Vorlesung Kryptographie

Teil 2

Dr. Jan Vorbrüggen

Übersicht

- Teil 1
  - (Nicht-) Ziele
  - Steganographie vs. Kryptographie
  - Historie
  - Annahmen
  - Diffie-Hellman
  - Angriffe
- Teil 2
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hashverfahren
  - Alles zusammen: elektronische Signatur
  - Rechtliche Aspekte
  - Standards
  - Komplexe Anwendungen
  - So bitte nicht!

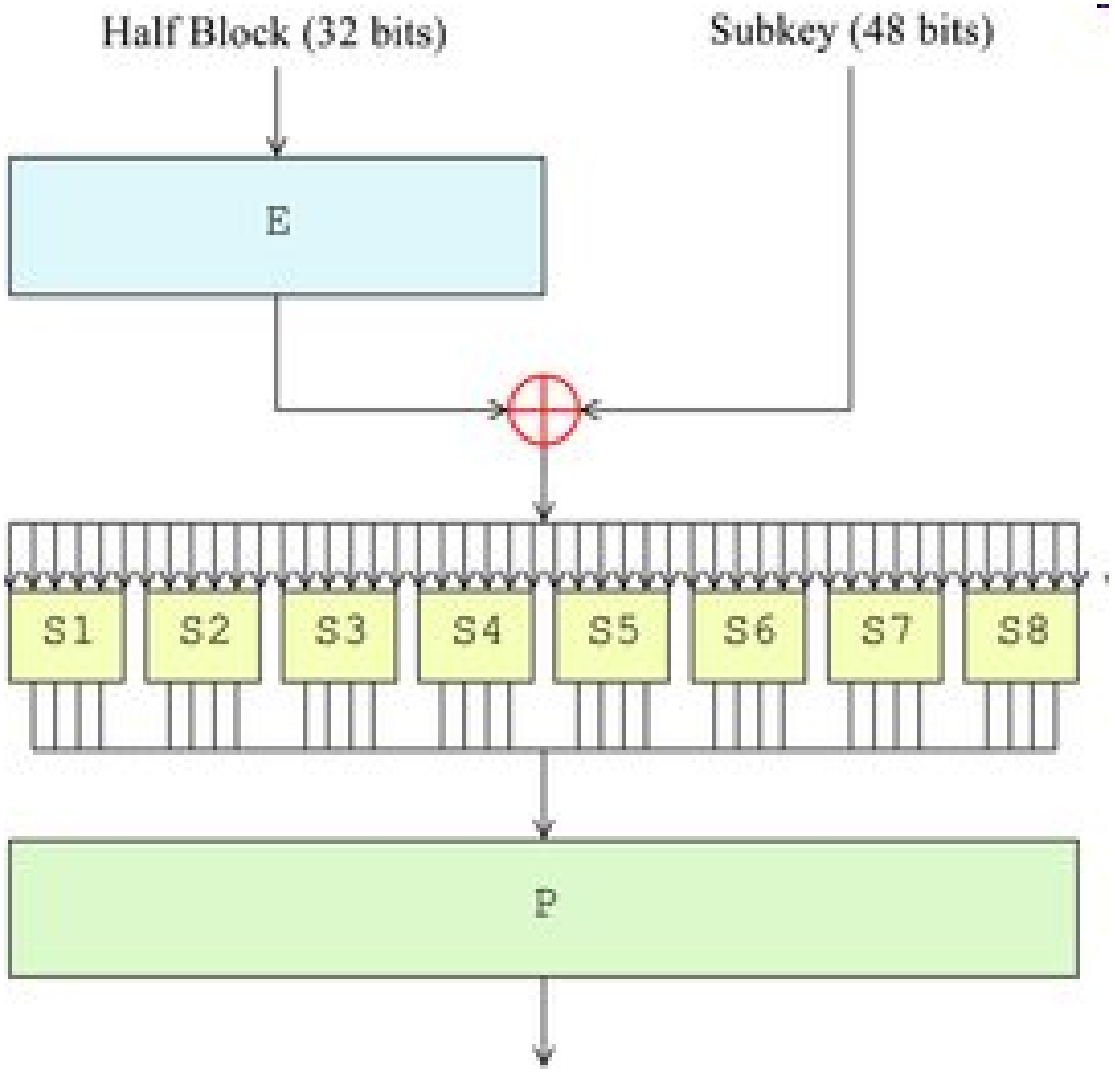
Symmetrische Verfahren

- Ziel: Sicherstellung der Vertraulichkeit
- Eigenschaften
  - Ein gemeinsamer Schlüssel für Ver- und Entschlüsselung
  - Sicherheit beruht auf Unkenntnis des Schlüssels
  - Schutz insbesondere vor Klartext-Angriffen und differentieller Kryptoanalyse

