

IT-Sicherheit

Marian Margraf

18. November 2014

Inhaltsverzeichnis

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- 1 Einleitung
- 2 Grundlegende Begriffe
- 3 Kryptologie
- 4 Authentisierung
- 5 Netzwerk- und Internetsicherheit
- 6 Sicherheit für Ubiquitous Computing
- 7 Bewertungskriterien
- 8 IT-Sicherheitsmanagement
- 9 IT-Forensik
- 10 Sichere Softwareentwicklung

Aktuelle Angriffe

Einleitung

Grundlegende Begriffe

Kryptologie

Authentisierung

Netzwerk- und Internetsicherheit

Sicherheit für Ubiquitous Computing

Bewertungskriterien

IT-Sicherheitsmanagement

IT-Forensik

Sichere Softwareentwicklung

Ziel der IT-Sicherheit ist die Verfügbarkeit der Daten, Dienste und Anwendungen zu gewährleisten, sowie die Integrität und Vertraulichkeiten der Daten sicher zu stellen.

Beinahe täglich werden sicherheitskritische Schwachstelle von und Angriffe auf informationsverarbeitende Systeme veröffentlicht (vgl. www.heise.de/security)

- Aktuell: Malware auf Kassensystemen von US-Handelsketten greifen Kreditkarteninformationen ab
- Mitte 2014: Programmierfehler in OpenSSL (Heartbleed) kann zur Ausspähung von Passwörter genutzt werden
- Anfang 2014: 18 Millionen E-Mailkonten unter Nutzung von Botnetzen gestohlen

Motivation für Angriffe

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Klassische Angreifer:

- White-Hacker: Aufdecken von Sicherheitslücken
- Geheimdienste: Spionage, Sabotage und Überwachung
- Unternehmen: Wirtschaftsspionage (Zusammenarbeit mit Geheimdiensten)

Neueste Entwicklungen:

- Cracker: Etablierung einer stark professionalisierten Schattenwirtschaft
- Whistleblower: Veröffentlichung geheimer Informationen

Schattenwirtschaft

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Mit erfolgreichen Angriffen lässt sich viel Geld verdienen:

- Fälschung von PayTV-Karten
- Abgreifen von Kreditkarteninformationen (Warenkreditbetrug)
- Phishing-Angriffe im Bereich Online-Banking

Darüber hinaus gibt es einen etablierten Schwarzmarkt für Verwundbarkeiten von IT-Systemen (Exploits).

Angriffsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir erleben unterschiedlichste Arten von Angriffen:

- Ungezielte Angriffe z.B. über Massenmails, mit denen Viren, Würmer und Trojaner versandt oder Phishing-Angriffe durchgeführt werden.
- Gezielte Angriffe, z.B. zur Sabotage und Spionage, die auf bestimmte Institutionen gerichtet sind (DDoS-Angriffe auf staatliche Infrastrukturen).
- Skalpelartige Angriffe, z.B. gezielte Sabotage auf bestimmte IT-Systeme (Beispiel Stuxnet) oder auf Zertifikatediensteanbieter (Beispiel Fälschung von ssl-Zertifikaten der niederländischen Firma DigiNotar im Juli 2011, hiervon war auch das Serverzertifikat von google.com betroffen).

Schwachstellen in Software

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Einer der Gründe für erfolgreiche Angriffe ist die Fehleranfälligkeit von Software

- Heutige Betriebssysteme haben ca. 86.000.000 Zeilen Source-Code
- Untersuchungen zeigen: Fehlerquote liegt bei ca. 0.25 %
- Also ca. 200.000 potentiell ausnutzbare Fehler
- Hinzu kommt die Anwendungssoftware

Grundlegende Begriffe

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Definition und Präzisierung der Begriffe

- Information und Daten
- IT-System und IT-Verbund
- Sicherheit (Betriebs- und Informationssicherheit)
- Bedrohung, Gefährdung, Angriff, Risiko
- Schutzziele (z.B. Vertraulichkeit, Integrität, Verfügbarkeit)
- Datenschutz

Motivation

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Informationen sind schützenswerte Güter, z.B. hinsichtlich

- Verlust des informationellen Selbstbestimmungsrechts (Datenschutz): Informationen über Krankheiten, Einkommen
- finanzieller Verluste: Geschäftsgeheimnissen, Verträgen, Zugangsdaten zum Online-Banking
- persönlicher Unversehrtheit: Fehlfunktionen medizinischer Überwachungsgeräte, Verkehrsleitsysteme

Die Betrachtung/Beurteilung hinsichtlich IT-Sicherheit erfolgt meist ausgehend von den schützenswerten Informationen.

Information

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Definition des Begriffs Information nach deutschem Duden:

- 1 das Informieren; Unterrichtung über eine bestimmte Sache; Kurzwort: Info
- 2a [auf Anfrage erteilte] über alles Wissenswerte in Kenntnis setzende, offizielle, detaillierte Mitteilung über jemanden, etwas
- 2b Äußerung oder Hinweis, mit dem jemand von einer [wichtigen, politischen] Sache in Kenntnis gesetzt wird

Eine Information hat für den Empfänger einen Neuigkeitsgehalt.

Ihre Form kann unterschiedlich sein: gesprochen, geschrieben, gedacht, elektronisch.

Daten sind Repräsentationen von Informationen, z.B.

- als Bytefolge gespeichert auf einer Festplatte
- als Netzwerkpaket bei der Übertragung über das Internet

Der Begriff Datensicherheit ist also spezieller als Informationssicherheit

- Datensicherheit: Beschäftigt sich mit der Sicherheit von Daten
- Informationssicherheit: Beschäftigt sich mit der Sicherheit von Informationen (und damit auch von Daten, die die Informationen repräsentieren)

IT-System

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein IT-System ist ein dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Daten.

Beispiele:

- Computer, Tablettts, Smartphones
- Router, Switches, Netze
- Drucker, Scanner

IT-Verbund

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

Ein IT-Verbund kann verschiedene Ausprägungen haben, z.B.:

- eine gesamte Institution (z.B. Firma, Behörde)
- einzelne Bereiche einer Institution, die in organisatorische Strukturen (z.B. Abteilungen) gegliedert sind
- einzelne Bereiche einer Institution, die gemeinsame Geschäftsprozesse bzw. Anwendungen haben

Sicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Sicherheit ist der Schutz vor negativen Konsequenzen aus vorsätzlichen und berechtigten Handlungen.

In Bezug auf IT-Systeme unterscheiden wir zwei Arten von Sicherheit:

- Schutz vor negativen Konsequenzen aus berechtigten Handlungen: Betriebssicherheit/Funktionssicherheit (engl. Safety)
 - Ist-Funktionalität stimmt mit der spezifizierten Soll-Funktionalität überein (alles läuft wie geplant)
- Schutz vor negativen Konsequenzen aus vorsätzlichen Handlungen: Informationssicherheit (engl. Security)
 - Resistenz gegenüber Angriffen (keiner unautorisierte Informationsveränderung oder -gewinnung möglich)

Prävention

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Kernbestandteil von Betrachtungen über Sicherheit ist in erster Linie Prävention.

Beispiele hierfür sind

- Physikalische Sicherheitsmerkmale auf Geldscheinen (Ziel Fälschungssicherheit), wie z.B. Wasserzeichen, Sicherheitsfaden, Infrarot- und UV-Farben
- Physikalische und kryptographische Sicherheitsmerkmale bei hoheitlichen Dokumenten (Ziel Fälschungs- und Verfälschungssicherheit)
- Härtung von IT-Systemen durch Penetrationstests (Ziele nächste Folie)
- Verschlüsselung von Dokumenten, E-Mails

Schutzziele

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Klassische Schutzziele: Confidentiality, Integrity and Availability (CIA)

- Vertraulichkeit (engl. Confidentiality)
- Integrität (engl. Integrity)
 - Authentizität (engl. Authenticity)
 - Nichtabstreitbarkeit (engl. Non-Repudiation)
- Verfügbarkeit (engl. Availability)

Schutzziele bzgl. Datenschutz

- Anonymität
- Pseudonymität

Schutzziel Vertraulichkeit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Vertraulichkeit soll sicherstellen, dass Informationen nur autorisierten Personen zugänglich sind.

Maßnahmen zur Umsetzung des Schutzziels Vertraulichkeit:

- Kryptographische Verschlüsselungsverfahren
- Überbringen von Dokumenten durch vertrauenswürdigen Kurieren
- Zutrittsregeln (Gebäudesicherung, Raumsicherung)
- Zugriffskontrollen (geeignete Leserechte für gespeicherte Dateien/Verzeichnisse)

Schutzziel Integrität

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Unter Integrität versteht man die Vollständigkeit und Unverfälschtheit der Daten für den Zeitraum, in dem sie von einer autorisierten Person erstellt, übertragen oder gespeichert wurden. Darin sind sowohl absichtliche als auch unabsichtliche, z. B. durch technische Fehler verursachte, Veränderungen enthalten.

Maßnahmen zur Umsetzung des Schutzziels Integrität:

- Kryptographische Hashfunktionen, Datenauthentisierung
- Sichere Aufbewahrung von Kopien zum späteren Abgleich mit dem Original
- Zugriffs- und Zutrittsregeln

Schutzziel Datenauthentizität

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Die Authentizität von Daten ist gewährleistet, wenn der Urheber der Daten vom Empfänger eindeutig identifizierbar und seine Urheberschaft nachprüfbar ist. Dies beinhaltet auch die Integrität der Daten.

Maßnahmen zur Umsetzung des Schutzziels Datenauthentizität:

- Datenauthentisierung, elektronische Signaturen
- händisches Unterschreiben eines Dokumentes
- persönliche Übergabe von Daten

Schutzziel Instanzenauthenzizität

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein Objekt oder Subjekt wird als authentisch bezeichnet, wenn dessen Echtheit und Glaubwürdigkeit anhand einer eindeutigen Identität und charakteristischer Eigenschaften überprüfbar ist.

