CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand GmbH chr.schumacher@gmx.tm

Themen und Inhalte:

01 Geschichte der Kryptographie

02 Grundbegriffe der Kryptographie

Themen und Inhalte:

03 Symmetrisch Verschlüsselungsverfahren

04 Asymmetrisch Verschlüsselungsverfahren

Themen und Inhalte:

05 Hashfunktionen

06 Angriffe auf Kryptosysteme

Themen und Inhalte:

07 Kryptographie im Alltag

08 Zukunftsthemen:
Post-Quanten-Kryptographie

Themen und Inhalte:

09 Steganographie

01 Geschichte der Kryptographie

Geschichte der Kryptographie

Kryptographie existiert seit der Antike:

- Skytale (Sparta, ca. 500 v. Chr.):
  Holzstab zur Transpositionsverschlüsselung
- Caesar-Verschlüsselung (Römisches Reich, ca. 50 v. Chr.): Buchstabenverschiebung
- Ziele dabei immer:
  Militärische Kommunikation schützen Kryptographie

Geschichte der Kryptographie

Mittelalter & Renaissance:

- Vigenère-Chiffre (16. Jh.):
  Polyalphabetische Verschlüsselung
- Kryptographie als Geheimsprache bei Diplomatie & Spionage
- Häufig auch Codierungen, z.B. Zahlen für Wörter

Geschichte der Kryptographie

Moderne – Mechanische Verschlüsselung:

- Enigma-Maschine (Deutschland, 1920er–1945):
  Elektromechanische Verschlüsselung im 2. Weltkrieg
- Wettrüsten: Codeknacker vs. Kryptographen
  (Bletchley Park, Alan Turing)
- Meilenstein:
  Erste systematische Kryptoanalyse
- Grundstein für spätere Computerentwicklung

Geschichte der Kryptographie

Computerzeitalter und digitale Kryptographie:

- Entwicklung elektronischer Verschlüsselungsverfahren (ab 1970er)
- DES (Data Encryption Standard, 1977)
- RSA (erstes asymmetrisches Verfahren, 1977)
- AES (Advanced Encryption Standard, ab 2001)
- Kryptographie als Basis der IT-Sicherheit (z.B. Internet, E-Mail)

Geschichte der Kryptographie

Ausblick – Kryptographie heute & morgen:

- Allgegenwärtig:
  Smartphones, Cloud, Banking
- Stetiger Wettlauf:
  Stärkere Algorithmen vs. leistungsfähigere Angreifer
- Zukunft:
  Quantenkryptographie, Post-Quantum-Kryptographie
- Zentraler Bstandteil unserer heutigen Gesellschaft

Grundlegendes

Wie aus der Historie hervorgeht, dreht sich bei der Kryptographie schlussendlich alles um die CIA-Triade:

- Vertraulichkeit:
  Schutz vor unbefugtem Zugriff

- Integrität:
  Schutz vor unbemerkter Veränderung

- Authentizität:
  Nachweis der Identität von Kommunikationspartnern

02 Grundbegriffe der Kryptographie

Grundbegriffe der Kryptographie

Symmetrische und asymmetrische Kryptosysteme:

- Symmetrisch:
  Gleicher Schlüssel für Ver- und Entschlüsselung
  - Schnell, aber Schlüsselverteilung ist schwierig
  - Beispiele: AES, DES
- Asymmetrisch:
  Verschiedene Schlüssel (öffentlich & privat)
  - Ermöglicht Schlüsselaustausch und digitale Signaturen
  - Beispiele: RSA, ECC

Grundbegriffe der Kryptographie

Wichtige Begriffe:

- Klartext:
  Ursprüngliche, lesbare Nachricht
- Chiffretext:
  Verschlüsselte Nachricht
- Schlüssel:
  Geheime Information zur Ver- und Entschlüsselung
- Algorithmus:
  Verfahren/Regelwerk der Verschlüsselung
  Kryptographie Kryptographie

Grundbegriffe der Kryptographie

Hashfunktionen und digitale Signaturen:

