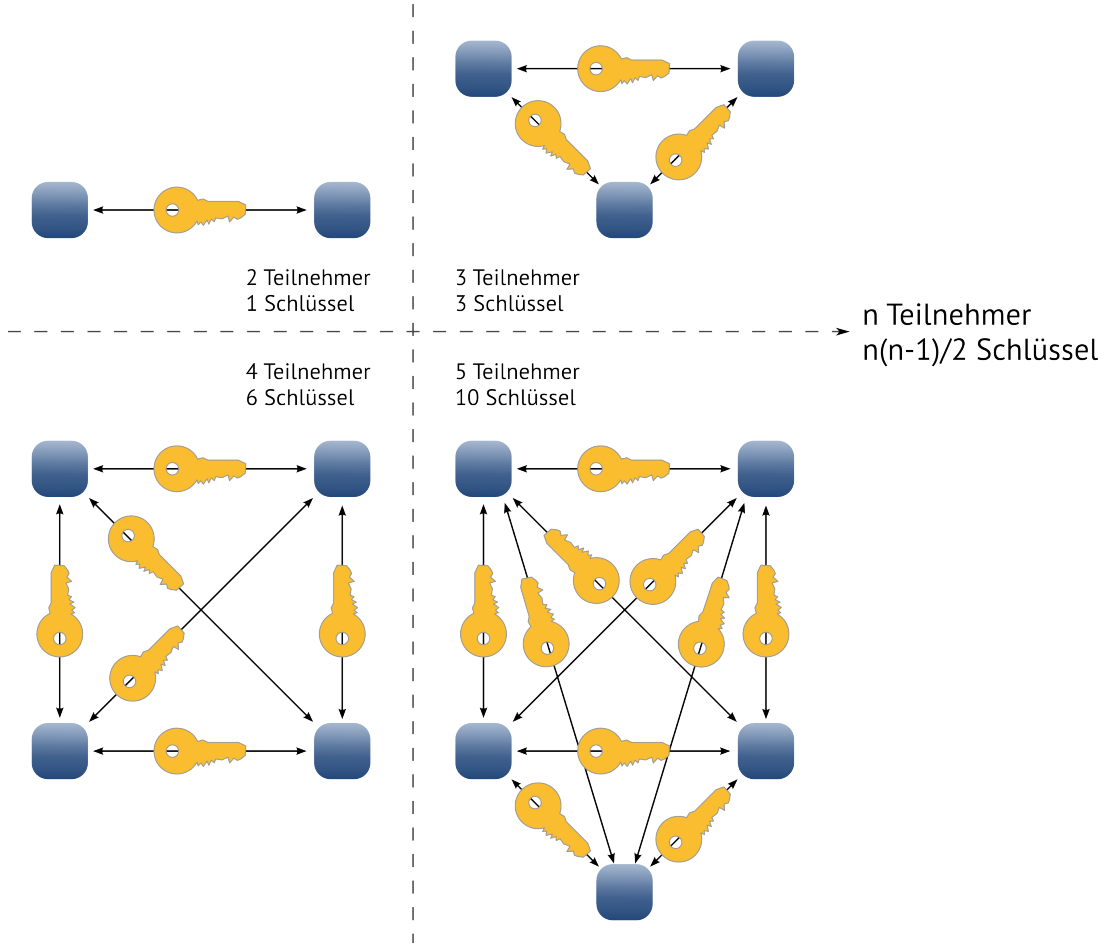


Abbildung : Schlüsselanzahl steigt exponentiell mit der Teilnehmeranzahl

Asymmetrische Verschlüsselung

Lösung der Probleme symmetrischer Verschlüsselung:
⇒ Aufteilung des Schlüssels in:

- öffentlicher Schlüssel (*Public Key*)
  Zum Verschlüsseln einer Nachricht benutzt man den öffentlichen Schlüssel des Empfängers.
- geheimer Schlüssel (*Private Key*)
  Zum Entschlüsseln einer Nachricht benutzt man den eigenen privaten (geheimen!) Schlüssel.