Maßnahmen zur Umsetzung des Schutzziels Instanzenauthenzizität:

- Benutzername/Passwort
- Challenge-Response-Protokolle
- Ableich der Identität auf Basis hoheitlicher Dokumente (Reisepass, Personalausweis)

Schutzziel Nichtabstreitbarkeit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Die Nichtabstreitbarkeit von Daten ist gewährleistet, wenn der Ersteller der Daten die Erzeugung im Nachhinein nicht abstreiten kann (gerade auch gegenüber Dritten).

Maßnahmen zur Umsetzung des Schutzziels Nichtabstreitbarkeit:

- elektronische Signaturen
- händische Unterschrift
- Nutzung vertrauenswürdiger Zeugen (z.B. Notar)

Schutzziel Integrität, Authentizität, Nichtabstreitbarkeit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Abgrenzung der Begriffe Integrität, Authentizität und Nichtabstreitbarkeit:

- Offensichtlich gilt:
 - Aus der Nichtabstreitbarkeit folgt die Authentizität
 - Aus der Authentizität folgt die Integrität
- Die Umkehrung gilt im Allgemeinen nicht:
 - Sicheres Aufbewahren einer Kopie zum späteren Abgleich sorgt für die Integrität, es kann damit aber nicht festgestellt werden, wer die Daten erzeugt hat.
 - Bei einer persönlichen Übergabe weiß der Empfänger, von wem er die Daten hat, kann dies aber gegenüber einem Dritten nicht nachweisen.

Authentisierung, Authentifizierung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Abgrenzung der Begriffe Authentisierung, Authentifizierung
(beide engl. authentication):

- Authentisierung: Nachweis der Identität
 - Ich weise mich durch Eingabe meines Benutzernamens/Passwortes aus
 - Ich weise mich mit meinem Personalausweis aus
- Authentifizierung: Prüfung des Nachweises
 - Benutzername/Passwort wird geprüft
 - Personalausweis und Verknüpfung mit meiner Person werden geprüft

Nach der Authentifizierung ist das Subjekt autorisiert entsprechend seiner Berechtigungen zu arbeiten.

Schutzziel Verfügbarkeit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein IT-System gewährt Verfügbarkeit, wenn autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Die Messung der Verfügbarkeit erfolgt üblicherweise nach folgender Formel:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtlaufzeit} - \text{Ausfallzeit}}{\text{Gesamtlaufzeit}}$$

Maßnahmen zur Umsetzung des Schutzziels Verfügbarkeit:

- Datensicherung
- Vertretungsregeln

Schutzziele Anonymität und Pseudonymität

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Anonymität: Personenbezogene Daten werden so verändert, dass diese nicht oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können.
- Pseudonymität: Personenbezogene Daten werden so verändert, dass diese nur unter Kenntnis der Zuordnungsvorschrift einer Person zugeordnet werden können.

Anonymität, Pseudonymität

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Abgrenzung der Begriffe Anonymität, Pseudonymität

- Beispiele für Anonymität sind
 - Aliase in Foren, Chaträumen, die keine Anmeldung erfordern oder keine personenbezogenen Daten erheben
- Beispiele für Pseudonymität sind
 - Aliase in Foren, Chaträumen, die personenbezogene Daten erheben
 - Aliase in Webdiensten wie ebay, amazon (diese erheben personenbezogene Daten)

IT-Sicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel der IT-Sicherheit ist die Verfügbarkeit der Daten, Dienste und Anwendungen zu gewährleisten, sowie die Integrität und Vertraulichkeiten der Daten sicher zu stellen.

Hierzu benötigen wir ein Verständnis für die Begriffe

- Gefahr, Bedrohung, Gefährdung
- Schwachstelle
- Angriff
- Schadensszenario
- Risiko

Gefahr

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Eine Gefahr ist ein Sachverhalt, bei dem ohne konkreten zeitlichen, räumlichen oder personellen Bezug bei ungehindertem Ablauf des zu erwartenden Geschehens in absehbarer Zeit mit hinreichender Wahrscheinlichkeit ein Schaden für ein schutzwürdiges Gut eintreten wird.

Beispiele hierfür sind (ohne besonderen Bezug zur IT-Sicherheit)

- Hochwasser (Gefahr für Leib und Leben, finanzieller Verlust)
- Pest (Gefahr für Leib und Leben)

Bedrohung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Eine Bedrohung ist eine Gefahr mit zeitlichem, räumlichem oder personellem Bezug zu einem Schutzziel.

Kurz: Bedrohungen sind potentielle Gefahren

- Hochwasser ist eine Bedrohung für Leib und Leben von Menschen an der Oder (aber nicht in Darmstadt)
- Pest ist eine Gefahr für Leib und Leben, aber keine Bedrohung (der Pesterreger ist ausgestorben)

Gefährdung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Eine Gefährdung bezieht sich ganz konkret auf eine bestimmte Situation oder auf ein bestimmtes Objekt und beschreibt die Wahrscheinlichkeit, mit der eine potenzielle Gefahr (d.h. Bedrohung) zeitlich oder räumlich auftritt.

Anders ausgedrückt: Trifft eine Bedrohung auf eine Schwachstelle (z.B. technische oder organisatorische Mängel), so entsteht eine Gefährdung.

- Bei zu niedrigen Deichen ist Hochwasser eine Gefährdung

Gefährdungskategorien

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Gefährdungen finden sich üblicherweise in folgenden Kategorien

- Höhere Gewalt (z.B. Hochwasser, Blitzeinschlag, globaler Stromausfall)
- Technische Fehler (z.B. defekte Datenträger, Ausfall einer Datenbank)
- Fahrlässigkeit (z.B. Nichtbeachtung von Sicherheitsmaßnahmen, ungeeigneter Umgang mit Passwörtern)
- Organisatorische Mängel (z.B. fehlende oder unzureichende Regelungen, nicht erkannte Sicherheitsvorfälle)
- Vorsätzliche Handlungen (z.B. Abhören und Manipulation von Leitungen, Schadprogramme, Diebstahl)

Angriff

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein Angriff bezeichnet einen unautorisierten Zugriff bzw. Zugriffsversuch auf ein IT-System oder eine Information.

Technische Angriffe lassen sich in zwei Kategorien unterteilen:

- Passive Angriffe: Zielen auf Informationsgewinnung (Schutzziel Vertraulichkeit) z.B. durch Abhören von Datenleitungen
- Aktive Angriffe: Zielen auf Informationsveränderung (Schutzziel Integrität und Verfügbarkeit) z.B. Vortäuschen einer falschen Identität, um Zugriff auf ein System zu erhalten

Angriffe gegen IT-Systeme geschehen auf Grund unterschiedlichster Motivationen:

- Hacker
- Cracker
- Unternehmen
- Geheimdienste
- Whistleblower

Schadensszenario I

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Das Brechen der definierten Schutzziele (erfolgreicher Angriff auf ein IT-Systeme durch Ausnutzen einer Schwachstelle) kann unterschiedliche Schäden verursachen.

Üblich ist die Einteilung in folgende Schadensszenarien:

- Verstoß gegen Gesetze, Vorschriften, Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung
- Finanzielle Auswirkungen

Risiko I

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz, bezogen auf die Abweichung des gesteckten Zieles.

In Bezug auf IT-Sicherheit, das Produkt aus

- Wahrscheinlichkeit dafür, dass ein Schutzziel gebrochen wird, und
- Höhe des Schadens, der sich daraus ergibt

Die Bestimmung der Risiken hilft bei der Priorisierung umzusetzender Maßnahmen

Risiko II

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

$$\text{Risiko} = \text{Eintrittswahrscheinlichkeit} \cdot \text{Schadenshöhe}$$

Eintrittswahrscheinlichkeit und Schadenshöhe lassen sich nur schwer quantifizieren

- Für Eintrittswahrscheinlichkeit: Welche Mittel wird ein Angreifer einsetzen
 - hängt von seiner Motivation ab
 - nicht nur abhängig von finanziellen Gewinnaussichten, sondern teilweise auch vom persönlichen Ergeiz (z.B. Whistleblower)
- Für Schadenshöhe: Abschätzung, welche Folgen ein Angriff hat
 - meist sind mehrere Schadensszenarien betroffen
 - hängt von der konkreten Institution ab
(für kleine Unternehmen kann ein Verlust von 100.000 Euro existenzgefährdend sein, für Konzerne nicht)

Risiko III

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

$$\text{Risiko} = \text{Eintrittswahrscheinlichkeit} \cdot \text{Schadenshöhe}$$

Folgende Vereinfachung (nicht quantitative, sondern qualitative Bewertung):

- Klassifiziere Eintrittswahrscheinlichkeit in mittel (1), hoch (2), sehr hoch (3)
- Klassifiziere Schadenshöhe in mittel (1), hoch (2), sehr hoch (3)
- Werte für das Risiko: 1 (unbedeutend) bis 9 (kritisch)

Rechtliche Rahmen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

IT-Sicherheit sollte nicht nur im Eigeninteresse einer Institution umgesetzt werden. Vielfach fordern Gesetze die Umsetzung geeigneter IT-Sicherheitsmaßnahmen, z.B.:

- Bundesdatenschutzgesetz und Datenschutzgesetze der Bundesländer
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- Teledienstedatenschutzgesetz
- Telekommunikationsgesetz

Mit Datenschutz wird der Schutz personenbezogener Daten vor Missbrauch durch Dritte bezeichnet.

- Die Privatsphäre jedes Einzelnen soll geschützt werden.
- Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung.
- Grundidee ist, dass der Einzelne die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält.

Bundesdatenschutzgesetz I

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundpfeiler des Bundesdatenschutzgesetzes (BDSG) sind die Prinzipien

- Datenvermeidung,
- Datensparsamkeit, sowie
- das allgemeine Verbot der Verarbeitung personenbezogener Daten.

Grundsätzlich dürfen personenbezogene Daten nur mit Einwilligung der Betroffenen oder aufgrund gesetzlicher Gestattung verarbeitet werden (§ 4 Abs. 1 BDSG).

Bundesdatenschutzgesetz II

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Das Bundesdatenschutzgesetz (§ 9) verpflichtet Daten verarbeitende Stellen, geeignete technische und organisatorische Maßnahmen zum Schutz der erhobenen Daten zu treffen (Datensicherheit).

Personenbezogene Daten dürfen

- nur Befugten zugänglich sein, da sie vertraulich sind, und
- dürfen nicht unbemerkt verändert oder gelöscht werden.

