



**KBS EDV QBAK PHSE**

P.E., M.M.

# Gliederung

2

3

4

5

6



## Hashfunktionen

# Kryptographie im Altertum



## Skytale der alten Griechen

Band mit scheinbar  
willkürlichen Buchstaben  
Empfänger benötigt Stab mit  
richtigem Durchmesser



## Cäsar-Chiffre

Alle Buchstaben werden um  
bestimmte Zahl verschoben  
Verschiebungszahl  Schlüssel

# Kryptographie im 20. Jahrhundert



**Enigma**

Verwendung im 2. Weltkrieg

Mechanischer Mechanismus zur  
Verschlüsselung einzelner  
Buchstaben

Mehrere Walzen stellen  
elektrische Kontakte her

# Symmetrische Verschlüsselung

Hashfunktionen



# Kryptographie in der IT

## Symmetrische Verschlüsselung



# Kryptographie in der IT

## Symmetrische Verschlüsselung



# Kryptographie in der IT

## Symmetrische Verschlüsselung



# Kryptographie in der IT

## Symmetrische Verschlüsselung

Beispielsalgorithmen:

DES(„Data Encryption Standard“): Veröffentlicht 1975;

gilt als unsicher wegen kurzer Schlüssellänge

Triple-DES(3DES)(=DES 3 mal hintereinander  
ausgeführt)

Blowfish: Veröffentlicht 1993,

AES(„Advanced Encryption Standard“)/Rijndael:

Veröffentlicht 1998; Nachfolger des DES; gilt als sehr  
sicher

# Kryptographie in der IT

## Symmetrische Verschlüsselung

Anwendung:

Lokale Dateiverschlüsselung/Laufwerksverschlüsselung  
Transportverschlüsselung, wenn beide Partner den  
gemeinsamen Schlüssel kennen

Vorteil:

Arbeitet schnell und schon bei mittleren  
Schlüssellängen sehr sicher

Nachteil:

Problem des Schlüsselaustauschs, nur wenn beide  
Partner den Schlüssel über ein sicheres Medium kennen  
ist dieses Verfahren sicher

# Asymmetrische Verschlüsselung



Hashfunktionen



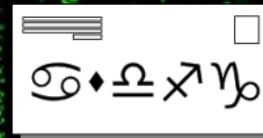
# Kryptographie in der IT

## Asymmetrische Verschlüsselung



# Kryptographie in der IT

## Asymmetrische Verschlüsselung



Verschlüsseln der Nachricht mit  
öffentlichen Schlüssel des  
Empfängers



# Kryptographie in der IT

## Asymmetrische Verschlüsselung

Beispielsalgorithmen:

RSA (1977): Primfaktorzerlegung als Grundlage

McEliece (1978): Goppa-Codes (z.B. Hyperelliptische Kurve) aus Generatormatrix

Elgamal (1985): Diskreter Logarithmus

Anwendung:

Verschlüsselung über unsicheres Medium (z.B. Schlüsselaustausch)

Authentifizierungen und der Sicherung der Integrität

# Kryptographie in der IT

## Asymmetrische Verschlüsselung

### Vorteil

Relativ hohe Sicherheit

Kein Schlüsselverteilungsproblem, da Public Key für jeden ohne Probleme zu erreichen ist.

Möglichkeit der Authentifikation durch elektronische Unterschriften (digitale Signaturen)

### Nachteil

Verfahren beruhen auf unbewiesenen mathematischen Annahmen

Sehr langsam, bis zu 10.000 langsamer als symmetrische Verfahren

# Hashfunktionen



## Hashfunktionen

# Kryptographie in der IT

## Hashfunktionen

Bildet eine große Menge auf eine kleine Zielmenge ab (z.B. Quersumme)

Funktioniert nur in eine Richtung

Ändert sich bei jeder Änderung der Quellmenge (auch bei kleinsten Veränderungen)

### Anwendung:

Sicheres Abspeichern und Vergleichen von Passwörtern

Als Prüfsumme, um große Mengen oder Nachrichten auf Veränderung zu prüfen

### Mechanismen

MD5 (Message-Digest Algorithm) □ 128 Bit Hashwert

Sicherheitsschwächen durch Kollisionsberechnung

SHA-3 (Secure Hash Algorithm) □ Schneller und sicherer als MD5

# Zertifikat

## Hashfunktionen



# Kryptographie in der IT

## Zertifikate

Zertifikatsinhaber

Zertifizierungsstelle

Zertifikat



- Land
- Stadt
- Organisation, etc.