Vor- und Nachteile

- Vorteile
  - schnell
    - ca. 1000mal im Vergleich zu RSA
    - „wire speed“
    - Implementierung in Hardware möglich
  - block- oder strom-orientiert
- Nachteile
  - Schlüssel-Erzeugung
  - Schlüssel-Austausch

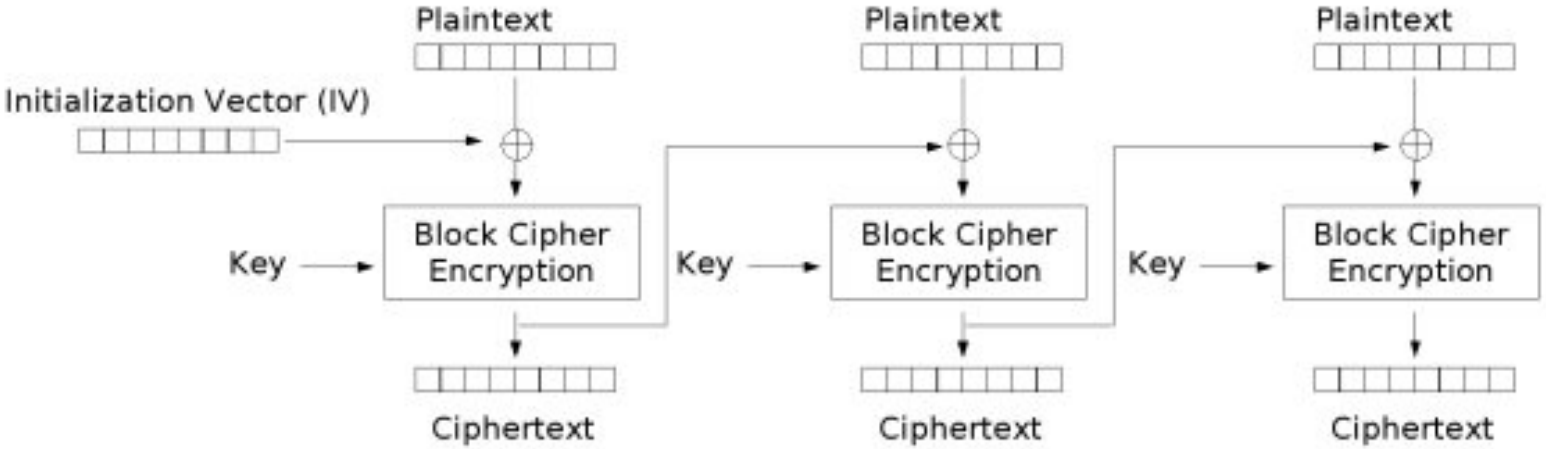
Operationen am Beispiel DES



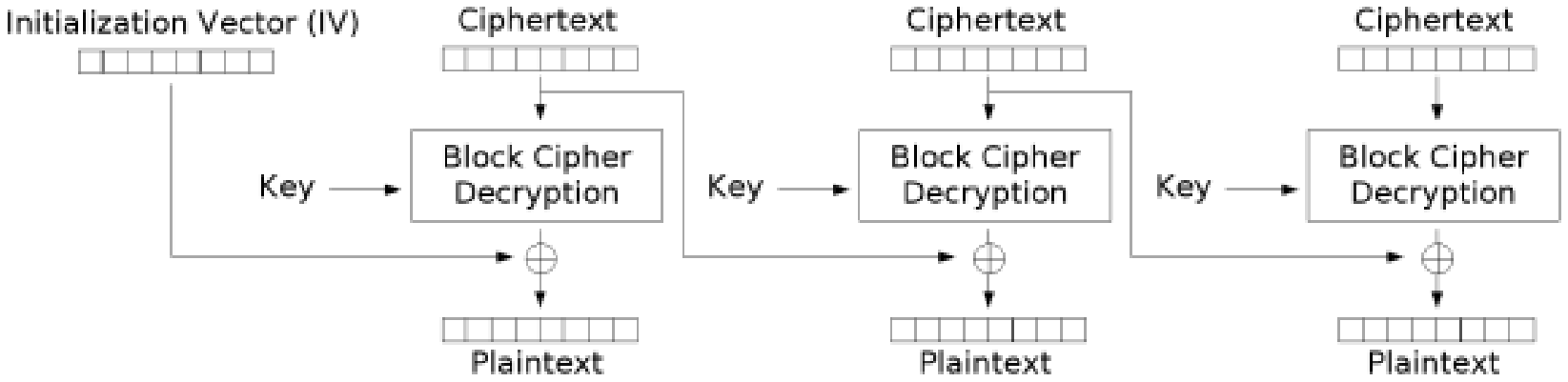
Klassen von sym. Chiffren

- Blockchiffren
  - Eine Dateneinheit wird verschlüsselt
  - Eine Dateneinheit ist typischerweise 128 bit, unabhängig von der Schlüssellänge
  - Damit ist Chiffre eine Bijektion aus der Menge der $2^{128}!$ möglichen Permutationen
  - $\Rightarrow$ Der Schlüssel sollte mindestens 128 bit sein
- Stromchiffren
  - wenn Datenmenge unbekannt und variabel
  - z.B.: RC4 in WiFi, A5/1 und A5/2 bei GSM

CBC – *cipher block chaining*



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Beispiele

- DES – digital encryption standard, 1976
  - 64 bit Blocklänge
  - 56 bit Schlüssellänge
- Triple DES
  - Effektive Schlüsselänge 112 bit
- AES – advanced encryption standard
  - Nach 5 Jahren Evaluierung 2001 standardisiert
  - 128 bit Blocklänge
  - 128, 192, 256 bit Schlüssellänge