- Hashfunktion:
  „Fingerabdruck“ einer Nachricht bzw. von Daten
  Merkmal: feste Länge
  Beispiele: SHA-256, SHA-3

- Digitale Signatur:
  Elektronische Unterschrift zur Prüfung von Integrität und Authentizität.
  Einsatz z.B. bei Software-Updates und Zertifikaten

03

Symmetrische Verschlüsselungs-verfahren

Symmetrische Verschlüsselungsverfahren

Prinzip und Beispiel:

- Grundprinzip:
  Ein Schlüssel für Ver- und Entschlüsselung

- Anwendung für schnelle, sichere Datenübertragung

- Beispiel:
  Dateien, Festplatten, Netzwerkverbindungen

Symmetrische Verschlüsselungsverfahren

Funktionsweise symmetrischer Verfahren:

- Sender und Empfänger teilen einen geheimen Schlüssel
- Klartext => Verschlüsselungsalgorithmus => Chiffretext
- Chiffretext => Entschlüsselungsalgorithmus => Klartext
- Schnelle und effiziente Verarbeitung

Symmetrische Verschlüsselungsverfahren

Bekannte symmetrische Algorithmen:

- DES (Data Encryption Standard):
  56 Bit, historisch wichtig, heute unsicher
- AES (Advanced Encryption Standard):
  128/192/256 Bit, aktueller Standard
- Blowfish, Twofish, RC4, ChaCha20:
  Weitere verbreitete Verfahren
- Unterschiede liegen hauptsächlich in der Geschwindigkeit, Sicherheit und dem Einsatzgebiet

Symmetrische Verschlüsselungsverfahren

Vor- und Nachteile symmetrischer Verfahren:

Vorteile:

Sehr schnell, geringe Rechenleistung erforderlich.

Ideal für große Datenmengen.

Nachteile:

Schlüsselverteilung ist ein zentrales Problem.

Keine direkte Möglichkeit für digitale Signaturen

Symmetrische Verschlüsselungsverfahren

Anwendungen im Alltag:

- Festplatten- und Dateiverschlüsselung
  (z.B. BitLocker, VeraCrypt)
- VPNs und sichere Netzwerkkommunikation
- Verschlüsselte Messenger und Cloud-Speicher
- Basis für viele hybride Kryptosysteme
  (Kombination mit asymmetrischer Verschlüsselung)

04

Asymmetrische Verschlüsselungs-verfahren

Asymmetrische Verschlüsselungsverfahren

Merkmal und Prinzip:

- Bei der asymmetrischen Verschlüsselung existieren immer zwei Schlüssel:
  öffentlich und privat
- Prinzip:
  Was mit dem Einen verschlüsselt wird, kann nur mit dem Anderen (Schlüssel) entschlüsselt werden.
- Zentrale Technik für sichere Kommunikation im Internet