⇒ Sender und Empfänger brauchen sich nicht auf einen Schlüssel zu einigen. Lediglich ein öffentlicher Schlüssel des Empfänger für Absender nötig, der von jedem benutzt werden kann.
⇒ Für n Kommunikationsteilnehmer sind nur n Schlüsselpaare notwendig.
Voraussetzung: ⇒ Einwegfunktionen

Einwegfunktionen – Etwas Mathematik

- Informelle Definition:
  Eine Funktion $f : M \longmapsto N$ heißt Einwegfunktion, wenn für „fast alle“ Bilder $y \in N$ ein Urbild $x \in M$ mit $f(x) = y$ nicht effizient bestimmbar ist.
- Bei computergestützter Kryptographie: Ausgangswerte sind nicht in angemessener Zeit bestimmbar.
- Beispiele:
  - Faktorisierungsproblem großer Zahlen (z.B. RSA)
  - Diskreter Logarithmus (z.B. DH, ElGamal, DSA, ECC)
- Spezialfall: Hashfunktionen sind Einwegfunktionen, für die üblicherweise kein Urbild bestimmbar ist (z.B. SHA, MD5).

Hashfunktionen

- Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet.
- Bedingungen:
  - Einwegfunktion:
    Es ist praktisch unmöglich, zu einem gegebenen Ausgabewert y einen Eingabewert x zu finden, den die Hashfunktion auf y abbildet.
  - Kollisionsresistenz:
    Es ist praktisch unmöglich, für einen gegebenen Wert x einen davon verschiedenen x' zu finden, der denselben Hashwert liefert.
- Beispiel für eine einfache Hashfunktion: einstellige Quersumme
- Schlüsselabhängige Hashfunktionen werden auch *Message Authentication Codes* (MAC) genannt (HMAC, UMAC, ...).

Hashalgorithmen – Anwendungen (SHA)

Signierung von Daten

⇒ Schutz vor Datenmanipulation

Prüfsummen

⇒ Erkennung von Übertragungsfehlern

Identifikation größerer Datenmengen mit Hashwert

⇒ Identifikation von Inhalten
(z.B. in Peer-to-Peer-Tauschbörsen)

Kennwortschutz

⇒ Speicherung des Passwort-Hashwerts statt des Klartextes
(z.B. in `/etc/passwd`, für Internetseiten, . . .)

Hashalgorithmen – Beispiel

Beispiel: Kennwortverschlüsselung

```
$ python -c "import crypt; print crypt.crypt('GEHEIM', '\$6')"
```

Beispiel: Hashwert für „Chemnitzer Linux Tage“

```
$6$$OPxjQOG6PCWLKlzznD.5MEg3F4GlrrBJJkEk.byq38C7q \
AgjHSqmwsGMGZ5yN48oLOMQXi9hEtraVpPtkv5xl.
```

Beispiel: Hashwert für „Chemnitzer Linux-Tage“

```
$6$$LfRk.b5duLePawDExTb7EPgOAb/W1Oyfg1/TU3FCtEe7o \
UrVhS.b8U3PEhAA7l.XKxSlgfyLxA3pZM2pz26Hv/
```

Faktorisierungsproblem

- Multiplizieren zweier – auch großer Zahlen – ist einfach.
- Zerlegung einer großen Zahl in Primfaktoren dagegen ist (noch?!) aufwändig (Faktorisierungsproblem).
- Beispiel von Martin Gardner im Scientific American (1977):
  Die 129stellige Zahl:
  114 381 625 757 888 867 669 235 779 976 146 612 010 218 296
  721 242 362 562 561 842 935 706 935 245 733 897 830 597 123
  563 958 705 058 989 075 147 599 290 026 879 543 541
  ist Produkt zweier Primzahlen. Wie lauten die Faktoren?
  $\Rightarrow$ erst nach 16 Jahren Lösung durch Paul Leyland (Universität Oxford), Michael Graff (Universität von Iowa) und Derek Atkins (Massachusetts Institute of Technology)
- Wegen der Asymmetrie auch Begriff der „Falltür“: leicht, in das Loch hineinzufallen, schwer wieder herauszukommen.