  - Multiplikative Inverse über GF(2^8)

Asymmetrische Verfahren

- Grundidee:
  - Verschlüsselung und Entschlüsselung benötigen verschiedene Schlüssel
  - Der eine Schlüssel kann aus dem anderen errechnet werden…
  - …aber nicht umgekehrt!
- Mögliche Grundlagen:
  - Faktorisierung großer Zahlen: RSA
  - diskreter Logarithmus: ECC
    - *elliptic curve cryptography*

Eigenschaften

- RSA
  - etabliert, gut untersucht
  - standardisiert, viele Implementierungen
  - langsam
  - Schlüssellängen 1024, 2048 Bit und mehr
- ECC
  - nicht so etabliert, recht gut untersucht
  - gerade standardisiert, nicht so viele Impl.
  - schneller als RSA – Faktor 3-5
  - Schlüssellängen 160-384 Bit
  - *nonce* erforderlich

Anwendungsszenarien

- Elektronische Signatur:
  - Verschlüsselung mit dem privaten Schlüssel, Entschlüsselung mit dem öffentlichen Schlüssel
- Verschlüsselung an Empfänger
  - Verschlüsselung mit dem öffentlichen Schlüssel, Entschlüsselung mit privaten dem Schlüssel

Zur Erinnerung: Ziele von Kryptographie

- Vertraulichkeit / confidentiality
- Änderungsschutz / integrity
- Fälschungsschutz / authenticity