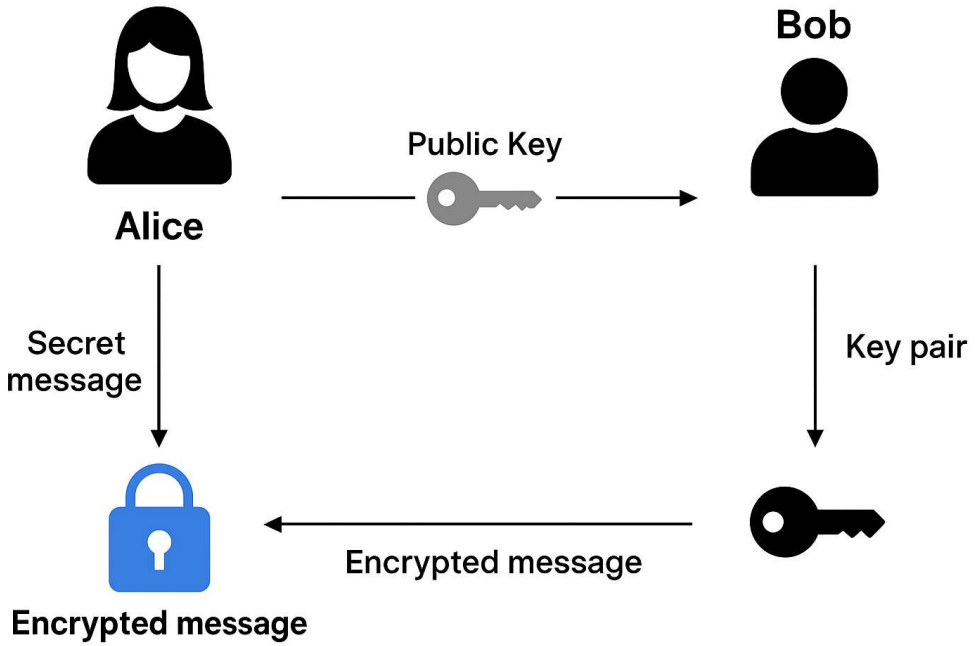
Asymmetrische Verschlüsselungsverfahren

Funktionsweise asymmetrischer Verfahren:

- Schlüsselpaar:
  - Öffentlicher Schlüssel: Wird verteilt
  - Privater Schlüssel: Bleibt geheim
- Beispiel:
  Person A verschlüsselt Nachricht mit dem öffentlichen Schlüssel von B.
  Nur B kann die Nachricht mit seinem privaten Schlüssel entschlüsseln.
- Anwendung auch für digitale Signaturen

Asymmetrische Verschlüsselungsverfahren

Funktionsweise asymmetrischer Verfahren:



Asymmetrische Verschlüsselungsverfahren

Bekannte asymmetrische Algorithmen:

- RSA:
  Seit 1977, basiert auf Faktorisierung großer Zahlen.
  Weit verbreitet für Verschlüsselung und Signaturen.
- Diffie-Hellman:
  Ermöglicht sicheren Schlüsselaustausch.
- ECC (Elliptic Curve Cryptography):
  Hohe Sicherheit mit kurzen Schlüsseln.
  Besonders geeignet für mobile Geräte

Asymmetrische Verschlüsselungsverfahren

Anwendungsbeispiele im Alltag:

- TLS/SSL:
  z.B. Verschlüsselte Webseiten (https)
- E-Mail-Verschlüsselung:
  OpenPGP, S/MIME
- Digitale Signaturen:
  Nachweis von Authentizität und Integrität
- Kryptowährungen:
  Wallets und Transaktionen

Asymmetrische Verschlüsselungsverfahren

Vor- und Nachteile asymmetrischer Verfahren:

- Vorteile:
  - Sichere Schlüsselverteilung
  - Ermöglicht digitale Signaturen
  - Kein vorheriger Schlüsselaustausch nötig
- Nachteile:
  - Langsamer als symmetrische Verfahren
  - Rechenintensiv

05
Hashfunktionen

Hashfunktionen

Eigenschaften kryptographischer Hashfunktionen:

- Feste Ausgabelänge:
  Unabhängig von der Eingabemenge
- Schnelle Berechnung
- Einwegfunktion:
  Aus dem Hashwert kann der Ursprung nicht rekonstruiert werden
- Bei der kleinsten Änderung resultiert daraus ein komplett anderer Hashwert.

Hashfunktionen

Bekannte Hash-Algorithmen:

- MD5:
  Schnell, aber unsicher (Kollisionen möglich)
- SHA-1:
  Veraltet, nicht mehr empfohlen
- SHA-2 (SHA-256, SHA-512):
  Weit verbreitet und sicher
- SHA-3:
  Neuer Standard mit alternativer Architektur

Hashfunktionen

Anwendungsbeispiele:

- Integritätsprüfung von Dateien und Downloads
- Speicherung und Vergleich von Passwörtern
- Digitale Signaturen
- Blockchains und digitale Währungen
- Datenbanken und Hash-Tabellen

06
Angriffe auf Kryptosysteme

Angriffe auf Kryptosysteme

- Ziel:
  Schwächen von Verschlüsselung erkennen und ausnutzen.
- Unterschiedliche Methoden und Werkzeuge
- Schutzmaßnahmen

Angriffe auf Kryptosysteme

Brute-Force-Angriffe:
(Wörterbuchattacken und Rainbowtables)

