Assymetrische Kryptographie

Grundlagen

Berufsförderungswerk Berlin-Brandenburg e.V.

Asymmetrische Kryptographie

Übersicht

Berufsförderungswerk Berlin-Brandenburg e.V.

Griechisch: *kryptós*, deutsch ‚verborgen', ‚geheim'
gráphein, deutsch ‚schreiben'

Wissenschaft der Verschlüsselung / Informationssicherheit

Methoden:

- **symmetrisch (secret key / shared secret)**
- **asymmetrisch (public key)**
- **hybrid (asymmetrisch + symmetrisch)**

Asymmetrische Kryptographie

Übersicht

Berufsförderungswerk Berlin-Brandenburg e.V.

Problem:

- Unsicherer Kanal
- Symmetrischer Schlüssel gefährdet

Lösung:

- Asymmetrische Verschlüsselung
- Öffentlicher Schlüssel: verschlüsseln
- Privater Schlüssel: entschlüsseln

Nachteil:

Rechenaufwändig, langsamer als symmetrische Verschlüsselung

Asymmetrische Kryptographie

Geschichte

Berufsförderungswerk Berlin-Brandenburg e.V.

1976: Stanford University

- **Whitfield Diffie, Martin E. Hellman, Ralph Merkle**
- **Diffie-Hellman-Merkle-Schlüsselaustausch**

1977: MIT

- **Ronald Rivest, Adi Shamir, Leonard Adleman**
- **Asymmetrisches Kryptosystem, 1983 patentiert (ausgelaufen)**

Vorläufer 1969: britischer Geheimdienst:

- **James H. Ellis, Clifford Cocks, Malcolm J. Williamson**
- **Nie veröffentlicht, 1997 bekannt geworden**

Assymetrische Kryptographie

Prinzip

Berufsförderungswerk Berlin-Brandenburg e.V.

Privat

Öffentlich

Assymetrische Kryptographie

Prinzip

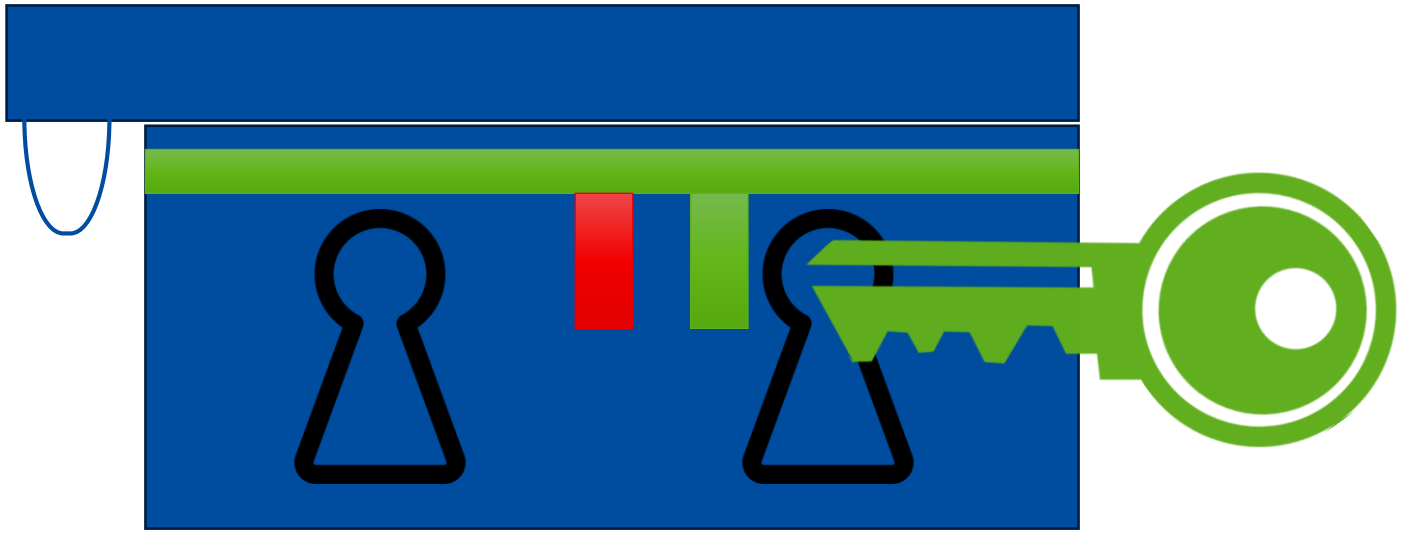
Berufsförderungswerk Berlin-Brandenburg e.V.