- Nicht-Abstreitbarkeit / non-repudiation
- Erneuerbarkeit / renewability

Ein Beispiel

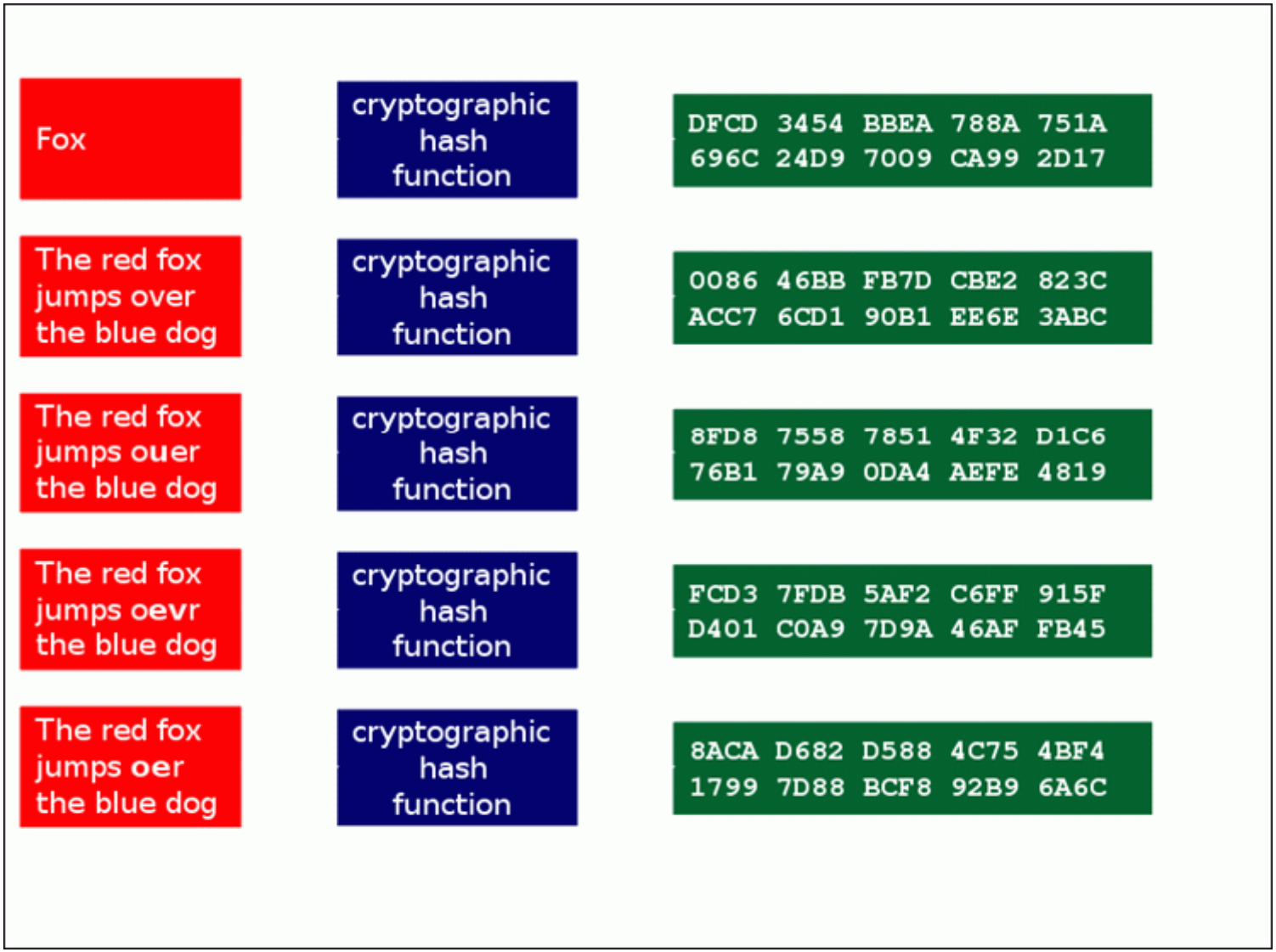
- Sie möchten einen vertraulichen Brief per e-mail versenden
- Nur der Empfänger soll ihn lesen können
  - Vertraulichkeit bei Übertragung *und* Speicherung
- Der Empfänger soll die Nachricht Ihnen eindeutig zuordnen können
- Übertragungsfehler sollen erkannt werden
- PKI o.ä. wird vorausgesetzt
- Einfache und optimierte Varianten erwünscht