Weitere Gesetze I

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich:

- Verpflichtet u.a. Aktiengesellschaften zur Schaffung eines unternehmensinternen Risikofrüherkennungssystems
- § 91 Abs. 2: Der Vorstand muss geeignete Maßnahmen treffen, um den Fortbestand der Gesellschaft gefährdende Entwicklungen früh zu erkennen
- Gefährdungen können auch durch fehlende IT-Sicherheit entstehen

Weitere Gesetze II

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Teledienstedatenschutzgesetz:

- § 4 Abs. 4 Nr. 3 besagt: Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.
- Anwendungsbereich:
 - Internet- und E-Mailprovider wie Deutsche Telekom, Strato usw.
 - Institutionen, die ihren Mitarbeitern Zugang zu Internet und E-Mail gewähren

Weitere Gesetze III

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Telekommunikationsgesetz:

- Enthält eine Reihe von Vorschriften (§§ 88-115)
 - zum Schutz des Fernmeldegeheimnisses (Vertraulichkeit),
 - zum Datenschutz, und
 - zu Belangen der öffentlichen Sicherheit (Verfügbarkeit)
- Verpflichtet Diensteanbieter zur Ausarbeitung eines IT-Sicherheitskonzepts

Privacy by Design

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Entwickelt in den 90er Jahren von Ann Cavoukian
(Information & Privacy Commissioner der Kanadischen Provinz Ontario)

Grundidee:

- Rechtsvorschriften allein sind nicht ausreichend für die Gewährleistung von Datenschutz
- Nutzerinnen und Nutzer müssen wieder in die Lage versetzt werden, über ihre personenbezogenen Daten bestimmen zu können

Hierfür wurden sieben Grundprinzipien aufgestellt

Privacy by Design: Sieben Grundprinzipien

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
Der Privacy by Design Ansatz sieht mögliche Verletzungen der Privatsphäre voraus und verhindert sie, bevor sie entstehen könnten.
2. Datenschutz als Standardeinstellung
Ein IT-System bietet systemimmanent als Standardeinstellung den Schutz der Privatsphäre und personenbezogener Daten.
3. Der Datenschutz ist in das Design eingebettet
Zur Entwurfsphase eines IT-Systems, einer Software oder eines Geschäftsprozesses wird der Datenschutz bereits berücksichtigt.

Privacy by Design: Sieben Grundprinzipien

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

4. Volle Funktionalität

Datenschutz und Sicherheit können in einem System gleichzeitig realisiert werden und nicht nur das eine auf die Kosten des anderen. Die Umsetzung von Sicherheit und Datenschutz bringt alle Vorteile für alle Beteiligten.

- ## 5. Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus
- Personenbezogene Daten sind von der Erfassung bis zur Vernichtung im gesamten Lebens- und Verarbeitungszyklus innerhalb einer Software bzw. eines IT-Systems mittels starker Sicherheitsmaßnahmen geschützt.

Privacy by Design: Sieben Grundprinzipien

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

6. Sichtbarkeit und Transparenz - Für Offenheit sorgen
Komponenten und Verfahren eines IT-Systems können unabhängigen Prüfungen unterzogen werden. Sie sind einsehbar und für alle Beteiligten (Nutzer und Anbieter) transparent.
7. Die Wahrung der Privatsphäre der Nutzer - nutzerzentrierte Gestaltung
Betreiber und Architekten von IT-Systemen stellen den Nutzer und seine Interessen bzgl. personenbezogener Daten und Privatsphäre in den Mittelpunkt. Voreinstellungen sind datenschutz- und benutzerfreundlich. Darüber hinaus bieten IT-Systeme angemessene Benachrichtigungen bzgl. personenbezogener Daten an.

Privacy by Design: Wettbewerbsvorteil

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Werden solche Produkte von den Nutzerinnen und Nutzern honoriert?

- Für Datenschutz und IT-Sicherheit interessiert sich nur eine Minderheit
- Seit Bekanntwerden der massiven Überwachungsprogramme der US-amerikanischen und britischen Geheimdienste ändert sich das
- US-amerikanische Firmen sehen einen klaren Wettbewerbsnachteil durch die Verpflichtung, mit den Geheimdiensten zusammenzuarbeiten.
- Seit iOS8 gibt es keine Möglichkeit mehr für Behörden auf iPhones und iPads zuzugreifen (auch nicht mit Apples Hilfe)
- Google folgt mit Android

Kryptologie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Das Wissenschaftsgebiet Kryptologie setzt sich zusammen aus den Teilgebieten:

- Kryptographie: altgriechisch „κρυπτος“ (geheim) und „γραφειν“ (schreiben)
Ursprünglich also Wissenschaft der Verschlüsselung von Nachrichten
- Kryptoanalyse: altgriechisch „αναλυσις“ (Auflösung)
Analyse der Verfahren, um diese zu brechen oder Sicherheit zu erhöhen

Kryptologie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Die klassische Kryptologie diente der Geheimhaltung von Nachrichten und wurde hauptsächlich von Militärs, Geheimdiensten und Diplomaten genutzt.
 - Schutzziel Vertraulichkeit
- Die moderne Kryptographie (etwa seit 1975) beschäftigt sich mit erheblich weitergehenden Kommunikations- und Sicherheitsproblemen.
 - Schutzziele Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit

Kommunikationsmodell

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

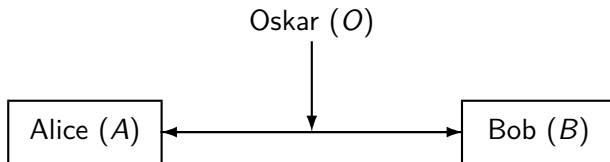
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Alice (A) und Bob (B) wollen sicher kommunizieren (vgl. Schutzziele)
- Oskar (O) versucht, die Schutzziele zu durchbrechen
 - Passiver Angriff: Abhören der Daten
 - Aktiver Angriff: Manipulation (z.B. Verändern, Fälschung Sender) der Daten



Schutzziele

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

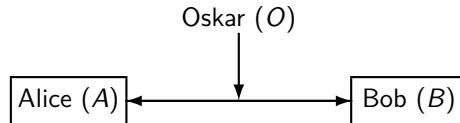
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- *Vertraulichkeit*: Nachricht zwischen A und B kann nicht von O gelesen werden
- *Integrität*: Nachricht zwischen A und B wird nicht verändert bzw. A und B können erkennen, ob Nachrichten verändert wurden
- *Datenauthentizität*: B kann Nachricht von A zweifelsfrei A zuordnen
- *Instanzauthentizität*: B kann die Identität von A zweifelsfrei feststellen
- *Nichtabstreitbarkeit*: B kann Nachricht von A zweifelsfrei auch einer dritten Partei als Nachricht von A nachweisen

Kryptographische Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beispiele für kryptographische Verfahren für alle Schutzziele:

- *Vertraulichkeit*: Verschlüsselung
- *Integrität*: Hashfunktionen, Message Authentication Codes (MAC), Signaturen
- *Datenauthentizität*: Message Authentication Codes (MAC), Signaturen
- *Nichtabstreitbarkeit*: Signaturen
- *Instanzauthentizität*: Challenge Response Protokolle

Kerckhoffsche Prinzipien

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Auguste Kerckhoffs (ein niederländischer Linguist und Kryptograph) 1883:
(La Cryptographie militaire)

- Ist ein System nicht beweisbar sicher, so sollte es praktisch sicher sein.
- Das Design eines System sollte keine Geheimhaltung erfordern und sollte sich ohne Gefahr in den Händen des Feindes befinden können.
- Ein Kryptosystem muss einfach bedienbar sein.

Wichtigstes Kerckhoffsches Prinzip

Ein Angreifer kennt das kryptographischen Verfahren, nur die privaten oder symmetrischen Schlüssel sind geheim.

Symmetrische und Asymmetrische Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir unterscheiden zwei Klassen kryptographischer Verfahren

- *Symmetrische Verfahren*: A und B nutzen den selben Schlüssel
 - Der Schlüssel muss zwischen A und B sicher ausgetauscht werden
 - vertraulich: O darf den Schlüssel nicht kennen
 - authentisch: A und B müssen wissen, wem sie vertrauliche Nachrichten schicken
- *Asymmetrische Verfahren*: A und B haben jeweils ein Schlüsselpaar
 - A hat Schlüsselpaar (pk_A, sk_A) (pk_A : public key, sk_A : secret key)
 - B hat Schlüsselpaar (pk_B, sk_B) (pk_B : public key, sk_B : secret key)
 - Die öffentlichen Schlüssel müssen zwischen A und B sicher ausgetauscht werden
 - authentisch: A und B müssen wissen, wem sie vertrauliche Nachrichten schicken
 - O darf die Schlüssel pk_A, pk_B nicht kennen (sk_A, sk_B aber schon)

Symmetrische Verschlüsselungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schutzziel: Vertraulichkeit

- Verschlüsselungsfunktion enc (encryption):
 - Klartext m , Schlüssel k , Chiffre $c = \text{enc}(k, m)$
- Entschlüsselungsfunktion dec (decryption):
 - Chiffre c , Schlüssel k , Klartext $m = \text{dec}(k, c)$
- Zusammenhang: Für alle Klartexte m und Schlüssel k : $\text{dec}(k, \text{enc}(k, m)) = m$

A Schlüssel: k

B Schlüssel: k

compute $c := \text{enc}(k, m)$

\xrightarrow{c}

compute $m' := \text{dec}(k, c)$

Wegen $\text{dec}(k, \text{enc}(k, m)) = m$ gilt $m = m'$.