Geheimnis

Assymetrische Kryptographie

Prinzip

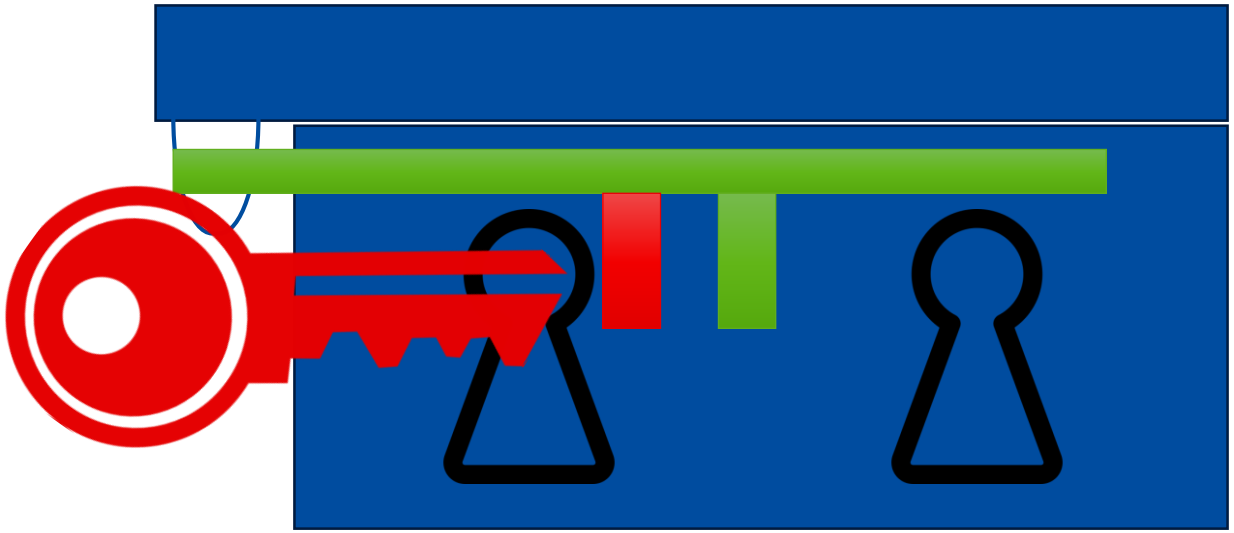
Berufsförderungswerk
Berlin-Brandenburg e.V.



Assymetrische Kryptographie

Prinzip

Berufsförderungswerk
Berlin-Brandenburg e.V.



Asymmetrische Kryptographie

Grundlage

Berufsförderungswerk Berlin-Brandenburg e.V.

Mathemathematische „Einweg“-Verfahren,

- **Umkehrung lässt sich nicht effizient berechnen**
- **Beispiele:**
  - **Primfaktorenzerlegung großer Zahlen**
  - **Schnittpunkte elliptischer Kurven mit Geraden**

Berufsförderungswerk Berlin-Brandenburg e.V.

X.509

- **Standard der Internationalen Fernmeldeunion engl.** International Telecommunication Union (ITU)
- **beschreibt eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate.**

Berufsförderungswerk Berlin-Brandenburg e.V.

