Formelsammlung Krypto

David Jäggli

6. Mai 2024

Inhaltsverzeichnis

1 Allg

2 Terminologie

Kryptographie	Entwerfen von Krypto-Algorithmen
Kryptoanalyse	Brechen von Krypto-Algorithmen
Perfekte Sicherheit	Unendlich viele Ressourcen sind equivalent zu raten
Unkeyed Kryptographie	Hashfunktionen
Symmetrische Krypt.	Beide den gleichen Schlüssel - $\mathcal{O}(n)$
Asymmetrische Krypt.	Öffentlicher und privater Schlüssel - $\mathcal{O}(n)$

3 Symmetrische Kryptographie

4 Asymmetrische Kryptographie

5 Blinde Signaturen

Generelle Beschreibung: Anna weis nicht WAS sie unterschreibt, wenn sie das Dokument später sieht, weis sie aber DASS sie es unterschrieben hat.
Nutzen:

- Unverfällschbarkeit
- Anonymität
- Unlinkbarkeit

Ablauf:

1. Kunde zieht geld ab
2. Bank signiert den Betrag
3. Kunde bezahlt im Shop
4. Shop schickt die Unterschrift an die Bank
5. Bank prüft Unterschrift
6. Bank validiert Unterschrift und zieht Geld ab

Beispiel: Siehe s.100 Folien 09

6 Einführung in die Public-Key Infrastruktur (PKI)

6.1 Verschlüsseln und Signieren (repetition)

6.1.1 Verschlüsseln

6.1.2 Signieren

Ablauf signieren:

1. Dokument von Alice ist Ausgangswert
2. Hash berechnen → Hashwert
3. chiffrieren (mit private key und Hash) → Signatur
4. Dokument & Signatur + Zertifikat → signiertes Dokument

Warum Zertifikat? → um sicherzustellen, dass der öffentliche Schlüssel auch wirklich von Alice ist.

Ablauf Signatur prüfen:

1. Dokument von Alice ist Ausgangswert
2. Signatur mit öffentlichem Schlüssel entschlüsseln → Hashwert
3. Hashwert von Dokument berechnen
4. Hashes vergleichen
5. Zertifikat Überprüfen

6.2 Zertifikate

6.2.1 Herstellung eines Zertifikats

1. Zertifikatsinhalt
   - Version
   - Serial Number
   - Subject
   - Public Key
2. Inhalt hashen
3. Hash signieren
4. Signitierter Hash + Zertifikatsinhalt → Zertifikat

6.2.2 Zertifikatsklassen

- **Klasse 1:** wenig Sicherheit, keine Identitätsprüfung
- **Klasse 2:** mittlere Sicherheit, schwache Identitätsprüfung
- **Klasse 3:** hohe Sicherheit, strenge Identitätsprüfung
- **Qualified Certificate:** höchste Stufe, werden nur für natürliche Personen ausgestell