- Vorgehensweise:
  Systematisches Durchprobieren aller möglichen Schlüssel

- Erfolgreich, wenn der Schlüsselraum klein ist

- Je länger und komplexer der Schlüssel, desto sicherer das System

Angriffe auf Kryptosysteme

Brute-Force-Angriffe:

- Beispielprogramme:

Programm	Verwendung
JTR bzw. John the Ripper	Passwörter
Hashcat	Hashwerte
Hydra	Login-Formulare und Netzwerkdienste

Angriffe auf Kryptosysteme

Kryptoanalyse:

- Vorgehensweise:
  Mathematische oder statistische Analyse, um Schwächen im Algorithmus oder der Implementierung auszunutzen
- Häufiges Ziel:
  Alte oder fehlerhaft implementierte Verfahren
- Erfolgreich, z. B. bei schwachen Algorithmen wie MD5, SHA-1, DES

Angriffe auf Kryptosysteme

Kryptoanalyse:

- Beispielprogramme:
  - Cryptool
  - HashClash (Kollisionsangriffe auf Hashfunktionen)

Angriffe auf Kryptosysteme

Man-in-the-Middle (MITM):

- Vorgehensweise:
  Angreifer schaltet sich zwischen Sender und Empfänger
- Kommunikation wird mitgelesen, manipuliert oder umgeleitet
- Besonders gefährlich bei ungesicherter Verbindung (z. B. ohne TLS/SSL)

Angriffe auf Kryptosysteme

Man-in-the-Middle (MITM):

- Beispielprogramme:
  - Bettercap
  - Ettercap
  - mitmproxy

Angriffe auf Kryptosysteme

Seitenkanalangriffe:

- Vorgehensweise:
  Ausnutzung physikalischer Merkmale (z. B. Stromverbrauch, Laufzeit, elektromagnetische Strahlung)
- Kein Angriff auf die Mathematik, sondern auf die konkrete Implementierung
- Praktisch vor allem bei Smartcards, IoT-Geräten oder Hardware-Tokens

Angriffe auf Kryptosysteme

Seitenkanalangriffe:

- Beispielprogramme / Tools:
  - ChipWhisperer (Hardware-Toolkit)
  - Riscure Inspector (professionelle Analyseplattform)

Angriffe auf Kryptosysteme

Schutzmaßnahmen gegen Angriffe auf Kryptosysteme

- Regelmäßige Überprüfung und Aktualisierung der eingesetzten Algorithmen
- Einsatz starker Schlüssel und sicherer Protokolle
- Software und Hardware gegen Seitenkanäle absichern
- Wachsamkeit gegenüber neuen Angriffsmethoden und Tools

07
Kryptographie im Alltag

Kryptographie im Alltag

Allgemeines:

- Kryptographie ist die Grundlage für den Datenschutz in der IT-Sicherheit
- Steigende Bedeutung durch immer weiter gehende Digitalisierung.
  Dabei muss die CIA-Triade eingehalten werden.
- Kontinuierliche Weiterentwicklung gegen neue Bedrohungen
- Bewusstes Verhalten wichtig für eigene Sicherheit (**Awareness!**)

Kryptographie im Alltag

Sicheres Surfen – TLS/SSL:

- Verschlüsselte Verbindungen mit HTTPS
- Schutz vor Abhören und Manipulation beim Surfen
- Einsatz: Online-Banking, E-Commerce, E-Mail
- Erkennbar am „Schloss“-Symbol im Browser

Kryptographie im Alltag

Sichere Kommunikation – Messenger & E-Mail:

- Ende-zu-Ende-Verschlüsselung
  (z. B. Signal, WhatsApp, Threema)
- Verschlüsselte E-Mails, z.B. mit OpenPGP
- Schützt Privatsphäre bzw. sensible Daten
- Durch die Implementierung sicherer Kommunikation ist keine Einsichtnahme durch 3rd Parties möglich

Kryptographie im Alltag

Datensicherheit – Verschlüsselte Festplatten & Geräte:

