Kryptocalypse Now

Das Jahr 2013...

- Massenhafte Überwachung durch die NSA
- einziger (?) Ausweg: Verschlüsselung
- Problem: Verschlüsselung ist kompliziert (bestes Beispiel: Greenwald)
- weiteres Problem: Verschlüsselung ist nicht immer sicher

Symmetrische und asymmetrische Kryptographie

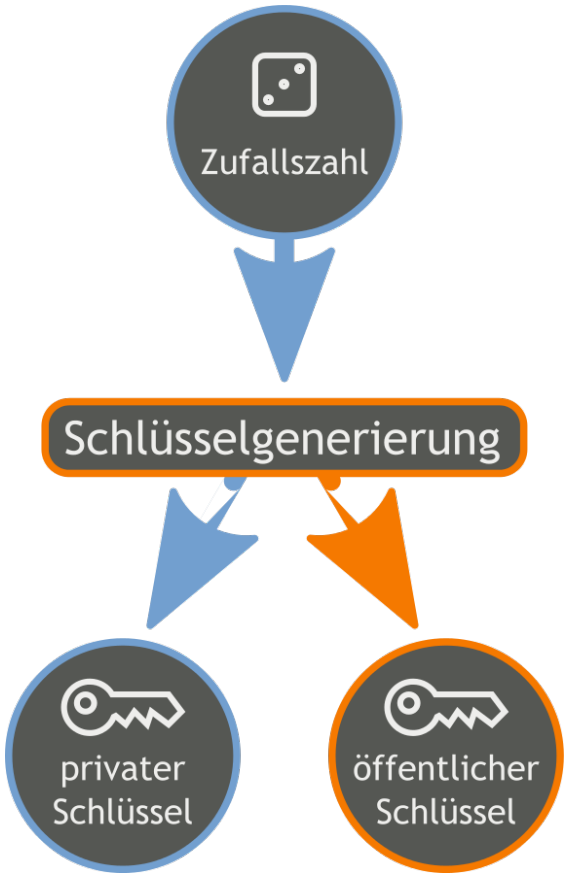
Symmetrische Kryptographie:

- gleicher Schlüssel zum Ver- und Entschlüsseln
- schnell
- Beispiele: AES, DES, Tripple-DES, Blowfish, RC2, RC4, RC5, RC6

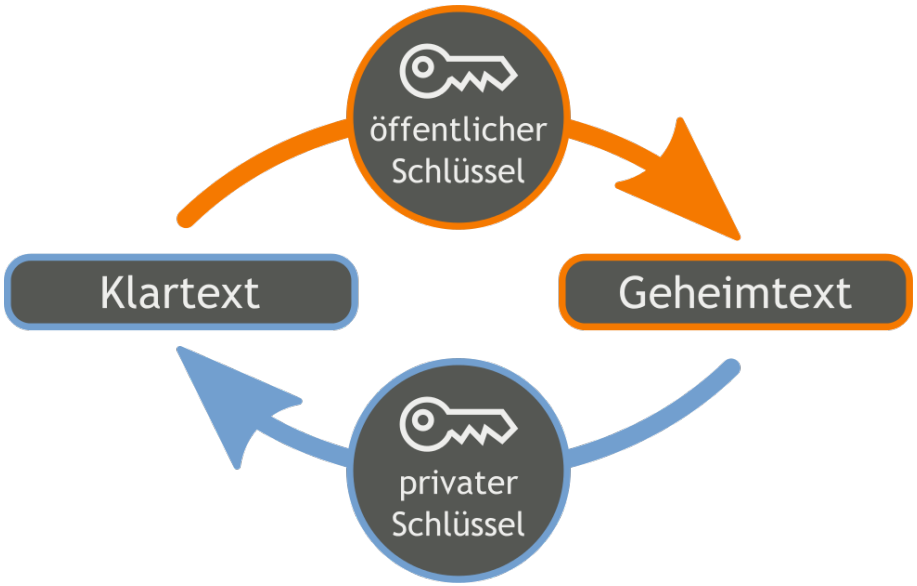
Asymmetrische Kryptographie:

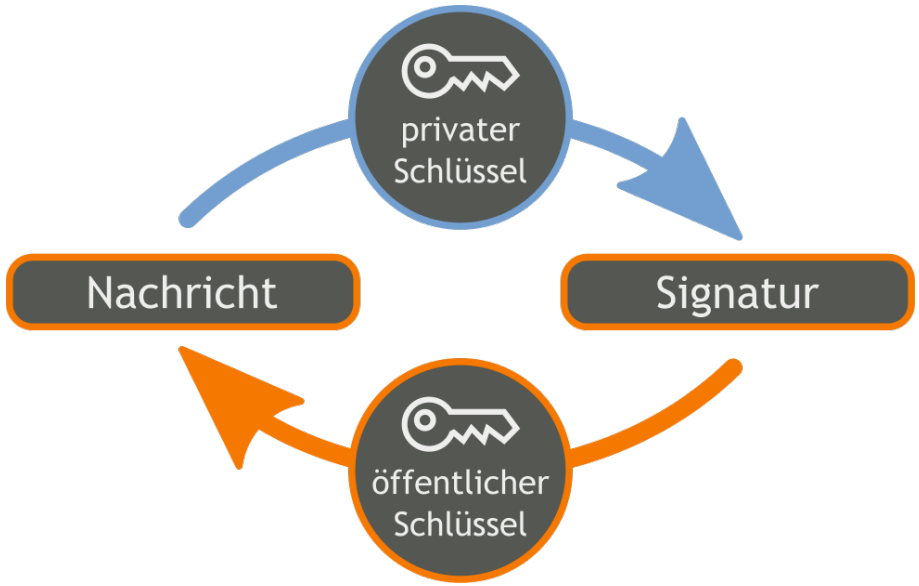
- beide Parteien müssen keine gemeinsamen Schlüssel kennen
- Benutzer erzeugt Schlüsselpaar: geheimer und öffentlicher Schlüssel
- langsam
- Beispiele: RSA, DSA, Diffie-Hellman

