Kryptographie und Komplexität

Einheit 7

Rückblick und Ausblick

1. Private- und Public-Key Verfahren
2. Komplexität von Angriffen
3. Sicherheitsprotokolle
4. Zukunftsträchtige Themen

Einfache Kryptosysteme

- **Buchstabenorientierte Systeme**
  - Substitution von Buchstaben durch andere Symbole des Alphabets
  - Mono- und polyalphabetische Variante
  - Anfällig für Brute-Force Attacken oder statistische Analysen
  - One-Time Pads: perfekte Geheimhaltung bei zu großem Aufwand
- **Blockbasierte Verschlüsselung**
  - Permutationen und affin-lineare Chiffren
  - Anfällig für known plaintext Attacken mit Matrix-Invertierung
- **Strombasierte Verschlüsselung**
  - Approximation von One-Time Pads durch lange Schlüsselströme macht statistische Analysen nahezu undurchführbar
  - Schlüsselerzeugung mit und ohne Verwendung des Klartextes
  - Zu brechen, wenn Erzeugungsverfahren für Schlüsselstrom bekannt

Keine Sicherheit gegen moderne Angriffsverfahren

Iterative Blockchiffren (DES /AES)

- **Erfolgreich in der Praxis**
  - Bei großen Schlüsseln sicher gegen alle bekannten Attacken
    - Große S-Boxen erzeugen starke Nichtlinearität
    - Lineare Transformationen erzeugen hohe Diffusion
    - Große Block- und Schlüsselgröße verhindert statistische Analysen
  - Effizient durch Verwendung von $\oplus$ und einfachen Operationen
    - Komponenten benötigen nur Tabellensuche oder ähnliches
    - Großer Datendurchsatz möglich
- **Es gibt keine theoretischen Sicherheitsgarantien**
  - Sicherheit basiert auf Erfahrung, nicht auf mathematischen Beweisen
- **Verfahren sind symmetrisch**
  - Schlüssel müssen zuvor über sichere Kanäle ausgetauscht werden
  - Aufbau einer spontanen sicheren Verbindung nicht möglich

Public Key Kryptographie mit RSA

- **Ver- und Entschlüsselung nutzt verschiedene Schlüssel**
  - Empfänger erzeugt beide Schlüssel, legt einen Schlüssel offen
  - Jeder Teilnehmer kann einen sicheren Kanal zum Empfänger aufbauen
- **RSA ist ältestes/bedeutendstes Public-Key Verfahren**
  - Ver-/Entschlüsselung ist Potenzieren mit e bzw. d modulo n
  - Rahmenbedingung $d = e^{-1} \bmod \varphi(n)$
  - n zusammengesetzt aus zwei großen Primzahlen p und q
  - n, e liegt offen, d, p und q bleiben geheim
- **Schlüsselerzeugung benötigt Primzahltests**
  - Schnellste Verfahren sind probabilistisch (Miller-Rabin)
- **Sicherheit basiert auf Faktorisierungsproblem**
  - Schlüsselangriff äquivalent zu Lösung des Faktorisierungsproblems
  - Faktorisierung ist subexponentiell $\mathcal{O}(e^{1.92 \cdot \|n\|^{1/3} \cdot (\log(\|n\|))^{2/3}})$
  - Sicherheit nur noch für Schlüsselgröße über 1024 Bit
  - Semantische Sicherheit nur mithilfe von Randomisierung

Faktorisierungsangriffe

- **Probedivision** $\mathcal{O}(2^{\|n\|})$
  - Standardverfahren, gut für kleine Faktoren
- **Methoden für spezielle Zahlen**
  - Pollard $p{-}1$: Für Faktor p hat $p{-}1$ nur kleine Primfaktoren
  - Fermat-Methode: Faktoren liegen nahe bei $\sqrt{n}$
- **Pollard ρ** $\mathcal{O}(2^{\|n\|/2})$
  - Systematische Suche nach Kollisionen $x \equiv x' \bmod p$ für unbekanntes p
- **Methoden auf Basis quadratischer Kongruenzen**
  - Dixon Random Squares, Quadratische Siebe $\mathcal{O}(2^{(1+o(1))\cdot\|n\|^{1/2}\cdot\,\log\|n\|^{1/2}})$
  - Zahlkörpersiebe $\mathcal{O}(2^{1.92\cdot\|n\|^{1/3}\cdot\,\log\|n\|^{2/3}})$
- **Elliptische-Kurven-Faktorisierung**
  - Probabilistischer Algorithmus auf Basis elliptischer Kurven