Öffentlicher Schlüssel.



# Kryptographie in der IT

## Zertifikate



Prüfsumme.

Verschlüsselte  
Prüfsumme

# Kryptographie in der IT

## Zertifikate



Entschlüsselte  
Prüfsumme

=

ü

Kann die Häufigschlüssel mit  
Prüfsummen in Schritten  
Entschlüsselt werden?



# Signaturen

## Hashfunktionen



# Kryptographie in der IT

## Signatur



Senden des öffentlichen  
Öffentlicher  
Schlüssels über unsicheren Kanal



Privater  
Schlüssel PC1

# Kryptographie in der IT

## Signatur



# Kryptographie in der IT

## Signatur



Senden der  
unsicheren



# Kryptographie in der IT

## Signatur



Berechnen der Prüfsumme  
der Nachricht  
Entschlüsseln der  
mitgeschickten Prüfsumme



Prüfsumme

# Kryptographie in der IT

## Signatur



Vergleichen der beiden

Prüfsummen

Falls Prüfsummen gleich  
sind, wurde die Nachricht  
nicht verändert



HALLO

Prüfsumme



Prüfsumme



# Anwendung

## Hashfunktioner



# Kryptographie in der IT Anwendung: HTTPS



Zusätzliche Schicht zwischen TCP und HTTP  
Entwickelt von Netscape 1994  
Kommunikation zwischen Webserver und Browser  
Dient zur Verschlüsselung(Vertraulichkeit) und  
Authentifizierung(Authentizität)

# Kryptographie in der IT Anwendung: HTTPS

## Vorbereitung

Zertifizierungsstelle(CA) generiert Public/Private-Schlüsselpaar.

Dann wird ein Zertifikat(das den Public-Key enthält) erstellt und veröffentlicht.

Die Browserhersteller müssen das Zertifikat als Stammzertifizierungsstelle in ihre Browser integriert.

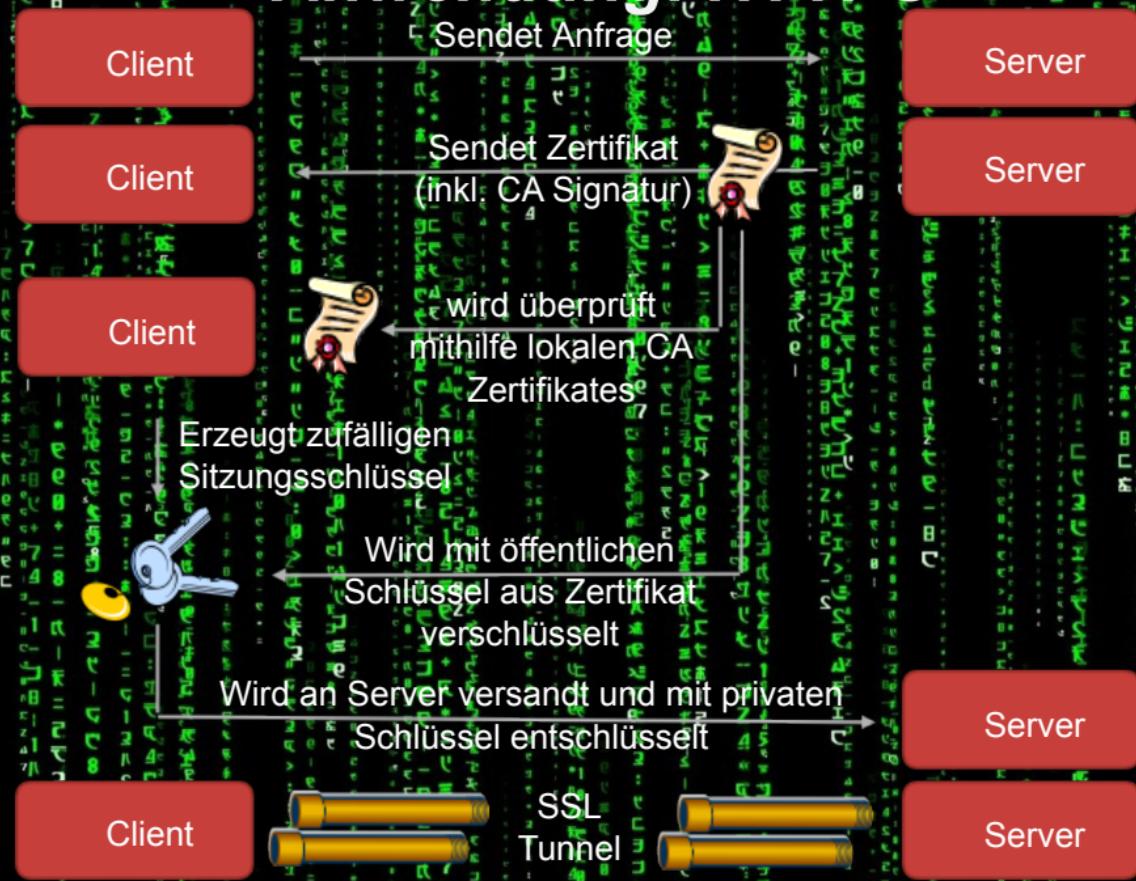
Webserver generiert Public/Private-Schlüsselpaar.