Das entwickeln wir jetzt an der Tafel

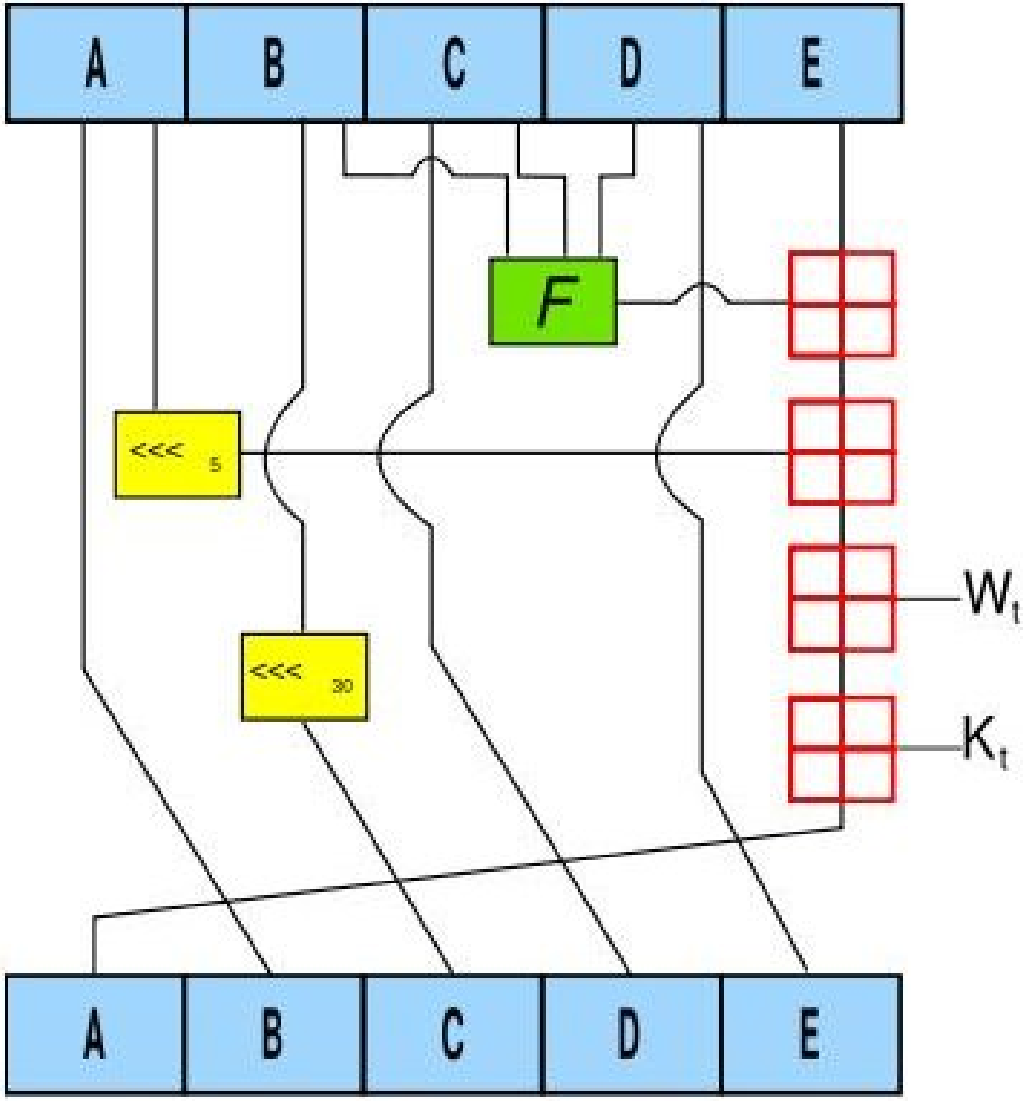
Kryptographische Hashverfahren

- Zweck: Reduziere beliebige Menge an Daten auf eine feste Menge mit folgenden Eigenschaften:
  - leicht zu berechnen
  - schwierig zu invertieren
  - schwierig, Änderung der Daten ohne Änderung des Hashwertes zu erreichen
  - Kollisionsfrei
- Deterministisch, d.h. benötigt keinen Schlüssel
- Synonyme: Hashwert, *(message) digest*

Beispiel – SHA-1



Was macht ein Hash „inside“?



Anwendungen

- Integrität von Nachrichten
- Identifikation von Dateien
- Speicherung und Prüfung von Passwörtern
- Erzeugung von Pseudozufallszahlen