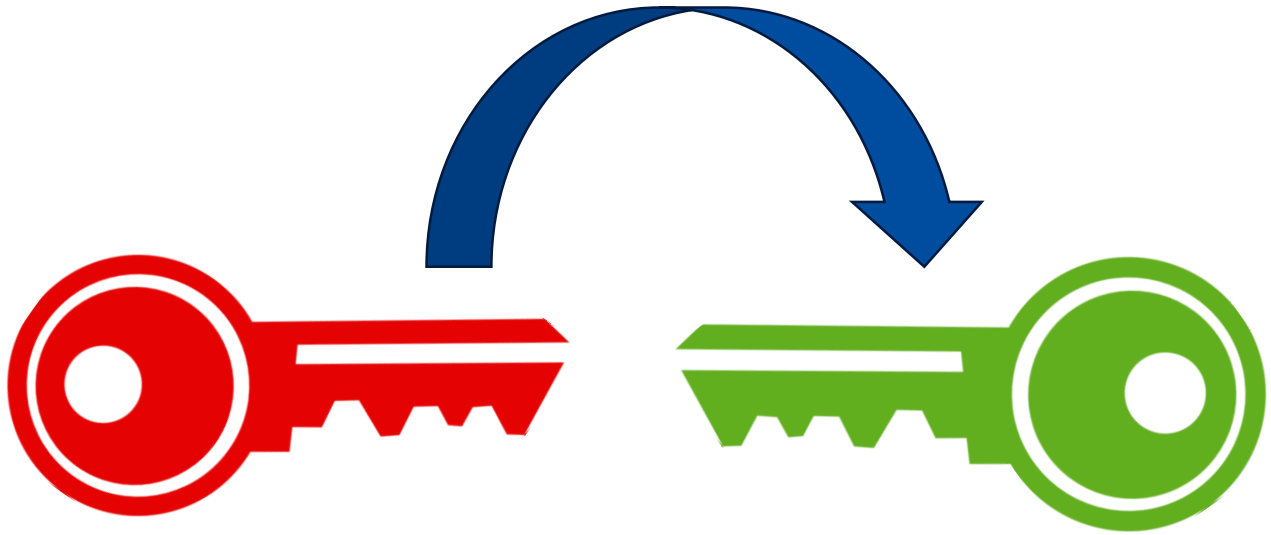
Bestandteile

- **Zertifikate (*certificate*)**
- **Zertifizierungsstelle (*Certificate Authority, CA*)**
- **Registrierungsstelle (*Registration Authority, RA*)**
- **Zertifikatssperrliste (*Certificate Revocation List, CRL*)**
- **Validierungsdienst (*Validation Authority, VA*)**

Berufsförderungswerk Berlin-Brandenburg e.V.