$\vdots \qquad\qquad \vdots$

ElGamal Verfahren

- **Effizientes Public-Key Kryptosystem**
  - Potenzierung von Elementen einer (beliebigen) zyklischen Gruppe
  - Sicherheit der Schlüssel basiert auf Problem des diskreten Logarithmus
  - Erhöhte semantische Sicherheit durch Randomisierung
  - Nachrichtenexpansion um Faktor 2
- **Effizienter als RSA**
  - Bei 'nichtarithmetischen' Gruppen mit schwerem DL Problem hat die beste Attacke eine Laufzeit von $\mathcal{O}(2^{\|n\|/2})$
  - Schlüssellängen von 160 Bit gelten als sicher
  - Implementierbar auf Smartcards mit geringer Prozessorleistung
  - Elliptische Kurven gelten derzeit die beste Grundlage

Berechnung diskreter Logarithmen

- **Aufzählungsverfahren**
  – Standardverfahren, gut für kleine Gruppenordnungen $\mathcal{O}(2^{\|n\|})$
- **Algorithmus Algorithmus von Shanks**
  – Zerlegung der Suche in Baby- und Giantsteps Zeit/Platz $\mathcal{O}(2^{\|n\|/2})$
- **Pollard ρ**
  – Systematische Suche nach Kollisionen $\mathcal{O}(2^{\|n\|/2})$
- **Pohlig-Hellman Verfahren**
  – Reduktion auf Primfaktoren von n $\mathcal{O}(\sum_{p|n} e_p \cdot \sqrt{p})$
- **Index-Calculus Methode**
  – Aufbau von Logarithmen einer Faktorbasis $\mathcal{O}(2^{(1+o(1))\cdot\|n\|^{1/2}\cdot \log\|n\|^{1/2}})$
  – Zahlkörpersieb als effizienteste Variante $\mathcal{O}(2^{1.92\cdot\|n\|^{1/3}\cdot \log\|n\|^{2/3}})$
  – Verallgemeinert sehr schlecht auf andere Gruppen

SICHERHEITSPROTOKOLLE

- **Kryptographische Verschlüsselungsverfahren**
  – Ziel ist Vertraulichkeit von Information
- **Kryptographische Hashfunktionen**
  – Offenbaren Fälschung/Manipulation übermittelter Nachricht
  – Ziel ist Datenintegrität
- **Passwörter und Identitätszertifikate**
  – Identifizieren Teilnehmer vor der Vergabe von Rechten
  – Ziel ist Sicherung der Authentizität von Kommunikationsteilnehmern
- **Digitale Signaturen**
  – Binden Nachricht an ihren Absender
  – Ziel ist Verbindlichkeit digitaler Dokumente
- **Mehrparteien-Berechnung**
  – Ermöglichen Verteilung von Geheimnissen auf mehrere Personen
  – Ziel ist Sicherheit gegen Korrumpierbarkeit einzelner Teilnehmer

Weitere Fragestellungen der Kryptographie

- **Schlüsselverwaltung**
  - Kryptographische / organisatorische Maßnahmen für sichere Schlüssel
  - Erzeugung, Verteilung und sichere Speicherung von Schlüssel
  - Rückruf kompromittierter Schlüssel
  - Public-Key Infrastrukturen und Zertifizierungsinstanzen
- **Schlüsseletablierungsprotokolle**
  - Protokolle für Erzeugung gemeinsam nutzbarer geheimer Schlüssel
  - Schlüsseltransportprotokolle: Sichere Verteilung eines Schlüssels
  - Schlüsselvereinbarungsprotokolle: Gemeinsame Erzeugung
  - Protokolle müssen Authentifizierung mit einbauen
- **Anonymität von Systemteilnehmern**
  - Senderanonymität: Protokolle für anonyme Hinweise
  - Empfängeranonymität: Protokolle für anonyme Anfragen (Chiffre)
  - Kommunikationsanonymität: Kommunikation nach außen unsichtbar

Zukunftsträchtige Themen

- **Hyperelliptische Kurven**
  - Verallgemeinerung elliptischer Kurven
  - Höhere Sicherheit durch größere Auswahl von Parametern
- **Quantenkryptographie**
  - Berechnungen auf der Basis von Quantenzuständen und -verschränkung
  - Mehr Effizienz, da Qubits beliebig viele Zustände annehmen können
    Anwendung: Effiziente Faktorisierung (Algorithmus von Shor)
  - Mehr Sicherheit, da Beobachtung von Daten nie unbemerkt bleibt
    z.B. Quantum-Key Distributuion, Quantum Direct Communication
- **Viele Anwendungen**
  - Internetsicherheit als wichtigstes Problem
    Maximale Freiheit bei größtmöglicher Sicherheit
    Leichte Anwendung bei maximalem Schutz naiver Benutzer