Dann wird ein Zertifikat(das den Public-Key enthält) erstellt.

Dieses wird von der CA unterschrieben. -> Wer der CA vertraut, darf diesem Zertifikat auch vertrauen.

# Kryptographie in der IT

## Anwendung: HTTPS



# Kryptographie in der IT

## Anwendung: Festplattenverschlüsselung

# Betriebssystem

10010001000100110010001000 In Echtzeit entschlüsselte Festplatte

Treiber

Heade

Verschlüsselte Festplatte z.B. AES, Blowfish, Double Blowfish, ...

## Zufälliger Schlüsse

## Passwort

# Kryptographie in der IT

## Anwendung: WLAN

**WEP:** XOR Verknüpfung jeden Bits mit einem symmetrischen Schlüssel

**WPA:** Schlüsselaustausch über PSK  
Verschlüsselung mit TKIP/MIC (individuell)

**WPA2:** Schlüsselaustausch über PSK  
Verschlüsselung mit AES (individuell)

# Kryptographie in der IT Anwendung: *Bitcoin*

Schürfen neuer Bitcoins.

Ausgangswert

Hashwert

Versenden von Bitcoins

Bitcoin  
(Ausgangswert)

Transaktionsinfo  
(Empfänger)

Signatur



# Angriffsmöglichkeiten

## Hashfunktionen



# Kryptographie in der IT

## *Regeln einer sicheren Verschlüsselung*

Eine sichere Verschlüsselung muss folgenden Szenarien standhalten:

Stufe: Der Angreifer kann **beliebig viele Pakete mitlesen**

Stufe: Der Angreifer kann beliebig viele Pakete mitlesen und kennt deren **Quellinformation**

Stufe: Der Angreifer kann beliebig viele Pakete **selbst generieren**

# Kryptographie in der IT

## Angriffsmöglichkeiten

Zufallszahlengeneratoren können manipuliert werden □ Zufallszahlen werden vorhersehbar

Schlüssel wird vorhersehbar

Mathematisches Problem von asymmetrischen Verfahren kann gelöst werden

Schnellere Rechner (z.B. Quantencomputer) können schneller Brutforceattacken ausführen

Unsichere Zertifizierungsstellen

Aber: Die beste Methode helfen oft nichts wenn der User zu freizügig mit seinen Daten umgeht oder ein unsicheres Passwort wählt.

# Kryptographie in der IT

## Angriffsmöglichkeiten: Man in the Middle



# Kryptographie in der IT

## Angriffsmöglichkeiten: Man in the Middle



# Kryptographie in der IT

## Angriffsmöglichkeiten: Man in the Middle



# Kryptographie in der IT

## Angriffsmöglichkeiten: Man in the Middle



Angriffsmöglichkeit: Man in the Middle  
so genannte Man-in-the-Middle-Angriffe

# Kryptographie in der IT

## Fragen

Warum kann man asymmetrische Verschlüsselung nicht immer einsetzen, sondern muss oft symmetrische Verschlüsselung verwenden?

Siehe Nachteile asymmetrische Verschlüsselung

Nenne je einen Algorithmus zur symmetrischen und asymmetrischen Verschlüsselung.

z.B. AES(symmetrisch), RSA(asymmetrisch)

Wozu braucht man bei HTTPS Stammzertifizierungsstellen?

Die Stammzertifizierungsstellen signieren die Zertifikate der Webseiten, sodass die Browser wissen, dass die Zertifikate vertrauenswürdig sind.