RSA (Rivest, Shamir und Adleman)

- Anwendung des Problems der Faktorisierung großer Zahlen
- 1977 von Ronald L. Rivest, Adi Shamir und Leonard Adleman ($\Rightarrow$ Name) am MIT entwickelt
- Asymmetrisches kryptographisches Verfahren, das sowohl zur Verschlüsselung als auch zur digitalen Signatur eingesetzt werden kann.
- Verwendet ein Schlüsselpaar aus einem privaten Schlüssel und einem öffentlichen Schlüssel zum Verschlüsseln oder zur Prüfung von Signaturen.
- Basiert auf einer Einwegpermutation mit Falltür, die gleichzeitig bijektiv ist (Permutation).

Berechnung der RSA-Schlüssel

1. Wähle zwei Primzahlen $p \neq q$
2. Berechne die Zahl $N = p \cdot q$
3. Berechne die Eulersche Funktion $\phi(N)$
   (mit bekannter Primfaktorzerlegung: $\phi(N) = (p - 1) \cdot (q - 1)$)
4. Wähle zu $\phi(N)$ eine teilerfremde Zahl e mit $1 < e < \phi(N)$
5. Berechne privaten Schlüssel d mit $d \cdot e \bmod \phi(N) = 1$

$\Rightarrow$ N und e bilden den öffentlichen Schlüssel
$\Rightarrow$ N und d bilden den privaten Schlüssel

Diskreter Logarithmus-Problem (DLP)

- Der diskrete Logarithmus entspricht in der Gruppen- und Zahlentheorie dem Logarithmus aus der Analysis. ($\Rightarrow$ Modul-Arithmetik)
- Die Schwierigkeit seiner Berechnung ist Grundlage der Sicherheit.
- Das Diskreter Logarithmus-Problem (DLP) beruht auf der Diskreter-Logarithmus-Vermutung:
  Die Exponentialfunktion exp_g mod p[1] ist für fast alle Basen g eine Einwegfunktion.

x	1	2	3	4	5	6
$\mathbf{3^x}$	3	9	27	81	243	729
$\mathbf{3^x (mod 7)}$	**3**	**2**	**6**	**4**	**5**	**1**

[1] p ist eine Primzahl, g eine Primitivwurzel einer primen Restklassengruppe modulo p

Diffie–Hellman Key Exchange (DHKE)

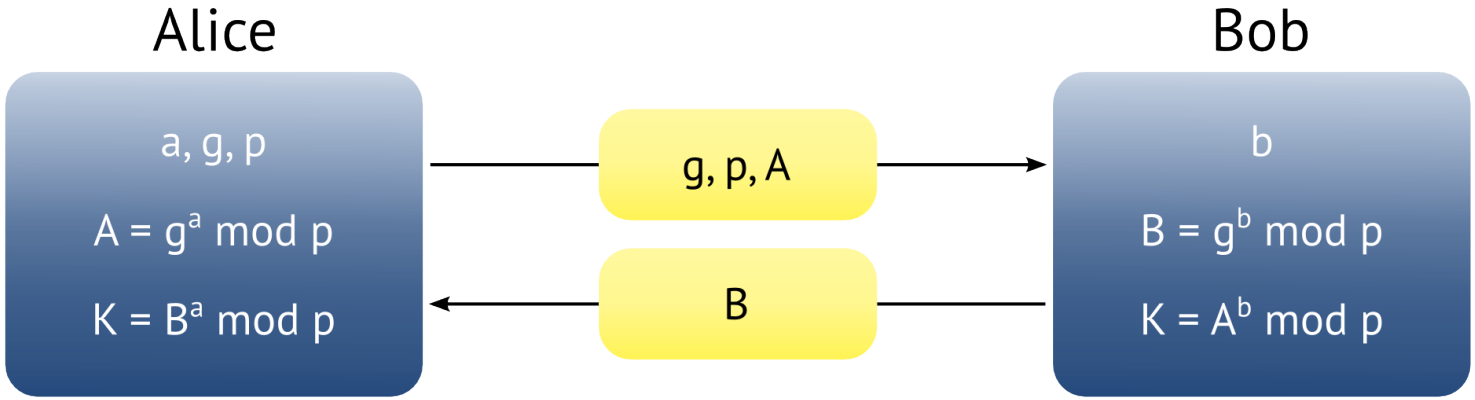
- basiert auf dem Diskreter Logarithmus-Problem (DLP)
- 1976 von Whitfield Diffie und Martin Hellman veröffentlicht
- nur Schlüsselaustauschprotokoll, kein Verschlüsselungsverfahren (dafür das DH-basierte ElGamal)
- häufig angewendet, u.a. bei:
  - Shell (SSH)
  - Transport Layer Security (TLS)
  - Internet Protocol Security (IPSec)