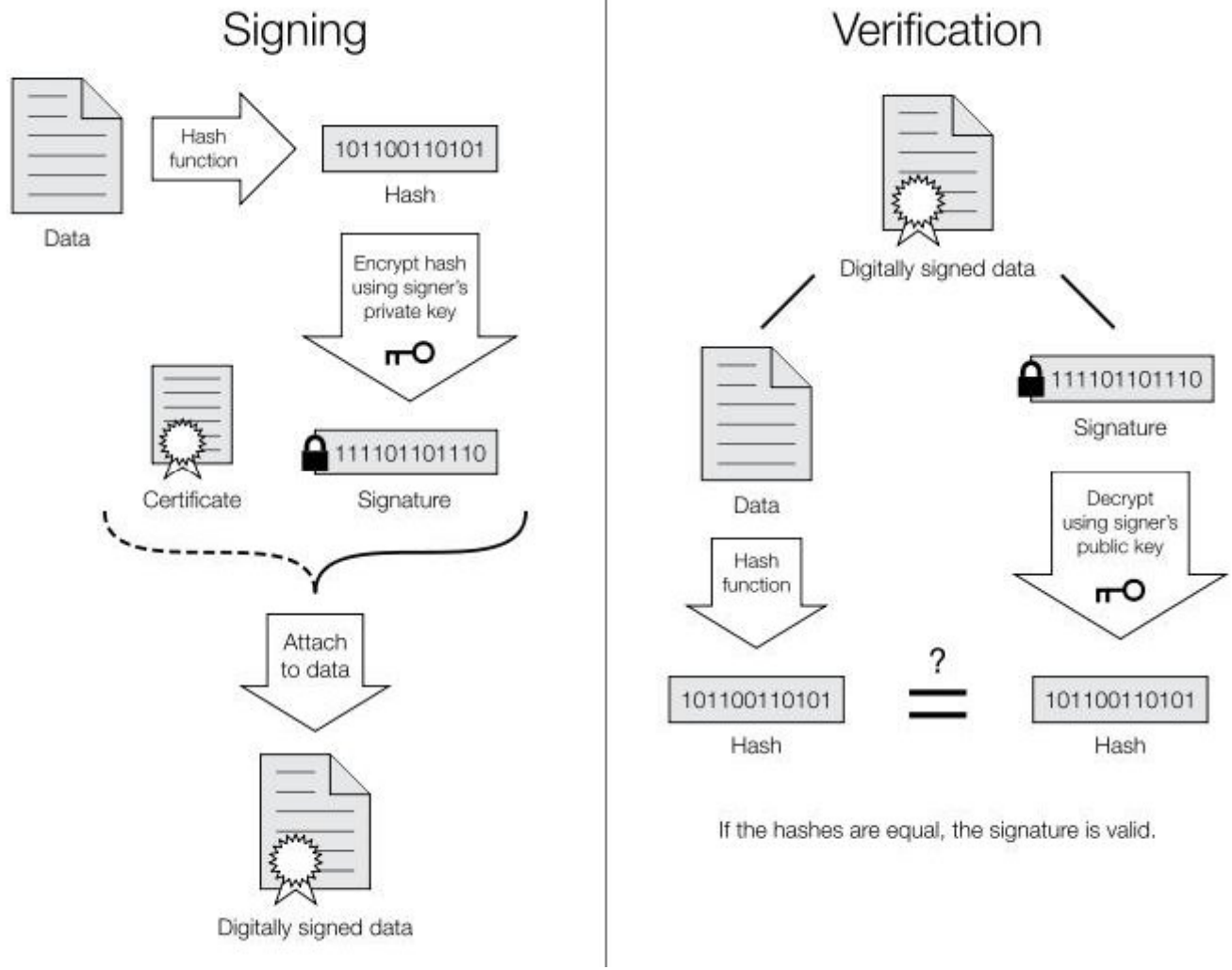
Bekannte Algorithmen

- MD5 (Rivest, 1991): 128 bit, kompromittiert
- RIPEMD-160 (KUL, 1996): 160 bit
- SHA-1 (NSA, 1995): 160 bit, Schwächen identifiziert
- SHA-256 (NSA, 2000): 256 bit
- SHA-512: gleiche Familie wie SHA-256

Alles zusammen: die elektronische Signatur

- Ziel: ersetze die Unterschrift des Ausstellers unter ein Dokument
  - Integrität
  - Authentizität
  - Nicht-Abstreitbarkeit
- Kein Ziel: Vertraulichkeit

Ablauf


Signing
Data
Hash function
101100110101
Hash
Encrypt hash using signer's private key
Certificate
111101101110
Signature
Attach to data
Digitally signed data
Verification
Digitally signed data
Data
111101101110
Signature
Hash function
Decrypt using signer's public key
?
101100110101
Hash
101100110101
Hash
If the hashes are equal, the signature is valid.