Asymmetrische Kryptographie



Asymmetrische Kryptographie





Beispiel: Diffie-Hellman

Funktionsweise:

1. Alice und Bob einigen sich auf eine Primzahl p und eine Primitivwurzel g.
2. Alice erzeugt eine Zufallszahl a, Bob erzeugt eine Zufallszahl b.
3. Alice berechnet $A = g^a \mod p$, Bob berechnet $B = g^b \mod p$. Alice und Bob übertragen A und B.
4. Alice berechnet $K = B^a \mod p$, Bob berechnet $K = A^b \mod p$.

Beide K gleich:

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

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

TLS

- TLS (**T**ransport **L**ayer **S**ecurity, früher SSL): Verschlüsselungsprotokoll zur sicheren Datenübertragung
- bekannte Anwendungsfälle: POP3, SMTP, NNTP, SIP, IMAP, XMPP, IRC, LDAP, FTP, OpenVPN
- Funktionsweise:
  1. Client baut Verbindung zum Server auf
  2. Server authentifiziert sich gegenüber Server mit einem Zertifikat
  3. Server schickt Client mit Zertifikat verschlüsseltes Geheimnis – oder Diffie-Hellman
  4. aus dem Geheimnis wird ein Schlüssel berechnet
  5. Schlüssel wird für symmetrische Kryptographie benötigt, Absicherung durch MACs

Probleme mit TLS

CBC:

- Frühjahr: erfolgreicher Angriff auf CBC in in TLS
- Unsicherheit seit 2008 bekannt, Angriffsszenario für unwahrscheinlich eingestuft
- Rat: auf RC4-SHA umstellen

RC4:

- RC4: Stromverschlüsselung
- Zufallsstrom von RC4 ist aber nicht immer Zufall
- darauf aufbauender Angriff

HTTPS heute

- RC4 und CBC angreifbar
- TLS 1.2 wird noch nicht wirklich unterstützt
- Server beharren teilweise auf RC4 (trauriges Beispiel: Allianz für Cybersicherheit)
- und: CA-System kaputt

E-Mail

Lavabit

- kurz nach den ersten Enthüllungen von Snowden schließt Lavabit
- Lavabit: E-Mail Provider für sichere Kommunikation, den Snowden nutzte
- Behörden wollten Betreiber Levinson zur Herausgabe der Master-SSL-Schlüssel zwingen
- damit wäre komplette Kummunikation – auch bisherige – entschlüsselbar gewesen
- Levabit stellte Dienst ein und erkläre Schlüssel für ungültig

Offene Fragen und Fazit

Offene Fragen:

- Wie viele solcher Gerichtsbeschlüsse wurden ausgehändigt?
- Wie viele Provider schweigen oder müssen schweigen?
- Verschlüssellung zwischen E-Mail Providern?

Fazit:

- Diffie-Hellman anstatt DSA für den Schlüsselaustausch $\Rightarrow$ Perfect Forward Security
- E-Mail ist unsicher
- DE-Mail ist keine Alternative (Entschlüsselung der Mails auf den Servern der Unternehmen)

Hintertürchen

Hintertürchen

- mögiche Hintertür im Zufallszahlengenerator Dual_EC_DRBG
- NSA soll am Standard nicht nur mitgearbeitet, sondern ihn alleine erstellt haben
- Zufallszahlengenerator kommt in kritischen Infrastrukturen weltweit zum Einsatz
- NIST und RSA rieten vom Gebrauch von Dual_EC_DRBG ab
- OpenSSL musste für FIPS-Zertifizierung Dual_EC_DRBG implementieren, die Implementation führte aber zum Absturz
- NSA und RSA
- NIST, SHA3 und Keccak

Hintertürchen II

- QFire:
  1. Turmoil: passive Variante, womit NSA alle elektronischen Spuren von Telekommunikationsnutzern weltweit sammle $\Rightarrow$ 15-jährige Vorratsdatenspeicherung, Deep-Packet-Inejection
  2. Turbine: Projekt, um Router und Webseiten zu kapern und den Betroffenen Schadcode zu unterjubeln
- GMail: GCHQ schnüffelt für die NSA
- Router zumindest von Huawei und Juniper, Server oder PCs und Mobiltelefone werden überwacht
- Firmware von Festplatten, Infrarotverbindungen von Servern, Rootkits im BIOS
- Auslesen von SMS, Kontakten und Aufnahmen der Kamera von iPhones
- Exploits auch für Sun Solaris

NSA und Tempest

- Bauteil Ragemaster wird im Ferrit, einer kleinen Ausbuchtung hinter dem Monitor-Stecker, versteckt
- Bauteil erzeugt ein Signal, das unter Verwendung eines externen Radarsystems aufgefangen werden kann
- aus den zurückgesendeten Strahlen lass sich der Bildschirminhalt rekonstruieren
- ähnliches System für Tastatureingaben
- Radardanlagen arbeiten zwischen 1-4 GHz mit Leistung von 1-2kW
- Hugo Chávez starb an Krebs


#NSA KILLED MY INTERNET
NOW I HAVE TO BUILD A GNU ONE

Happy 1984!