Beispiel CAESAR-Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Eingesetzt von Gaius Iulius Caesar (römischer Kaiser 100 - 44 v. Chr.):

- Verschlüsselung: Verschiebe alle Buchstaben um einen festen Wert k nach rechts
Für $k = 3$: $A \rightarrow D$, $B \rightarrow E$, $C \rightarrow F$, \dots , $Z \rightarrow C$
- Entschlüsselung: Verschiebe alle Buchstaben um den selben Wert nach links
Für $k = 3$: $A \rightarrow X$, $B \rightarrow Y$, $C \rightarrow Z$, \dots , $Z \rightarrow W$
- Dann gilt:
 - $\text{enc}(3, \text{CAESAR}) = \text{FDHVDU}$
 - $\text{dec}(3, \text{FDHVDU}) = \text{CAESAR}$

Sicherheit CAESAR-Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Um den Klartext zu erhalten, probieren wir alle Schlüssel aus:

Ciphertext:

OLYY KLY YPUNL

Verschiebung um 1 nach links:

NKXX JKX XOTMK

Verschiebung um 2 nach links:

MJWW IJW WNSLJ

Verschiebung um 3 nach links:

LIVV HIV VMRKI

Verschiebung um 4 nach links:

KHUU GHU ULQJH

Verschiebung um 5 nach links:

JGTT FGT TKPIG

Verschiebung um 6 nach links:

IFSS EFS SJOHF

Verschiebung um 7 nach links:

HERR DER RINGE

Sicherheit CAESAR-Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Es gibt 26 Buchstaben im deutschen Alphabet
 - Verschiebung um 27 ist das selbe wie Verschiebung um 1, ...
- Es gibt also nur 26 verschiedene Schlüssel
 - Durchsuchen des Schlüsselraums möglich (**Schlüsselexhaustion, Brute Force**)
- Für große Nachricht ergibt sich in der Regel nur ein sinnvollen Text
- Erster kryptoanalytischer Ansatz: Schlüsselexhaustion

Erkenntnis

Für die Sicherheit eines Verschlüsselungsverfahrens muss der Schlüsselraum (Menge der möglichen Schlüssel) so groß sein, dass nicht alle Schlüssel durchprobiert werden können.

Modifiziertes CAESAR-Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Ersetze Buchstaben nicht mittels fester Verschiebung, sondern beliebig (Monoalphabetische Verschlüsselung)

A	B	C	D	...	X	Y	Z
↓	↓	↓	↓	...	↓	↓	↓
X	E	S	U	...	M	H	P

- Wie viele Schlüssel gibt es?
 - A kann durch 26 Buchstaben ersetzt werden
 - B kann durch 25 Buchstaben ersetzt werden
 - Insgesamt: $26 \cdot 25 \cdot \dots \cdot 2 \cdot 1 = 26!$ verschiedene Schlüssel
- 26! Schlüssel sind zu viel, um alle durchzuprobieren

Große Zahlen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Anzahl Schlüssel: $26! \approx 2^{88} \approx 10^{27}$

- Anzahl der Atome der Erde 2^{170}
- Anzahl der Atome der Sonne 2^{190}
- Anzahl der Atome in unserer Galaxis 2^{223}
- Zeit bis die Sonne zur Nova wird 2^{30} Jahre

Angenommen, ein Computer berechnet pro Sekunde $2 \cdot 10^9$ Entschlüsselungen:

$$\begin{aligned} \frac{\text{Anzahl möglicher Schlüssel}}{\text{Entschl. je Sek.} \cdot \text{Sek. pro Jahr}} &= \frac{10^{27}}{(2 \cdot 10^9 \text{ s}^{-1}) \cdot (3.15 \cdot 10^7 \text{ s/Jahr})} \\ &= \frac{10^{11}}{6.3} > 10^{10} = 10.000.000.000 \text{ Jahre} \end{aligned}$$

Sicherheit des modifizierten CAESAR-Verfahrens

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Angriff über relative Häufigkeiten in sinnvollen deutschen Texten

1. Buchstabe E: 17.4 %

2. Buchstabe N: 09,8 %

3. Buchstabe I: 07.6 %

4. Buchstabe S: 07,3 %

5. Buchstabe R: 07,0 %

6. Buchstabe A: 06,5 %

7. Buchstabe T: 06,2 %

8. Buchstabe D: 05,1 %

⋮

26. Buchstabe Q: 00,02 %

- Richtige Wahl von E und N liefert schon ca. $1/4$ des Textes.
Rest erhält man durch geschicktes Raten.

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of

sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt

yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts

sof Kdafopdtp xt Meyyxtpot uoxt Otso.

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvy Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e e e e e e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt
e e e e e e e e e
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e e e e e e e e e e
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
e e e e E e

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E							

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e e e n n e e n n en e e
sortkonmhg ldf Aoxof hoxtoh oxtdtsovalxpghot Poydfghgkph oxt
e n e e e e ne e n n e en e e n
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e n e e e e en e e e e n
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
e e n n n en e n En e

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N						

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e e e n n e e n n en e e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt
e n e e e e ne e n n e en e e n
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e n e e e e e en e e e e e n
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
e e n n n en e n En e

Letztes Wort: Otse = Ende oder Ente

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N						

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e e e n n e e nd n end e d e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt
de n e e e e ne e n nde en e e n
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e nde e e e e en e de e ede nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
de e n n n en e n Ende

Letztes Wort: Otse = Ende oder Ente

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N				D		

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e e e n n e e nd n end e d e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de n e e e e ne e n nde en e e n
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e nde e e e e en e de e ede nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
de e n n n en e n Ende

Viertletzttes Wort: xt = in

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N				D		

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e i e e in n e e nd n endi e d e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt
de n e eie eine ein nde i en e ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e nde e i e e e en e de e ede nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
de e n in in en ein Ende

Viertletztes Wort: xt = in

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I			D		

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
e i e e in n e e nd n endi e d e
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de n e eie eine ein nde i en e ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
e nde e i e e e en e de e ede nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
de e n in in en ein Ende

Kurze Wörter: sof,soh = der,des

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I			D		

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvy Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
s err i e e in n e e s nd n endi e d ss er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de n e s r eier seines ein nde i s en e r s s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders r e i e es e en e r des eredes nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der re n in in en ein Ende

Kurze Wörter: sof,soh = der,des

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R		D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvy Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
s err i e e in n e e s nd n endi e d ss er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxphgot Poydfghgkph oxt
de n e s r eier seines ein nde i s en e r s s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders r e i e es e en e r des eredes nd
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der re n in in en ein Ende

dts = und

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R		D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
s err i eu e in n eu e s nd n uendi e d ss er
sortkonmhg ldf Aoxof hoxtoh oxtdtsovalxpghot Poydfghgkph oxt
de n e s ur eier seines einunde i s en e ur s s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders r e i es es e en e r des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der u re un in in en ein Ende

dts = und

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
s err i eu e in n eu e s nd n uendi e d ss er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de n e s ur eier seines einunde i s en e ur s s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders r e i es es e en e r des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der u re un in in en ein Ende

skhh = dass

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
A s err i eu e in n eu e sand an uendi e dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae s ur eier seines einunde i s en e ur s a s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae i es es e en e ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

skhh = dass

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvy Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
A s err i eu e in n eu e sand an uendi e dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae s ur eier seines einunde i s en e ur s a s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae i es es e en e ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

Kvh = Als

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
Als err il eu elin n eu elsand an uendi e dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae s ur eier seines einundel i s en e ur s a s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae i es es e en lle ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

Kvh = Als

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvy Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
Als err il eu elin n eu elsand an uendi e dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae s ur eier seines einundel i s en e ur s a s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae i es es e en lle ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

$G = T?$

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
Als err il eutelin n eutelsand an uendi te dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae st ur eier seines einundel i sten e urtsta s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae ti es est e en lle ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

$G = T?$

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	T

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
Als err il eutelin n eutelsand an uendi te dass er
sortkonmhg ldf Aoxof hoxtoh oxtdtsovalxpghot Poydfghgkph oxt
de nae st ur eier seines einundel i sten e urtsta s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
es nders rae ti es est e en lle ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in in en ein Ende

Moff = Herr, yohetsofh = besonders

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	T

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Modifizierten CAESAR-Verfahrens: Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Geheimtext:

Kvh Moff Yxvye Yodgovxt zet Yodgovhkts ktudotsxpgo, skhh of
Als Herr Bilbo Beutelin on Beutelsand an uendi te dass er
sortkonmhg ldf Aoxof hoxtoh oxttdtsovalxpghot Poydfghgkph oxt
de nae hst ur eier seines einundel i sten eburtsta s ein
yohetsofh wfkonmgxpoh Aohg poyot cevvo, ckf soh Pofosoh dts
besonders rae hti es est eben olle ar des eredes und
sof Kdafopdtp xt Meyyxtpot uoxt Otso.
der Au re un in Hobbin en ein Ende

Moff = Herr, yohetsofh = besonders

Häufigkeiten im Text (Plätze 1 - 8):

O	T	X	F	D	S	H	G
36	18	12	12	11	11	10	9
E	N	I	R	U	D	S	T

Relative Häufigkeiten (Plätze 1 - 8):

E	N	I	S	R	A	T	D
17,4	9,8	7,6	7,3	7,0	6,5	6,2	5,1

Sicherheit des modifizierten CAESAR-Verfahrens

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Solche Angriffe heißen auch statistische Angriffe

Erkenntnis

- Zur Beurteilung der Sicherheit müssen alle kryptoanalytischen Methoden berücksichtigt werden
- Größe des Schlüsselaums ist nur eine notwendige (keine hinreichende) Bedingung für die Sicherheit.

One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir betrachten Nachrichten als Bitstrings:

- Eine Nachricht $m = (m_1, \dots, m_n)$ besteht nur aus 0 und 1
- Für eine Nachricht der Länge $n \in \mathbb{N}$ schreiben wir auch kurz: $m \in \{0, 1\}^n$
- Beispiel: Kodierung der Buchstaben über ASCII-Kode
 $A = 01000001$, $B = 01000010$, ...

Als Schlüssel nutzen wir ebenfalls Bitstrings:

- Für eine Nachricht der Länge $n \in \mathbb{N}$ benötigen wir
- Schlüssel $k = (k_1, \dots, k_n) \in \{0, 1\}^n$ der Länge n .