RSA-Verfahren

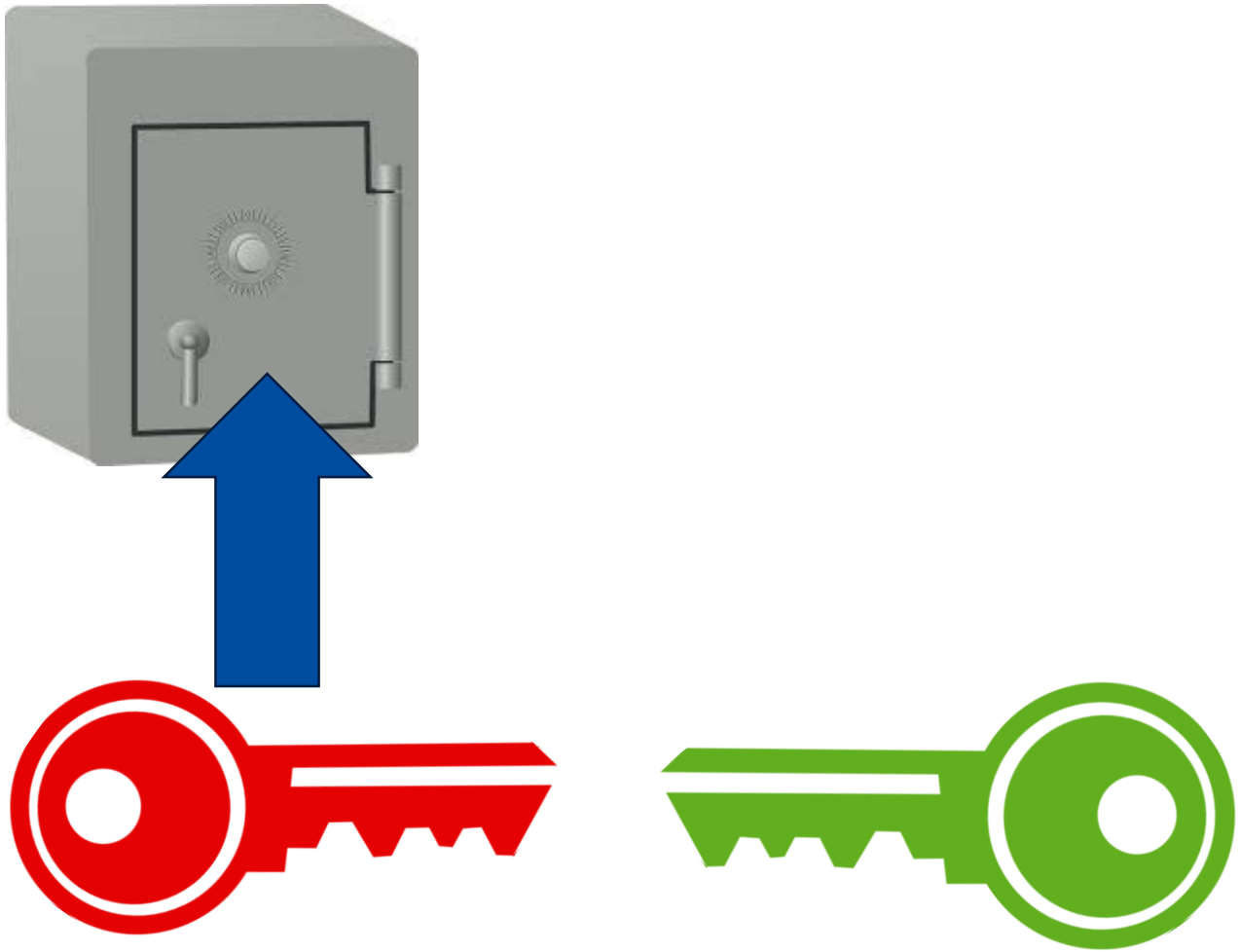
- öffentlicher Schlüssel aus Privatem berechnet
- 1977: Rivest, Shamir, Adleman



Assymetrische Kryptographie

PKI – Public Key Infrastruktur

Berufsförderungswerk Berlin-Brandenburg e.V.



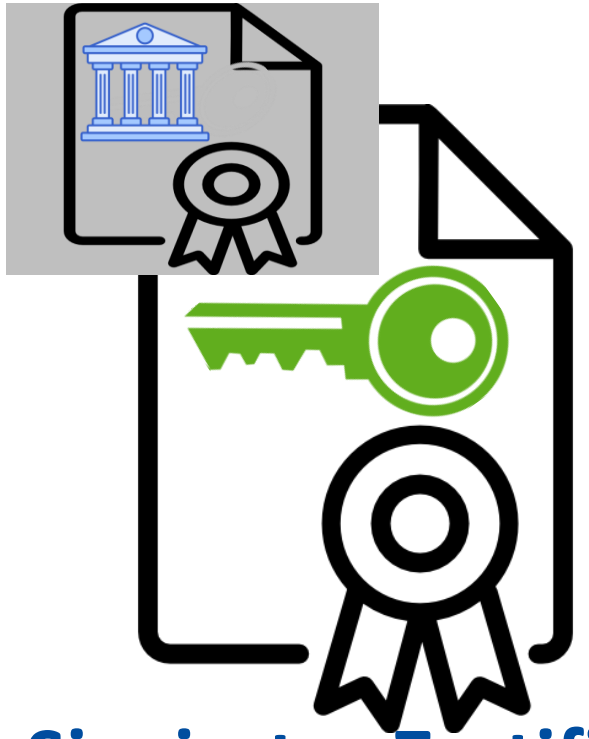
Assymetrische Kryptographie

PKI – Public Key Infrastruktur

Berufsförderungswerk Berlin-Brandenburg e.V.