Diffie-Hellman-Schlüsseltausch – Funktionsweise

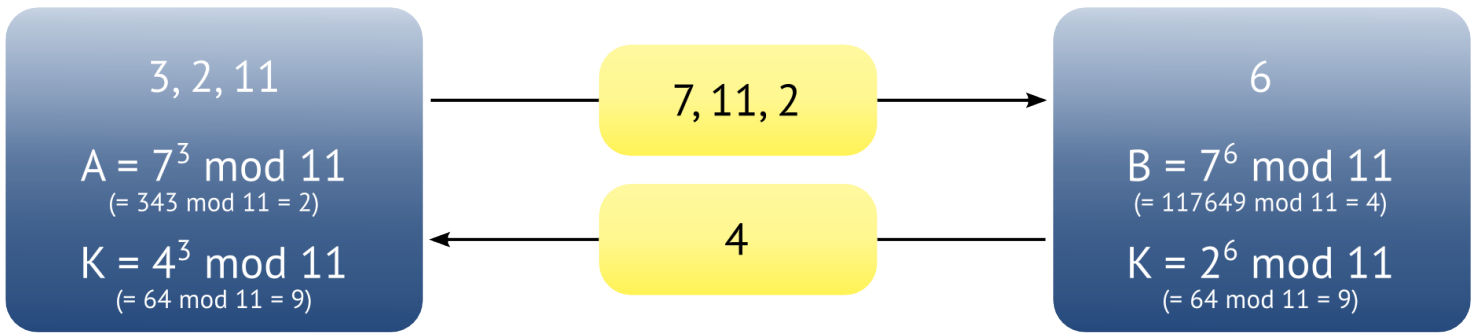
Problemstellung:
Alice und Bob wollen sich auf gemeinsamen Schlüssel K einigen, haben aber nur unsicheren Kommunikationskanal zur Verfügung.
Problemlösung:
(von Diffie und Hellman 1976 vorgeschlagen; beruht auf der Exponentialfunktion in endlichen Körpern, einer (mutmaßlichen) Einweg-Funktion :)

1. Alice und Bob einigen sich auf eine Primzahl p und eine Primitivwurzel g mod p mit $2 \leq g \leq p - 2$
2. Primzahl p und Primitivwurzel g können öffentlich bekannt sein.
3. Alice wählt natürliche Zahl $a \in 0,1, \ldots, p - 2$ zufällig und berechnet $A = g^a \bmod p$ und schickt A an Bob, hält aber ihren Exponenten a geheim.