- Verschlüsselung von Computern und Smartphones,
  z.B. durch:
  - BitLocker (Windows)
  - FileVault (macOS)
  - LUKS (Linux)
  - Smartphone-Verschlüsselung
- Schutz vor unbefugtem Zugriff bei Verlust oder Diebstahl

Kryptographie im Alltag

Zahlungsverkehr & Digitale Identitäten:

- Kryptographie im Online-Banking
  (TAN-Verfahren, Chipkarten, Mobile Payment)
- Digitale Identitäten und elektronische Signaturen,
  z.B. elektronische Ausweise oder digitale Signaturen für Dokumente
- Kryptowährungen (z. B. Bitcoin, Ethereum)

08

Zukunftsthemen: Postquanten-kryptographie

Postquanten-kryptographie

Generelles:

- Quantencomputer als neue Herausforderung für Kryptographie.
- Postquantenkryptographie (PQK) entwickelt Verfahren, die resistent gegen Angriffe durch Quantencomputer sind.
- Zukünftige Sicherung der Kommunikation notwendig.

Postquanten-kryptographie

Warum brauchen wir Postquantenkryptographie?

- Quantencomputer bedrohen klassische Verschlüsselungsverfahren
- Shors Algorithmus:
  Quantencomputer können RSA, ECC effizient brechen
- Gefahr für heutige IT-Systeme und Datensicherheit
- Rechtzeitige Entwicklung neuer Algorithmen erforderlich

Postquanten-kryptographie

Ausblick:

- Rechtzeitige Vorbereitung auf Postquantenära notwendig
- Hohe Relevanz für langfristige Datensicherheit („Store now, decrypt later“)
- Laufende Forschung notwendig zur Weiterentwicklung robuster Verfahren
- Unternehmen und Institutionen müssen sich frühzeitig mit PQK befassen

09 Steganographie

Steganographie

Was ist Steganographie?

- Definition:
  Geheime Informationen unauffällig in Medien verstecken
- Unterschied zur Kryptographie:
  Informationen nicht verschlüsseln, sondern verbergen
- Ziel:
  Unbemerkte Kommunikation, keine Aufmerksamkeit erregen

Steganographie

Geschichte der Steganographie:

- Antike Beispiele:
  Tätowierungen auf Sklavenköpfen, versteckte Botschaften in Wachstafeln
- Mittelalter & Renaissance:
  Geheime Botschaften in Büchern, Gemälden und Noten
- Moderne Nutzung:
  Digitale Medien wie Bilder, Audio- und Videodateien

Steganographie

Techniken und Vorgehensweise:

- Least Significant Bit (LSB)-Verfahren:
  Verstecken von Informationen in den Pixeln eines Bildes
- Audio-Steganographie:
  z.B. Frequenzänderungen in Audiodateien
- Text-Steganographie:
  Unsichtbare Zeichen, Schriftartänderungen
- Alle Techniken verfolgen immer ein Ziel:
  Informationen schwer nachweisbar integrieren

Steganographie

Anwendungsbeispiele:

- Schutz vertraulicher Informationen
  z. B. digitale Wasserzeichen
- Geheime Kommunikation in sensiblen Bereichen
  (Nachrichtendienste, Journalismus)
- Digital Rights Management (DRM), Copyright-Markierungen in digitalen Medien
- Verdeckte Datenübertragung in Cybersecurity
  z. B. Malware-Kommunikation

Steganographie

Programme und Tools für Steganographie

- Steghide:
  Verstecken von Dateien in Bildern und Audio
- OpenStego:
  Wasserzeichen und versteckte Daten in Bildern
- SilentEye:
  Einfache Oberfläche, vielseitig einsetzbar
- OutGuess
  Werkzeug zum Verstecken in JPEG-Bildern

Steganographie

Herausforderungen und Erkennung (Steganalyse)

- Schwierigkeit:
  Informationen unauffällig verstecken
- Steganalyse:
  Methoden zum Erkennen versteckter Informationen
- Techniken:
  Statistische Analysen, maschinelles Lernen
- Wettrüsten zwischen Steganographie und Steganalyse

DANKE!

Gibt es noch Fragen?

CloudCommand