Zertifizierungsstelle

unterzeichnen



Signiertes Zertifikat

Öffentlich verfügbar

einreichen

Assymetrische Kryptographie

X.509 - Standard für eine PKI (Public-Key-Infrastruktur)

Berufsförderungswerk Berlin-Brandenburg e.V.

Struktur eines X.509-v3-Zertifikats

- Zertifikat
- Zertifikat-Signaturalgorithmus
- Zertifikat-Signatur
- Attribute

Assymetrische Kryptographie

X.509 - Standard für eine PKI (Public-Key-Infrastruktur)

Berufsförderungswerk Berlin-Brandenburg e.V.

ZERTIFIKAT

- **Version** (z.Zt. 3)
- **Seriennummer** (fortlaufend)
- **Algorithmen-ID** (Hash, Crypt)
- **Aussteller** (CA)
- **Gültigkeit** (von bis)
- **Zertifikatinhaber** (Details)
  - **Zertifikatinhaber-Schlüsselinformationen**
    - **Public-Key-Algorithmus**
    - **Public Key des Zertifikatinhabers**
  - **Eindeutige ID des Ausstellers (optional)**
  - **Eindeutige ID des Inhabers (optional)**
  - **Erweiterungen**

Assymetrische Kryptographie

X.509 - Standard für eine PKI (Public-Key-Infrastruktur)

Berufsförderungswerk Berlin-Brandenburg e.V.

ZERTIFIKAT

- Gebräuchlicher Name (CN)
- Organisation (O)
- Organisationseinheit (OU)
- Land/Region (C)
- Bundesstaat (ST)
- Ort (L)

Assymetrische Kryptographie

TLS – Handshake Begriffe

Berufsförderungswerk Berlin-Brandenburg e.V.

- **TLS** = Transport Layer Security, Sicherheitsprotokoll
- **Cipher Suite** = Bündel von nutzbaren Verschlüsselungs- und Hash-Algorithmen
- **CA** = certificate authority, Zertifizierungsstelle
- **Sitzungsschlüssel** = symmetrischer Schlüssel für den Datenaustausch
- **RSA** = Verfahren zur Generierung von Schlüsselpaaren (privat + öffentlich)
- **Diffie-Hellmann(DH)** = Verfahren zum Schlüsselaustausch

Assymetrische Kryptographie

Kryptographie-Algorithmen

Berufsförderungswerk Berlin-Brandenburg e.V.

symmetrisch

- **DES** - 1975
  Data Encryption Standard
  - 3DES (Triple DES, Chipkarten)
- **AES** - 2000
  Advanced Encryption Standard

asymmetrisch

- **RSA** - 1977
  Rivest-Shamir-Adleman
- **DSA** - 1991
  Digital Signing Algorithm

Hash-Funktionen

- MD5 – 1991, Message-Digest Algorithm 5
- SHA – 1993, Secure Hash Algorithm

Assymetrische Kryptographie

TLS – Handshake Aufgaben

Berufsförderungswerk Berlin-Brandenburg e.V.

- TLS-Version (TLS 1.0, 1.2, 1.3 usw.) bestimmen
- Cipher Suites auswählen
- Authentifikation des Servers (digitale Signatur der CA)
- Generieren von Sitzungsschlüsseln für die symmetrische Verschlüsselung

Assymetrische Kryptographie

TLS – Handshake Aufgaben

Berufsförderungswerk Berlin-Brandenburg e.V.

- **TLS-Version festlegen**
- **Cipher Suites aushandeln**
- **Server authentifizieren**
  öffentlichen Schlüssel - Signatur der Zertifizierungsstelle
- **Sitzungsschlüssel generieren**
  für symmetrische Verschlüsselung nach Handshake

Assymetrische Kryptographie

TLS Handshake

Berufsförderungswerk Berlin-Brandenburg e.V.