Rechenoperation: Addition modulo 2 (XOR, in Zeichen \oplus)

- $0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$

One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Verschlüsselung: Ciphertext $c = m \oplus k$.

$$c = (c_1, \dots, c_n) = (m_1, \dots, m_n) \oplus (k_1, \dots, k_n) = (m_1 \oplus k_1, \dots, m_n \oplus k_n)$$

- Entschlüsselung: Klartext $m = c \oplus k$.

$$m = (m_1, \dots, m_n) = (c_1, \dots, c_n) \oplus (k_1, \dots, k_n) = (c_1 \oplus k_1, \dots, c_n \oplus k_n)$$

One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Verschlüsselung: Ciphertext $c = m \oplus k$.

$$c = (c_1, \dots, c_n) = (m_1, \dots, m_n) \oplus (k_1, \dots, k_n) = (m_1 \oplus k_1, \dots, m_n \oplus k_n)$$

- Entschlüsselung: Klartext $m = c \oplus k$.

$$m = (m_1, \dots, m_n) = (c_1, \dots, c_n) \oplus (k_1, \dots, k_n) = (c_1 \oplus k_1, \dots, c_n \oplus k_n)$$

- Korrektheit: Wegen $0 \oplus 0 = 0$ und $1 \oplus 1 = 0$ gilt

$$k \oplus k = (k_1, \dots, k_n) \oplus (k_1, \dots, k_n) = (k_1 \oplus k_1, \dots, k_n \oplus k_n) = (0, \dots, 0)$$

One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Verschlüsselung: Ciphertext $c = m \oplus k$.

$$c = (c_1, \dots, c_n) = (m_1, \dots, m_n) \oplus (k_1, \dots, k_n) = (m_1 \oplus k_1, \dots, m_n \oplus k_n)$$

- Entschlüsselung: Klartext $m = c \oplus k$.

$$m = (m_1, \dots, m_n) = (c_1, \dots, c_n) \oplus (k_1, \dots, k_n) = (c_1 \oplus k_1, \dots, c_n \oplus k_n)$$

- Korrektheit: Wegen $0 \oplus 0 = 0$ und $1 \oplus 1 = 0$ gilt

$$k \oplus k = (k_1, \dots, k_n) \oplus (k_1, \dots, k_n) = (k_1 \oplus k_1, \dots, k_n \oplus k_n) = (0, \dots, 0)$$

- Wir erhalten

$$c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$$

One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Klartext:	G	E	H	E	I	M
ASCII:	01000111	01000101	01001000	01000101	01001001	01001101
	\oplus					
Schlüssel:	00111000	10011110	10011111	00010111	10100111	10011110
	=					
Ciphertext:	01111111	11011011	11010111	01010010	11101110	11010011
	\oplus					
Schlüssel:	00111000	10011110	10011111	00010111	10100111	10011110
	=					
ASCII:	01000111	01000101	01001000	01000101	01001001	01001101
Klartext:	G	E	H	E	I	M

Einschub: Wahrscheinlichkeitstheorie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir betrachten folgendes Experiment: Münzwurf

- Bei einmaligem Münzwurf gibt es nur zwei Ereignisse: Kopf oder Zahl
 - Die Wahrscheinlichkeit, Kopf zu werfen, ist $\frac{1}{2}$, kurz $\Pr(\text{Kopf}) = \frac{1}{2}$
 - Die Wahrscheinlichkeit, Zahl zu werfen, ist ebenfalls $\frac{1}{2}$

Einschub: Wahrscheinlichkeitstheorie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir betrachten folgendes Experiment: Münzwurf

- Bei einmaligem Münzwurf gibt es nur zwei Ereignisse: Kopf oder Zahl
 - Die Wahrscheinlichkeit, Kopf zu werfen, ist $\frac{1}{2}$, kurz $\Pr(\text{Kopf}) = \frac{1}{2}$
 - Die Wahrscheinlichkeit, Zahl zu werfen, ist ebenfalls $\frac{1}{2}$

Identifiziere Kopf mit 0 und Zahl mit 1.

Einschub: Wahrscheinlichkeitstheorie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir betrachten folgendes Experiment: Münzwurf

- Bei einmaligem Münzwurf gibt es nur zwei Ereignisse: Kopf oder Zahl
 - Die Wahrscheinlichkeit, Kopf zu werfen, ist $\frac{1}{2}$, kurz $\Pr(\text{Kopf}) = \frac{1}{2}$
 - Die Wahrscheinlichkeit, Zahl zu werfen, ist ebenfalls $\frac{1}{2}$

Identifiziere Kopf mit 0 und Zahl mit 1.

- Bei zweimaligem Münzwurf gibt es vier Ereignisse: 00, 01, 10 und 11
 - $\Pr(00) = \Pr(01) = \Pr(10) = \Pr(11) = \frac{1}{4}$

Einschub: Wahrscheinlichkeitstheorie

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir betrachten folgendes Experiment: Münzwurf

- Bei einmaligem Münzwurf gibt es nur zwei Ereignisse: Kopf oder Zahl
 - Die Wahrscheinlichkeit, Kopf zu werfen, ist $\frac{1}{2}$, kurz $\Pr(\text{Kopf}) = \frac{1}{2}$
 - Die Wahrscheinlichkeit, Zahl zu werfen, ist ebenfalls $\frac{1}{2}$

Identifiziere Kopf mit 0 und Zahl mit 1.

- Bei zweimaligem Münzwurf gibt es vier Ereignisse: 00, 01, 10 und 11
 - $\Pr(00) = \Pr(01) = \Pr(10) = \Pr(11) = \frac{1}{4}$
- Bei n -maligem Münzwurf gibt es 2^n Ereignisse
 - Die Wahrscheinlichkeit, das richtige Ereignis zu raten: $\frac{1}{2^n}$

Sicherheit One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Für Nachricht $m \in \{0, 1\}^n$ benötigen wir Schlüssel $k \in \{0, 1\}^n$

- Wir nennen k zufällig, wenn $\Pr(k) = \frac{1}{2^n}$
(Wahrscheinlichkeit, dass Angreifer den richtigen Schlüssel errät, ist $\frac{1}{2^n}$)
- Die zufällige Wahl der eingesetzten Schlüssel ist wesentlich für die Sicherheit:
 - Sind alle Schlüssel gleichwahrscheinlich, hat der Angreifer keinen Anhaltspunkt, welcher Schlüssel eingesetzt wurde

Sicherheit One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Welche Angriffe gibt es gegen das One-time Pad?
(Unter der Voraussetzung, dass der Schlüssel zufällig gewählt wurde)
- In unserem Beispiel:
 - Aus Klartext $m = \text{GEHEIM}$ (48 Bit in ASCII) wurde mittels Schlüssel $k = (k_1, \dots, k_{48})$ ein Ciphertext $c = (c_1, \dots, c_{48})$
 - Durchprobieren aller Schlüssel auf den Ciphertext führt zu 2^{48} Klartexten
 - Nicht sinnvolle Texte: üÄY;- AAAAAA **LAIs
 - Sinnvolle Texte: Berlin BOSTON Er ist
 - Ein Angreifer hat keine Information, welcher der sinnvollen Texte der richtige ist

Sicherheit One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Klartext:	001001110	←	Kein Zufall
	\oplus		
Schlüssel:	100011100	←	Zufall
	$=$		
Ciphertext:	101010010	←	Zufall

Aus Sicht des Angreifers ist der Ciphertext eine absolut zufällige Bitfolge

- Genauso zufällig wie der eingesetzte Schlüssel
- Unabhängig vom verschlüsselten Klartext

Erkenntnis

Beim One-time Pad Verfahren liefert der Ciphertext keinerlei Informationen über den Klartext (und damit auch nicht über den eingesetzte Schlüssel).

Absolute Sicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Das One-time Pad ist also sicher im Sinne der folgenden Definition.

Definition

Ein Verschlüsselungsverfahren heißt absolut sicher, wenn es auch gegen Angreifer mit unbeschränkten Ressourcen (Zeit, Rechenleistung) sicher ist.

Absolute Sicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Absolut sichere Verschlüsselungsverfahren haben einen entscheidenden Nachteil:

Claude Shannon, 1948

Ein Verschlüsselungsverfahren kann nur dann absolut sicher sein, wenn der Schlüssel genauso lang ist wie die zu verschlüsselnde Nachricht.

Zum Teil müssen aber große Datenmengen verschlüsselt werden:

- Bilder und Videos von Spionagesatelliten
- Sprach- und Videotelephonie über das Internet

Für die Verschlüsselung von 10 GB benötigen wir einen Schlüssel der Größe 10 GB.

Modifiziertes One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Idee: Verwende den Schlüssel mehrfach

- Wir wollen zwei Nachrichten $m^1 = (m_1^1, \dots, m_n^1)$ und $m^2 = (m_1^2, \dots, m_n^2)$ mit **einem** Schlüssel $k = (k_1, \dots, k_n)$ verschlüsseln.
- Für die Ciphertexte $c^1 = m^1 \oplus k$ und $c^2 = m^2 \oplus k$ gilt dann

$$c^1 \oplus c^2 = (m^1 \oplus k) \oplus (m^2 \oplus k) = m^1 \oplus m^2 \oplus \underbrace{k \oplus k}_{=(0, \dots, 0)} = m^1 \oplus m^2 \quad (1)$$

Wir kennen also die Summe der Klartexte, ohne den Schlüssel kennen zu müssen.

Modifiziertes One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Statistischer Angriff

- Bestimme alle sinnvollen Texte für m^1
- Überprüfe, ob die Wahl von m^1 auch einen sinnvollen Text für m^2 ergibt:
Wegen $c^1 \oplus c^2 = m^1 \oplus m^2$ (Folie 98, Formel (1)) gilt

$$m^2 = c^1 \oplus c^2 \oplus m^1$$

- Wenn ja: haben wir die Nachrichten m^1, m^2 gefunden
 - Wenn nein: wählen wir einen anderen Kandidaten für m^1
- Wahrscheinlichkeit, dass es hier mehrere Möglichkeiten gibt, ist klein
- Wahrscheinlichkeit sinkt mit Anzahl der Nachrichten

Modifiziertes One-time Pad

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Erkenntnis

Selbst auf den ersten Blick kleine Veränderungen eines kryptographischen Verfahrens können zu einer massiven Senkung der Sicherheit führen.