Diffie-Hellman-Schlüsseltausch



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$



$K = 4^3 \bmod 11 = (7^3 \bmod 11)^6 = 7^{3x6} \bmod 11 = (7^6 \bmod 11)^3 \bmod 11 = 6^4 \bmod 11 = 9$

Anwendungen für kryptographische Verfahren

- Digitale Signaturen
- Secure Shell (SSH)
- SSL und TLS
- S/MIME
- Pretty Good Privacy (PGP)/GnuPG
- IPSec
- Electronic Commerce (SET, HBCI)
- ...

Digitale Signaturen

- Asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels (Private Key) zu einer digitalen Nachricht einen Wert berechnet.
- Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels (Public Key) die nichtabstreitbare Urheberschaft und Integrität der Nachricht zu prüfen.
- Daraus lassen sich sichere elektronische Signaturen ableiten. (fortgeschrittene elektronische Signaturen gem. § 2 Nr. 2 SigG bzw. qualifizierte elektronische Signaturen gem. § 2 Nr. 3 SigG)

Digitale Signatur

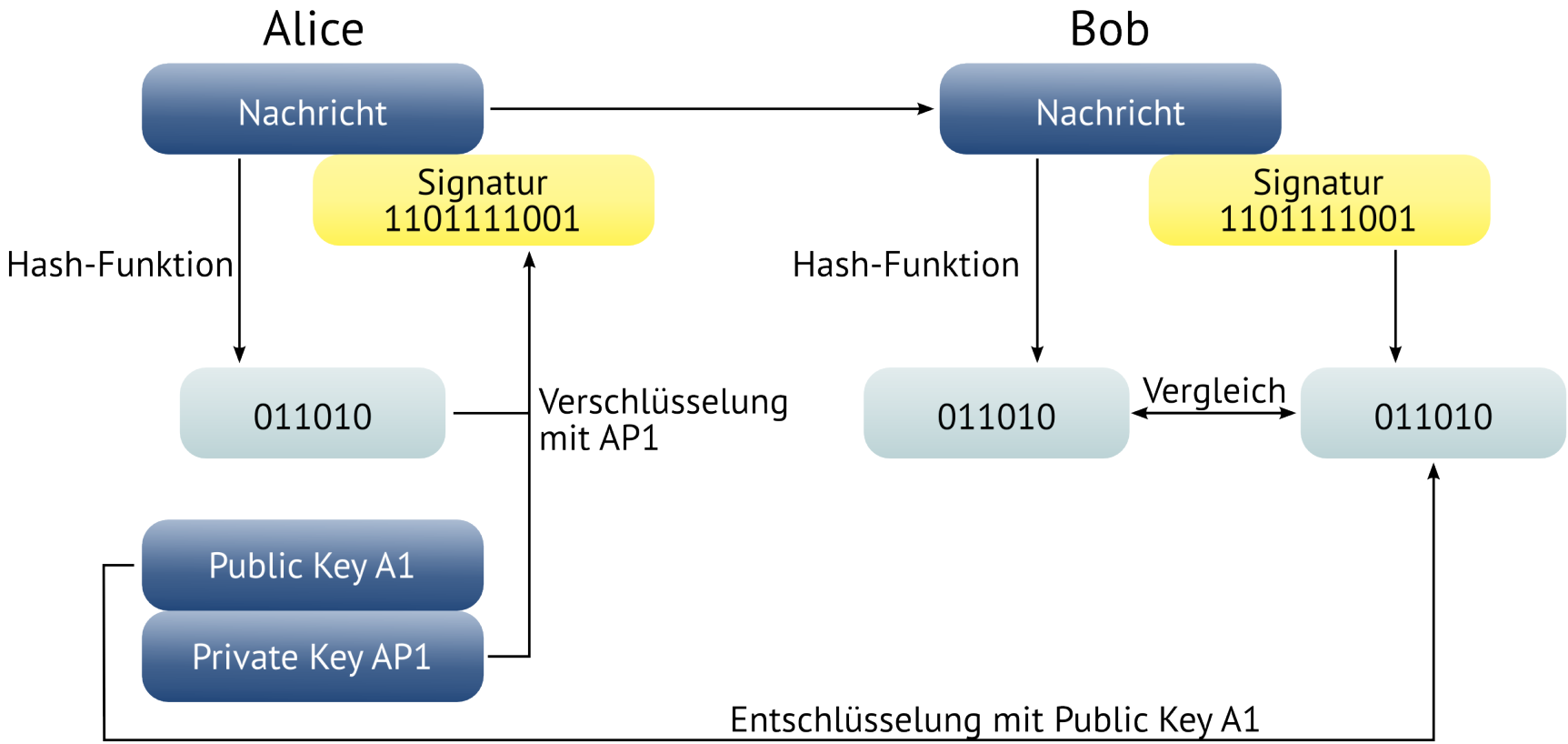


Abbildung : Digitale Signatur

Secure Shell (SSH)

- Meist für Zugriff auf entfernte Kommandozeile eingesetzt (z.B. zur Fernwartung).
- Zertifikatsbasierte Identifizierung per nutzt RSA, DSA oder ECDSA (SSH-2) zur Identifizierung.
- Authentifizierung wahlweise per Public-Key-Verschlüsselung oder mit gewöhnlichen Kennwort.
- Nach erfolgreicher Authentifizierung wird für die Dauer der Sitzung ein geheimer Schlüssel erzeugt, mit dem die weitere Kommunikation symmetrisch verschlüsselt wird. (mittels 3DES, Blowfish, Twofish, CAST, IDEA, u.a.)
- Aushandlung des Schlüssels ist unter bestimmten Bedingungen wiederholbar.
- IANA hat SSH den TCP-Port 22 zugeordnet.
- SSH-2 bietet weitere Funktionen wie Datenübertragung.