Komponenten

- kryptographische Hashfunktion
- asymmetrische Verschlüsselung
- *Zertifikat* mit öffentlichem Schlüssel
- asymmetrische Entschlüssellung
- PKI – *public key infrastructure*:
  - Zertifikatskette
  - „certificate authority“ – CA
  - Wurzel-Zertifikat

Probleme und Schwächen

- Wurzel-Zertifikate
- Gesperrte Zertifikate
- Speicher für den privaten Schlüssel
- WYSIWYS: *what you see is what you sign*
  - Was ist die Semantik der signierten Bits?
  - Wie kann ich der Darstellung auf meinem Bildschirm vertrauen?

Zeitstempel

- Ein elektronische Signatur hat keine zeitliche Lokalisierung
- Daher wird sie ungültig, wenn das zu Grunde liegende Zertifikat ungültig wird
- Lösung:
  - verlässliche Zeitangabe mit in Signatur aufnehmen
  - $\Rightarrow$ Zeitstempeldienst, in DE von Timeproof

Rechtliche Aspekte

- Darf ich überhaupt verschlüsseln?
- Darf ich mit Verschlüsselung handeln?
  - ITAR, …
- Welche Rechtsposition haben verschlüsselte Daten?

Elektronische Signatur

- Signaturgesetz (SigG) und –verordnung (SigV)
- Entsprechende EU-Richtlinie
- Definieren
  - einfache
  - fortgeschrittene
  - qualifizierte

  elektronische Signatur

Rechtposition der elektronischen Signatur

- Eine qualifizierte elektronische Signatur ist für alle Rechtsgeschäfte der handschriftlichen Signatur gleichgestellt. (BGB)

- Elektronische Rechnungen müssen mit einer qualifizierten elektronischen Signatur versehen werden – UStG, AO

Standards

- ISO / CEN / DIN
  - international / europäisch / deutsch
  - Genf / Brüssel / Berlin
- ITU-T / CCITT
  - Telekom-Industrie, international
  - Xnnn-Standards, z.B. X.400, X.509
  - ASN.1, H.264 (Video-Komp.), T.xx (Fax), …
- IETF – Internet Engineering Task Force
  - RFC – *Request for Comment*
- PKCS – Public Key Security Standards
  - Industriestandard von RSA Data Security Corp.
  - wird abgelöst, z.B. PKCS #11 $\Rightarrow$ CMS (IETF)

Komplexe Anwendungen

- SSL v3 / TSL v1
  - Industriestandard von Netscape / IETF-Draft
  - „secure sockets layer“ / „transport layer security“
  - Ende-zu-Ende-Verschlüsselung / App-Ebene
- Eigenschaften
  - Verhandlung der gemeinsamen Fähigkeiten
  - Authentisierung: Server, Client möglich
  - *confidentiality* und *integrity* der Daten
  - Schutz vor man-in-the-middle, replay-Angriff

Ablauf einer SSL-Verbindung

- *peer-to-peer negotiation* der Algorithmen – „*handshake*“
- Authentisierung
- Schlüsselerzeugung und -austausch
- Datenaustausch
  - symmetrisch verschlüsselt
  - einzeln authentisiert
- Definiertes Ende der Transaktion

IPSec / IKE

- Analog zu TSL, aber auf Netzwerkebene
- Anwendungsbereiche:
  - Virtuelles Intranet (gateway-to-gateway)
  - VPN (client-to-gateway)
- Details s. Wikipedia-EN

So bitte nicht!

- SSL v2
- WEP
- X.509 v3

SSL v2

- Unzureichender Schutz vor *MitM*-Angriff
  - kein Schutz der initialen Vereinbarung
- Verschlüsselung und MAC nutzen den gleichen Schlüssel
- Schwache symmetrische Chiffren u. MACs
- TCP FIN und Verbindungsende auf SSL-Ebene identisch

WEP

- Erster Versuch, WLAN gegen Abhören abzusichern
- Wesentliche Fehler:
  - Schlüsselraum zu klein $\Rightarrow$ *brute-force*-Angriff
  - Implementierung zu naiv $\Rightarrow$ *plain-text*-Angriff
- Details s. Wikipedia-EN/-DE

X.509 v3

- Legt Struktur von Zertifikaten (PKI) fest
- Ungenaue Definition von Feldern etc.
  - mangelnde Interoperabilität
- Semantik nicht ausreichend definiert
  - unklare Definition der Einsatzbereiche
  - damit unklare rechtliche Einschätzung
  - Beispiele:
    - X400-Namensfelder
    - Attribute