
Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

# Kapitel 8:
# Asymmetrische und hybride Kryptosysteme

# Inhalt

- Asymmetrische Kryptosysteme
  - RSA
  - Sicherheit von RSA
- Schlüssellängen und Schlüsselsicherheit
- Hybride Kryptosysteme
- Elektronische Signatur
- Quantencomputer und quantensichere Kryptographie

# Asymmetrische Verfahren

- Jeder Partner besitzt Schlüsselpaar aus
  - persönlichem, geheim zu haltenden Schlüssel (private key)
    (wird NIE übertragen)
  - und öffentlich bekannt zu gebenden Schlüssel (public key)
    (kann über unsichere und öffentliche Kanäle übertragen werden)
- Protokoll:
  1. Alice und Bob erzeugen sich Schlüsselpaare: $(k_e^A, k_d^A)$ $(k_e^B, k_d^B)$
  2. Öffentliche Schlüssel $(k_e^A, k_e^B)$ werden geeignet öffentlich gemacht
  3. Alice will m an Bob senden; dazu benutzt sie Bobs öffentlichen Schlüssel
     $$c = e(m, k_e^B)$$
  4. Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel:
     $$m = d(c, k_d^b) = d(e(m, k_e^b), k_d^b)$$
- Beispiele: RSA, DSA, ElGamal, ...

# Zielsetzung

- Effizienz / Performanz:
  - Schlüsselpaare sollen „einfach“ zu erzeugen sein.
  - Ver- und Entschlüsselung soll „schnell“ ablaufen.
- Veröffentlichung von $k_e$ darf keine Risiken mit sich bringen
- Privater Schlüssel $k_d$ darf nicht „einfach“ aus $k_e$ ableitbar sein
  - D.h. Funktion f mit $f(k_d) = k_e$ soll nicht umkehrbar sein („Einwegfunktion“)

- Einsatz zur Verschlüsselung:
  - Alice schickt Nachricht m mit Bobs Public Key verschlüsselt an Bob
  - Bob entschlüsselt den empfangenen Chiffretext mit seinem privaten Schlüssel

- Einsatz zur elektronischen Signatur:
  - Alice verschlüsselt ein Dokument mit ihrem privaten Schlüssel
  - Bob entschlüsselt das Dokument mit Alices öffentlichem Schlüssel

# RSA

- Benannt nach den Erfindern: Rivest, Shamir, Adleman (1978)
- Sicherheit basiert auf dem Faktorisierungsproblem:
  - Geg. zwei große Primzahlen p und q (z.B. 200 Dezimalstellen):
  - n=pq ist auch für große Zahlen einfach zu berechnen,
  - aber für gegebenes n ist dessen Primfaktorzerlegung sehr aufwendig
- Erfüllt alle Anforderungen an asymmetrisches Kryptosystem
- 1983 (nur) in USA patentiert (im Jahr 2000 ausgelaufen)
- Große Verbreitung, verwendet in:
  - TLS (Transport Layer Security)
  - PEM (Privacy Enhanced Mail)
  - PGP (Pretty Good Privacy)
  - GnuPG (GNU Privacy Guard)
  - SSH
  - ....

RSA

# Überblick über den Ablauf

- Erzeugung eines Schlüsselpaars
- Verschlüsselung
- Entschlüsselung

# Erzeugung eines Schlüsselpaars

- Randomisierte Wahl von zwei ähnlich großen, unterschiedlichen Primzahlen, p und q
- n = pq ist sog. RSA-Modul
- Euler'sche Phi-Funktion gibt an, wie viele positive ganze Zahlen zu n teilerfremd sind: $\Phi(n) = (p-1)(q-1)$
- Wähle teilerfremde Zahl e mit $1 < e < \Phi(n)$
  d.h. der größte gemeinsame Nenner von e und $\Phi(n)$ = 1
  - Für e wird häufig 65537 gewählt: Je kleiner e ist, desto effizienter ist die Verschlüsselung, aber bei sehr kleinen e sind Angriffe bekannt.
  - Der öffentliche Schlüssel besteht aus dem RSA-Modul n und dem Verschlüsselungsexponenten e.
- Bestimme Zahl d als multiplikativ Inverse von e bezüglich $\Phi(n)$

$$d = e^{-1} \bmod \Phi(n)$$

  - Berechnung z.B. über den erweiterten Euklidischen Algorithmus
  - n und d bilden den privaten Schlüssel; d muss geheim gehalten werden

# Ver- und Entschlüsselung

- Alice kommuniziert ihren öffentlichen Schlüssel (n,e) geeignet an Bob (Ziel hier: Authentizität von Alice, nicht Vertraulichkeit!)

- Bob möchte Nachricht M verschlüsselt an Alice übertragen:
  - Nachricht M wird als Integer-Zahl m aufgefasst, mit $0 < m < n$
    d.h. Nachricht m muss kleiner sein als das RSA-Modul n
  - Bob berechnet Ciphertext $c = m^e$ (mod n)
  - Bob schickt c an Alice

- Alice möchte Ciphertext c entschlüsseln
  - Alice berechnet hierzu $m = c^d$ (mod n)
  - Aus Integer-Zahl m kann Nachricht M rekonstruiert werden.

# Nomenklatur für kryptologische Verfahren

- Für Verschlüsselungsverfahren wird künftig die folgende Notation verwendet:

| | |
|---|---|
| Ap | Öffentlicher (public) Schlüssel von A |
| As | Geheimer (secret) Schlüssel von A |
| Ap{m} | Verschlüsselung der Nachricht m mit dem öffentlichen Schlüssel von A |
| As{m} oder A{m} | Von A erstellte digitale Signatur von m |
| S[m] | Verschlüsselung von m mit dem symmetrischen Schlüssel S |