SSH – Verbindungsaufbau

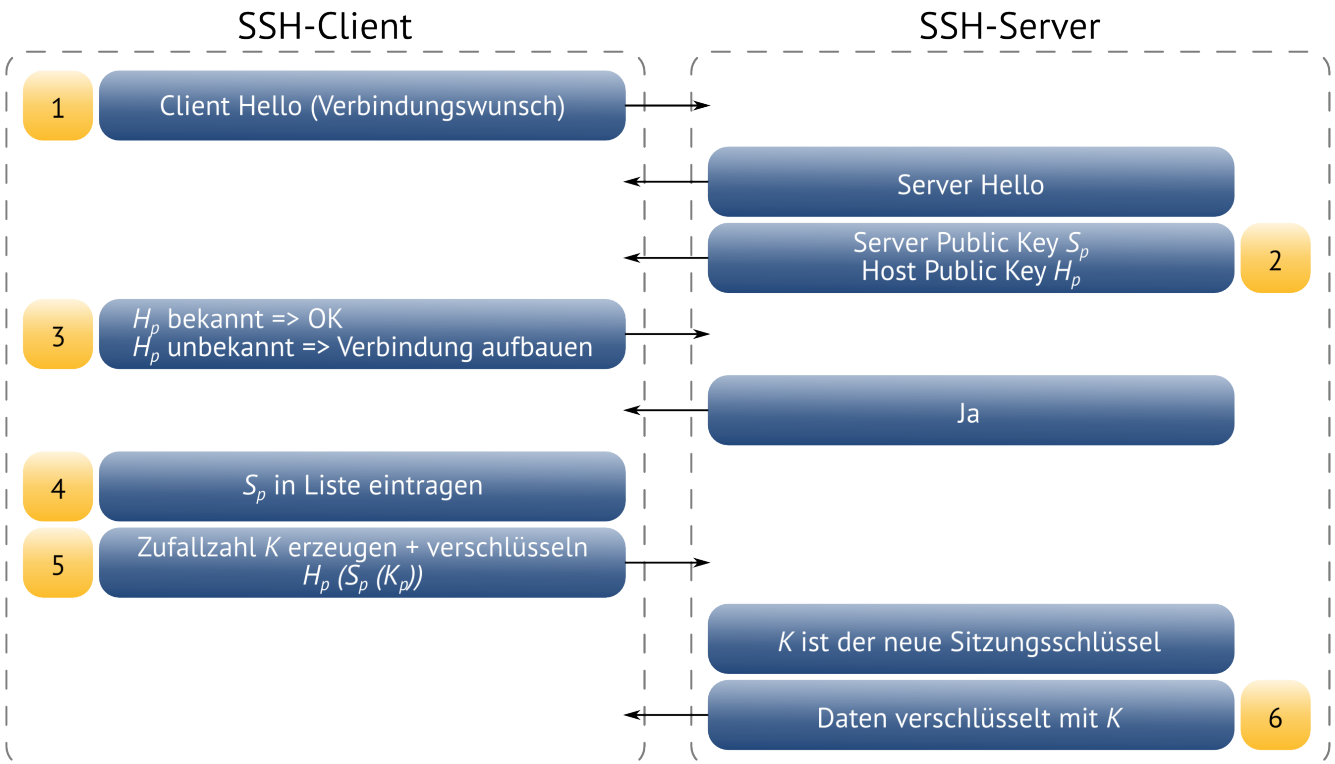


Abbildung : Aufbau einer SSH-Sitzung

Transport Layer Security (TLS)

- Hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet
- Diffie-Hellman-Schlüsselaustausch für Erzeugung eines gemeinsamen kryptographischen Schlüssels
- Schlüssel wird in der Folge zur symmetrischen Verschlüsselung genutzt
- Vorgänger Secure Sockets Layer (SSL); seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert
- Implementierungen: OpenSSL, GnuTLS, NSS, u.a.
- Verwendung auch bei HTTPS (Port 443)
- Ohne zertifikatsbasierte Authentifizierung anfällig für Man-In-The-Middle-Angriffe

Secure/Multipurpose Internet Mail Extensions

- Standard für Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein hybrides Kryptosystem
- *Cryptographic Message Syntax* beschreibt Verschlüsselung, Integritätsprüfung, Signatur beliebiger Nachrichten
- Nachrichtenformat besteht aus zwei Blöcken:
  - Daten mit MIME-Headers über welche die digitale Signatur erstellt wurde
  - Informationen, um die Signatur zu überprüfen
- Dienste auf Basis des Internet-MIME-Standards:
  - Authentifikation
  - Datenintegrität
  - Datenvertraulichkeit
  - Nachweis der Urheberschaft
- Alternative zu S/MIME: OpenPGP unter Verwendung einer PKI

S/MIME – Funktionsweise

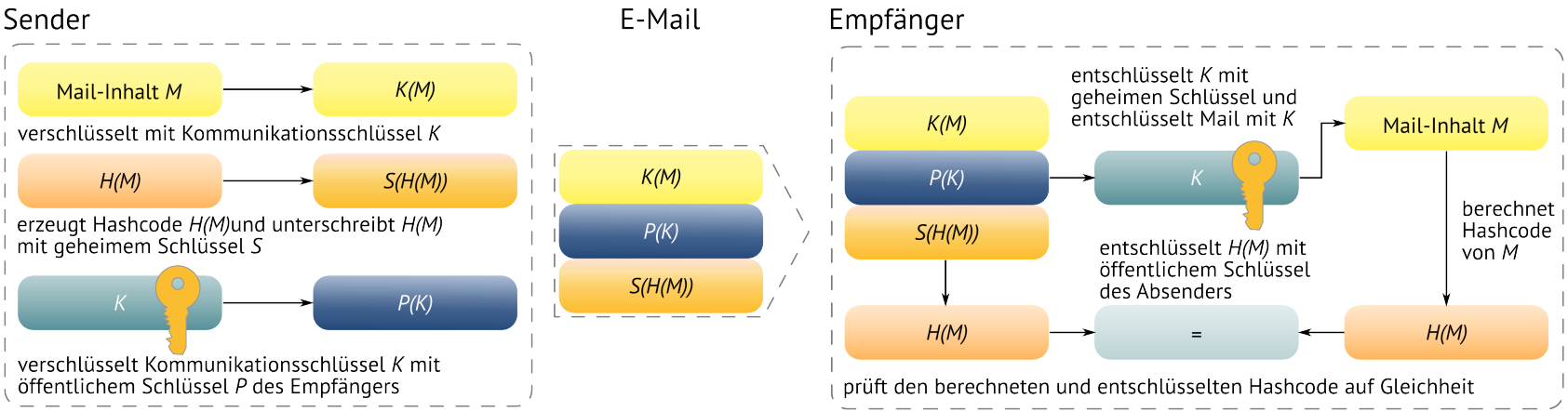


Abbildung : S/MIME

Pretty Good Privacy (PGP)

- 1991 von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten mit dem Ziel, alle Bürger und insbesondere Bürgerbewegungen vor dem Zugriff durch Geheimdienste zu schützen.
- Durfte bis Ende der 1990er Jahre nicht lizenzfrei aus den USA exportiert werden, da es wie Waffen unter das US-Exportgesetz fiel.
- Benutzt ein Public-Key-Verfahren (RSA-Algorithmus, später Elgamal-Algorithmus).
- Basiert auf dem *Web of Trust* (Vertrauen wird von den Benutzern selbst verwaltet, keine zentrale Zertifizierungsinstanz).
- Freie Implementierung des OpenPGP Standards: GnuPG

Zukunft: Kryptographie und Quantenphysik

Neue Situation durch die Anwendung von Erkenntnissen aus der Quantenphysik:

- Entschlüsseln bisheriger Verfahren durch die enorme Rechenleistung von Quantencomputern zukünftig möglich ?
  $\Rightarrow$ Alle Verfahren die auf Einwegfunktionen beruhen (z.B. RSA, TLS, SSH, ...) würden unbrauchbar.
- Verschlüsseln mit Quantenphysik (Quantenkryptographie):
  - Sichere Informationsübertragung durch Photonenübermittlung und Messung der Polarisation
  - Übertragung über Glasfaserkabel
  - Abhören würde in jedem Fall bemerkt werden
  - 1995 erfolgreicher Versuch der Universität Genf über eine quantenkryptographische Glasfaserverbindung (23 km)

Die Zukunft der Kryptographie

Abbildung : Quantenphysik und Sicherheit (Quelle: Physics World)

Zum Titel: Die Kopfrasur

Im antiken Griechenland wurde eine spezielle Form der Steganographie angewendet (nach Herodot):

- Sklaven wurde der Schädel geschoren.
- Anschließend die geheime Botschaft auf den Schädel gebrannt oder tätowiert.
- War das Haar wieder nachgewachsen, wurde er zum Empfänger geschickt.
- Dort wurde der Kopf erneut rasiert und die Botschaft konnte gelesen werden.

$\Rightarrow$ Beispiel für eine schlechte Kryptographie:
Methode benötigt viel Zeit, hat – bei ausgiebigerer Kommunikation – einen hohen Pro-Kopf-Verbrauch zur Folge und ist vor allem nicht ganz schmerzfrei ...

Quellen und weiterführende Literatur / Links

Diffie-Hellman-Schlüsselaustausch:
RFC 2631: „Diffie-Hellman Key Agreement Method“
`http://tools.ietf.org/html/rfc2631`

RSA:
Ronald L. Rivest, Adi Shamir, and Leonard Adleman: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“
`http://people.csail.mit.edu/rivest/Rsapaper.pdf`

Einer von vielen Enigma-Emulatoren:
`http://startpad.googlecode.com/hg/labs/js/enigma/enigma-sim.html`

Allgemein:
Albrecht Beutelspacher: „Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln“, Wiesbaden 2004
Simon Singh: „Geheime Botschaften“, München 2001

u.v.a.

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de
oder +49 (0)8457 - 931096