Absolute und praktische Sicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Absolute Sicherheit: Resistent gegen Angreifer mit unbeschränkten Ressourcen
- Praktische Sicherheit: Resistent gegen Angreifer mit beschränkten Ressourcen:
 - Angreifer haben nur beschränkte Rechenkapazität und Zeit
 - Kryptoverfahren sind nur sicher in Bezug auf diese Ressourcen

Definition Sicherheitsniveau

Ein Kryptoverfahren hat ein Sicherheitsniveau von $n \in \mathbb{N}$ Bit, wenn ein Angreifer 2^n Versuche benötigt, dass Verfahren zu brechen.
(Für Verschlüsselungsverfahren: den Klartext zu erhalten.)

Sicherheitsniveau

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Für die Beurteilung des Sicherheitsniveaus müssen alle kryptoanalytischen Verfahren herangezogen werden:
 - Schlüsselexhaustion (Durchprobieren aller Schlüssel)
 - statistische Angriffe (wie beim modifizierten CAESAR-Verfahren)
 - ...
- Sicherheitsniveaus der bisherigen Verfahren:
 - CAESAR-Verfahren: $26 < 2^5$ Schlüssel, also Sicherheitsniveau < 5 Bit
 - modifiziertes CAESAR-Verfahren (monoalphabetische Verschlüsselung)
 - $26! \approx 2^{88}$ Schlüssel, also Sicherheitsniveau nicht größer als 88 Bit
 - statistischer Angriff: Schwer zu quantifizieren, ca. $2^6 > 50$ Versuche
 - Sicherheitsniveau: < 6 Bit
 - One-time Pad: Sicherheitsniveau ∞ Bit, unabhängig von Schlüssellänge

Sicherheitsniveau

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Heutige Kryptoverfahren sollten ein Sicherheitsniveau ≥ 100 Bit haben
 - 2^{100} Versuche sind praktisch nicht durchführbar
 - Solche Verfahren gelten damit als **praktisch sicher**
- Erinnerung: Schlüsselexhaustion ist ein Angriff
 - Sicherheitsniveau ≥ 100 Bit bedeutet also mindestens 2^{100} Schlüssel
 - Für einen Schlüsselraum der Form $\{0, 1\}^n$ also $n \geq 100$

Stromchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

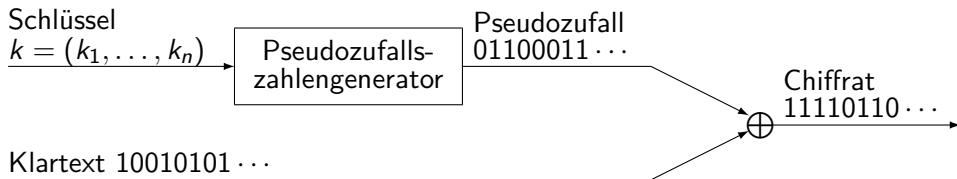
IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Nachbildung des One-time Pads

- Aus Schlüssel $k \in \{0, 1\}^n$, $n \geq 100$ wird ein pseudozufälliger Schlüssel generiert (Schlüsselstrom)
- Der Schlüsselstrom wird komponentenweise mit dem Klartext addiert (XOR)



Stromchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

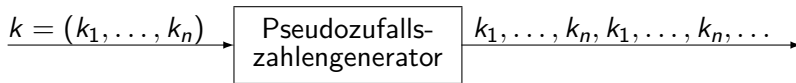
IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Bedingungen muss der Pseudozufallszahlengenerator erfüllen?

- Erste Idee: Nutze Schlüssel k mehrmals



- Unsicher, siehe Folie 99

Welche Bedingungen muss der Pseudozufallszahlengenerator erfüllen?

- Aus 100 Bit Zufall (Schlüssel) lässt sich nicht z.B. 200 Bit Zufall (Schlüsselstrom) berechnen
 - 200 Bit Zufall hieße: Angreifer rät Schlüsselstrom mit Wahrscheinlichkeit $1/2^{200}$
 - Er muss aber nur Schlüssel raten (Wahrscheinlichkeit $1/2^{100}$), und dann den Schlüsselstrom berechnen
- Wir benötigen nur praktische Sicherheit
 - Angreifer (beschränkte Ressourcen) sollte keinen Unterschied feststellen zwischen
 - echtem Zufall
 - Pseudozufall, der von einem Pseudozufallszahlengenerator stammt

Stromchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

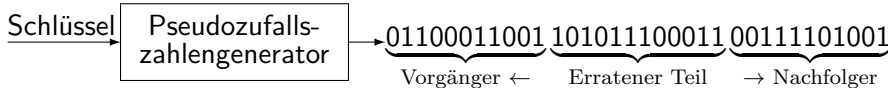
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

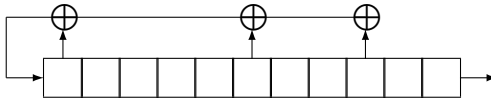
- Formale Definition von Pseudozufallszahlengenerator in den Vorlesungen
 - Kryptologie (Wahlpflicht im Bachelor)
 - Komplexitätstheorie (Master)
- Wichtig für die Sicherheit von Stromchiffren ist u.a. folgende Bedingung:
 - Aus Teilen des Schlüsselstroms dürfen keine Nachfolger bestimmt werden können
 - Aus Teilen des Schlüsselstroms dürfen keine Vorgänger bestimmt werden können



- Ansonsten statistische Angriffe wie beim modifizierten One-time Pad möglich (siehe Folie 99)

Stromchiffren: LFSR

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

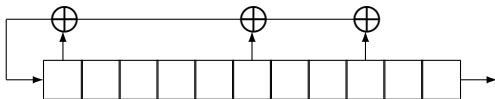
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert

Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

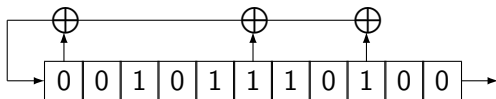
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert

Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

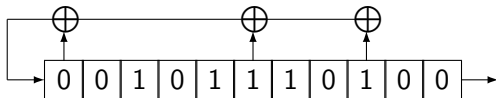
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert
- In jedem Schritt (Takt), wird
 - ein Bit ausgegeben (jenes aus dem letzten Feld)
 - alles um eine Stelle nach rechts verschoben und
 - die ausgezeichneten Bits addiert und an die erste Stelle geschrieben

Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

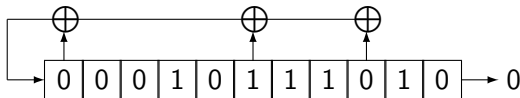
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert
- In jedem Schritt (Takt), wird
 - ein Bit ausgegeben (jenes aus dem letzten Feld)
 - alles um eine Stelle nach rechts verschoben und
 - die ausgezeichneten Bits addiert und an die erste Stelle geschrieben

Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

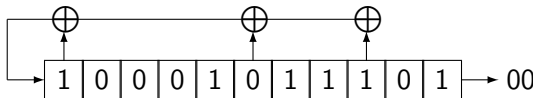
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert
- In jedem Schritt (Takt), wird
 - ein Bit ausgegeben (jenes aus dem letzten Feld)
 - alles um eine Stelle nach rechts verschoben und
 - die ausgezeichneten Bits addiert und an die erste Stelle geschrieben

Stromchiffren: LFSR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

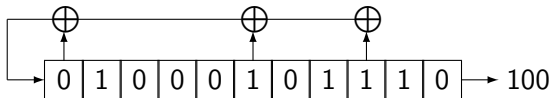
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundbaustein vieler Pseudozufallszahlengeneratoren für Stromchiffren
Linear Feedback Shift Register (LFSR)



- Im ersten Schritt wird das Register mit dem Schlüssel initialisiert
- In jedem Schritt (Takt), wird
 - ein Bit ausgegeben (jenes aus dem letzten Feld)
 - alles um eine Stelle nach rechts verschoben und
 - die ausgezeichneten Bits addiert und an die erste Stelle geschrieben

Stromchiffren: Pseudozufallszahlengeneratoren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

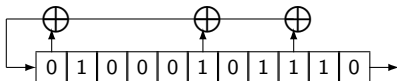
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- LFSRs allein sind nicht geeignet für sichere Pseudozufallszahlengeneratoren (werden als Grundbausteine verwendet)
- Hier lassen sich bei bekanntem Teil des Schlüsselstroms Nachfolger berechnen:
 - Inhalt des obigen Schieberegisters ist nach 11 Takten Teil des Schlüsselstroms
 - Errät ein Angreifer diesen Teil, kann er alle Nachfolger berechnen

Kombination von LFSRs

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Es gibt mehrere Möglichkeiten, LFSRs so zu kombinieren, dass die (gravierende) Schwäche verhindert wird

- Shrinking-Generator:
 - Nutzung von zwei LFSRs (R_1 , R_2)
 - Wenn R_1 Bit 1 ausgibt, wird die Ausgabe von R_2 für Schlüsselstrom genutzt
 - Wenn R_1 Bit 0 ausgibt, wird die Ausgabe von R_2 verworfen
- Summations-Generator:
 - Nutzung von zwei LFSRs (R_1 , R_2)
 - Die Ausgaben von R_1 und R_2 werden addiert (\oplus)
- Dadurch ist es einem Angreifer nicht möglich, aus dem Schlüsselstrom auf die internen Register der LFSRs zu schließen

Vorteile von Stromchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Statistisches Verhalten von LFSRs sind mathematisch sehr gut untersucht
- LFSRs sind sehr effizient in Hardware umzusetzen
 - Benötigen lediglich die Operationen \oplus und Shift
- Ver- und Entschlüsselung sind sehr effizient
- Typisches Beispiel:
 - A5/1: Sprachverschlüsselung zwischen Mobiltelefon und Funkmast
 - Eingesetzt seit den 1990er Jahren
 - Also auf Mobiltelefonen mit geringer Rechenleistung

Blockchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren bilden Bitstrings fester Länge auf Bitstrings der selben Länge ab:
 - Moderne Blockchiffren verarbeiten Bitstrings der Länge 128 (Klartextblock) (diese Länge heißt auch Blockgröße der Blockchiffre)
 - Genutzte Schlüssel müssen eine Bitlänge ≥ 100 haben (siehe Folie 103) (meist werden Schlüssel der Länge 128 Bit genutzt)

Blockchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

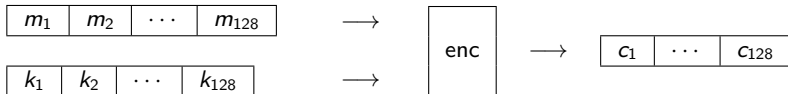
IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren bilden Bitstrings fester Länge auf Bitstrings der selben Länge ab:
 - Moderne Blockchiffren verarbeiten Bitstrings der Länge 128 (Klartextblock) (diese Länge heißt auch Blockgröße der Blockchiffre)
 - Genutzte Schlüssel müssen eine Bitlänge ≥ 100 haben (siehe Folie 103) (meist werden Schlüssel der Länge 128 Bit genutzt)

$$\text{enc} : \underbrace{\{0, 1\}^{128}}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^{128}}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^{128}}_{\text{Chifftrate}}$$



Blockchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

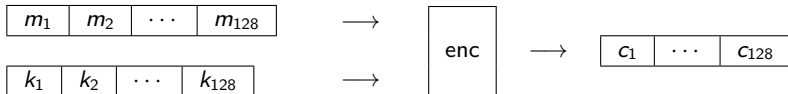
IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren bilden Bitstrings fester Länge auf Bitstrings der selben Länge ab:
 - Moderne Blockchiffren verarbeiten Bitstrings der Länge 128 (Klartextblock) (diese Länge heißt auch Blockgröße der Blockchiffre)
 - Genutzte Schlüssel müssen eine Bitlänge ≥ 100 haben (siehe Folie 103) (meist werden Schlüssel der Länge 128 Bit genutzt)

$$\text{enc} : \underbrace{\{0, 1\}^{128}}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^{128}}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^{128}}_{\text{Chifftrate}}$$



- Für längere Klartexte werden sogenannte Betriebsarten genutzt (siehe Folie 139)

Blockchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir behandeln zunächst nur die einzelne Blockchiffre

$$\text{enc} : \underbrace{\{0, 1\}^{128}}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^{128}}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^{128}}_{\text{Chifftrate}}$$

Es gibt zwei etablierte Konstruktionsmethoden

- Feistel-Chiffren:
 - Entwickelt von Horst Feistel in den 1970er Jahren im IBM-Projekt Lucifer
 - Prominentes Beispiel: Data Encryption Standard (DES)
- Substitutions-Permutations-Netzwerk (SPN)
 - Grundidee geht auf Claude Shannon aus dem Jahr 1949 zurück
 - Prominentes Beispiel: Advanced Encryption Standard (AES), Nachfolger von DES

Blockchiffren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beide Konstruktionsmethoden nutzen die selben Ideen:

- Diffusion:
 - Verteilung der Informationen des Klartextes über den gesamten Chiffretext
 - Jedes Bit des Chiffretext hängt von jedem Bit des Klartext ab
 - Bei Änderung eines Klartextbits ändern sich ca. 50 % der Geheimtextbits
 - Realisiert durch Permutationen (spezielle lineare Abbildungen)
- Konfusion
 - Zusammenhang zwischen Klartext und Chiffretext soll hochgradig komplex sein
Gleiches gilt für den Zusammenhang zwischen Schlüssel und Chiffretext
 - Realisiert durch Substitutionen (nicht-lineare Abbildungen)
- Rundenbasiert: Wiederholte Anwendung von Diffusion, Konfusion und Schlüssel

Permutationen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

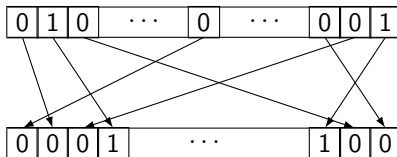
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

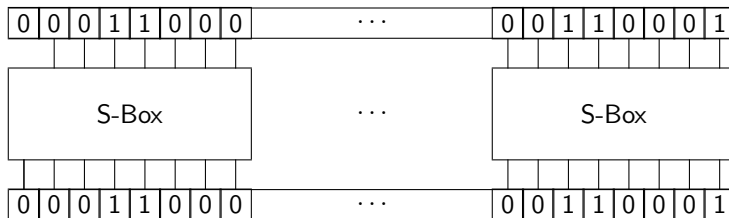
IT-Forensik

Sichere
Software-
entwicklung



- Reihenfolge der Bits werden über den gesamten Block (128 Bit) vertauscht
- Effekt der Diffusion ergibt sich erst nach mehreren Runden

Substitutionen



- S-Boxen sind nicht-lineare Abbildungen $\{0, 1\}^n \rightarrow \{0, 1\}^n$
- Werden üblicherweise nur auf Bitstrings der Länge 8 oder 16 angewandt
- Damit effizient zu implementieren über Arrays der Länge 2^8 oder 2^{16} (Arrays der Länge 2^{128} sind nicht speicherbar)

Substitutions-Permutations-Netzwerk: Beispiel AES

Klartextblock (128 Bit)

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Substitutions-Permutations-Netzwerk: Beispiel AES

Klartextblock (128 Bit)

1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$
 n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Substitutions-Permutations-Netzwerk: Beispiel AES

Klartextblock (128 Bit)

- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

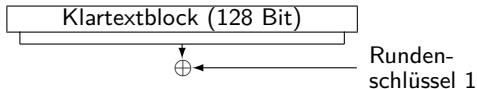
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

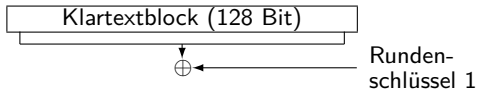
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$
 n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet

2) In Runde 1 wird r_1 auf den Klartext addiert

3) In Runde 2 werden zunächst Substitution und
Permutation angewandt und danach r_2 addiert

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

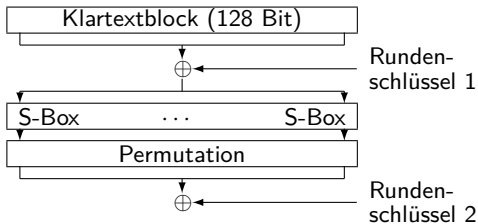
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$
 n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet

2) In Runde 1 wird r_1 auf den Klartext addiert

3) In Runde 2 werden zunächst Substitution und
Permutation angewandt und danach r_2 addiert

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

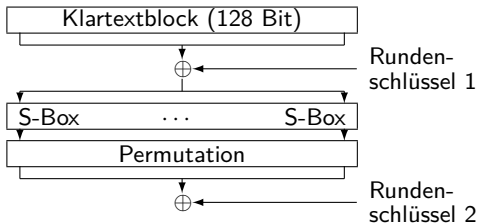
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert
- 3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert
- 4) Runden 3 bis n laufen genauso

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

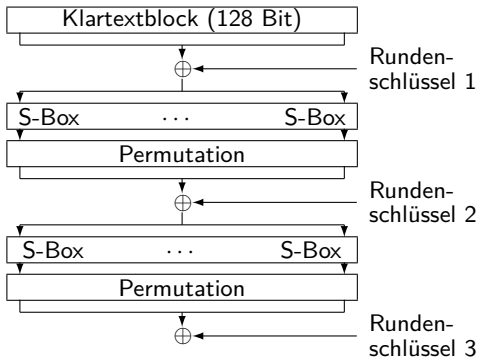
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert
- 3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert
- 4) Runden 3 bis n laufen genauso

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

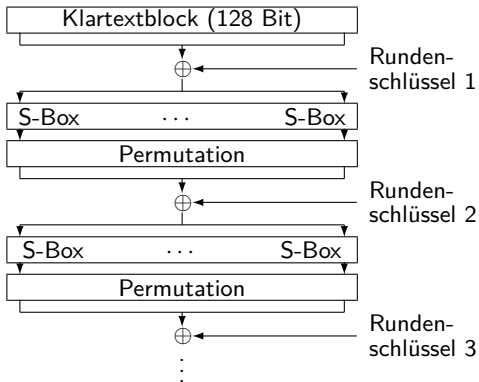
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert
- 3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert
- 4) Runden 3 bis n laufen genauso

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

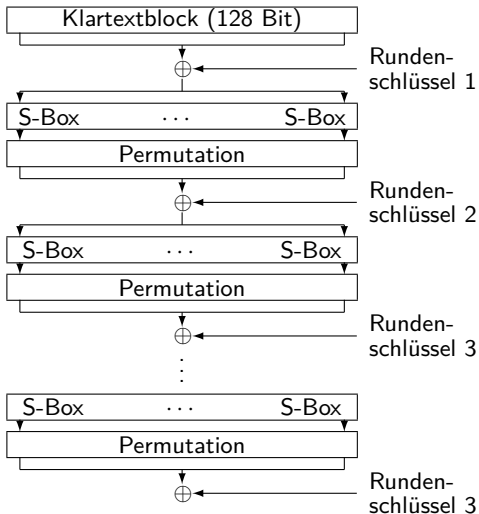
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



- 1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundenschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet
- 2) In Runde 1 wird r_1 auf den Klartext addiert
- 3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert
- 4) Runden 3 bis n laufen genauso

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

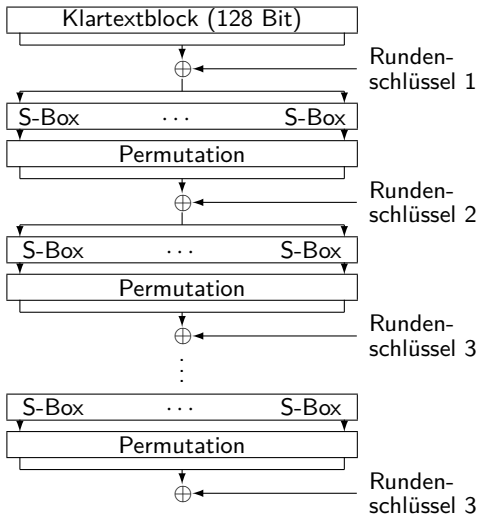
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet

2) In Runde 1 wird r_1 auf den Klartext addiert

3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert

4) Runden 3 bis n laufen genauso

5) Nach Runde n erhalten wir den Chiffretext

Substitutions-Permutations-Netzwerk: Beispiel AES

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

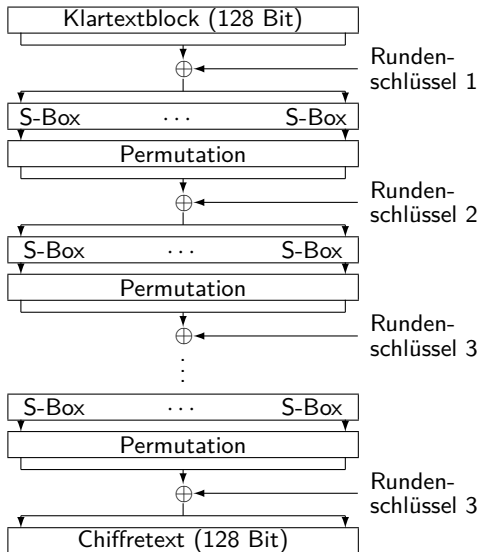
Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung



1) Zunächst werden aus dem Schlüssel $k \in \{0, 1\}^{128}$ n Rundschlüssel $r_1, \dots, r_n \in \{0, 1\}^{128}$ abgeleitet

2) In Runde 1 wird r_1 auf den Klartext addiert

3) In Runde 2 werden zunächst Substitution und Permutation angewandt und danach r_2 addiert

4) Runden 3 bis n laufen genauso

5) Nach Runde n erhalten wir den Chiffretext

SPN: Sicherheitsdiskussion

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beide Grundbausteine (Permutation, Substitution) werden benötigt:

- Lassen wir Substitutionen weg, dann ist die Blockchiffre eine lineare Abbildung
 - Angreifer will aus Ciphertexten c_1, \dots, c_n Klartexte m_1, \dots, m_n bestimmen
 - Es gilt

$$c_1 = \text{enc}(k, m_1), c_2 = \text{enc}(k, m_2), \dots, c_n = \text{enc}(k, m_n) \quad (2)$$

mit Unbekannten k, m_1, \dots, m_n

- Ist enc eine lineare Abbildung, so ist (2) ein lineares Gleichungssystem (Lineare Gleichungssysteme sind effizient lösbar)

SPN: Sicherheitsdiskussion

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beide Grundbausteine (Permutation, Substitution) werden benötigt:

- Lassen wir Permutationen weg, dann gilt:
 - Bit 1 – 16 des Geheimtextes hängen nur von Bit 1 – 16 des Klartextblocks ab
 - Bit 17 – 32 des Geheimtextes hängen nur von Bit 17 – 32 der Klartextblocks ab
 - usw.
- Damit sind statistische Angriffe möglich
(vgl. Sicherheitsbetrachtung monoalphabetischer Verfahren, Folie 63)

Betriebsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren verschlüsseln zunächst nur Klartexte einer bestimmten Blockgröße

$$\text{enc} : \underbrace{\{0, 1\}^I}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^n}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^n}_{\text{Chiffrate}}$$

(Schlüssellänge $I \geq 100$, Blockgröße heute meist $n = 128$)

Betriebsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren verschlüsseln zunächst nur Klartexte einer bestimmten Blockgröße

$$\text{enc} : \underbrace{\{0, 1\}^I}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^n}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^n}_{\text{Chiffrate}}$$

(Schlüssellänge $I \geq 100$, Blockgröße heute meist $n = 128$)

- Für die Verschlüsselung längerer Klartexte zerlegen wir den Klartext in Blöcke:

Betriebsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren verschlüsseln zunächst nur Klartexte einer bestimmten Blockgröße

$$\text{enc} : \underbrace{\{0, 1\}^I}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^n}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^n}_{\text{Chifftrate}}$$

(Schlüssellänge $I \geq 100$, Blockgröße heute meist $n = 128$)

- Für die Verschlüsselung längerer Klartexte zerlegen wir den Klartext in Blöcke:

011000..... 1011110
Block 1 (128 Bit) Block 2 (128 Bit)

Betriebsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Blockchiffren verschlüsseln zunächst nur Klartexte einer bestimmten Blockgröße

$$\text{enc} : \underbrace{\{0, 1\}^I}_{\text{Schlüssel}} \times \underbrace{\{0, 1\}^n}_{\text{Klartexte}} \longrightarrow \underbrace{\{0, 1\}^n}_{\text{Chifftrate}}$$

(Schlüssellänge $I \geq 100$, Blockgröße heute meist $n = 128$)

- Für die Verschlüsselung längerer Klartexte zerlegen wir den Klartext in Blöcke:

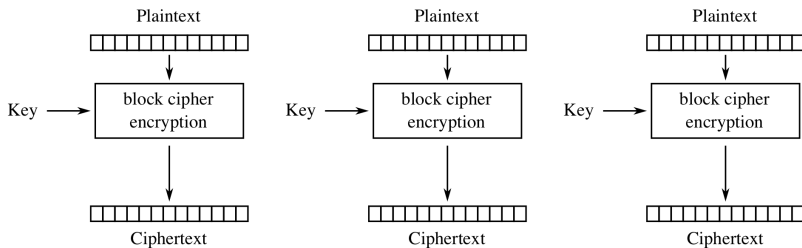
$$\underbrace{011000 \dots \dots \dots}_{\text{Block 1 (128 Bit)}} \underbrace{\dots \dots \dots}_{\text{Block 2 (128 Bit)}} \dots \dots \dots \underbrace{1011110 \text{ PADDING}}_{\text{Block s (128 Bit)}}$$

- Sollte der letzte Block nicht die Länge 128 haben, füllen wir entsprechend auf

Betriebsart: Electronic Code Book (ECB)

Einfachste Betriebsart

- Der Klartext wird, wie auf Folie 139 erläutert, in Blöcke der benötigten Blocklänge zerlegt und Block für Block verschlüsselt

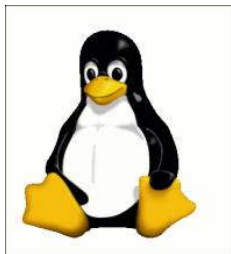


Electronic Codebook (ECB) mode encryption

Betriebsart: ECB

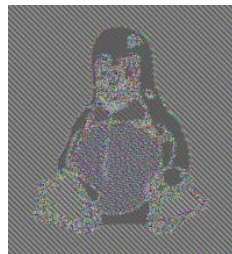
Probleme der Betriebsart ECB

- Gleiche Klartextblöcke werden zu gleichen Chiffretexten verschlüsselt
- Ein Angreifer kann so die Struktur des Klartextes erkennen



Klartext

AES im ECB Mode



Chiffretext

Betriebsarten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

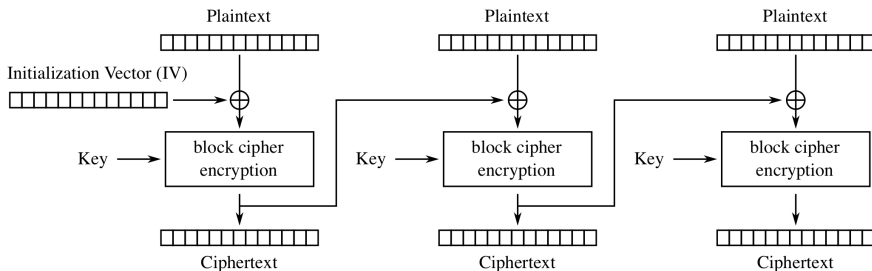
ECB ist nicht sicher

- Lösung:
 - Der Chiffretext sollte nicht nur von Schlüssel und Klartext abhängen,
 - sondern von einem weiteren Parameter
- Wir lernen zwei solcher Betriebsarten näher kennen
 - Cipher Block Chaining Mode (CBC)
 - Counter Mode (Ctr)
- Weitere bekannte Betriebsarten sind:
 - Cipher Feedback Mode (CFB)
 - Output Feedback Mode (OFB)

Betriebsart: Cipher Block Chaining

Weiterer Parameter: Vorheriger Chiffretext

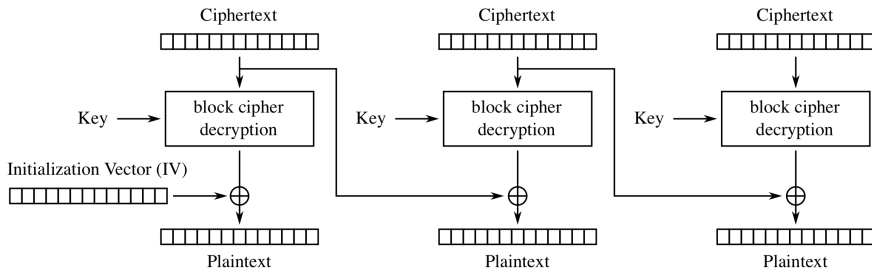
- Der i -te Klartext (Plaintext) m_i wird mit dem vorhergehenden Ciphertext c_{i-1} addiert und anschließend verschlüsselt: $c_i = \text{enc}(k, m_i \oplus c_{i-1})$
- Für den ersten Block wird ein Initialisierungsvektor benötigt



Cipher Block Chaining (CBC) mode encryption

Betriebsart: Cipher Block Chaining

- Für die Entschlüsselung wird der i -te Ciphertext c_i entschlüsselt und dann mit dem $(i - 1)$ -ten Ciphertext c_{i-1} addiert: $m_i = \text{dec}(k, c_i) \oplus c_{i-1}$
- Wegen $c_i = \text{enc}(k, m_i \oplus c_{i-1})$ erhalten wir tatsächlich den Klartext m_i

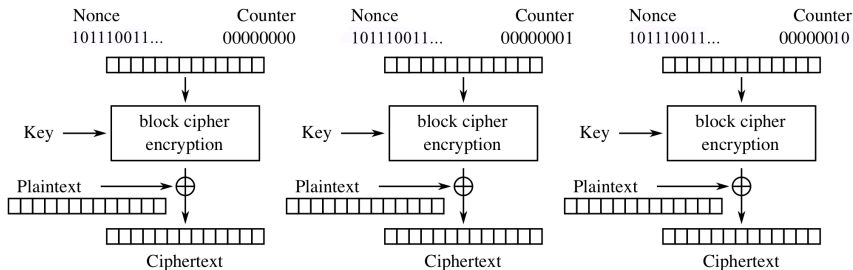


Cipher Block Chaining (CBC) mode decryption

Betriebsart: Counter Mode

Weiterer Parameter: Zähler (Counter)

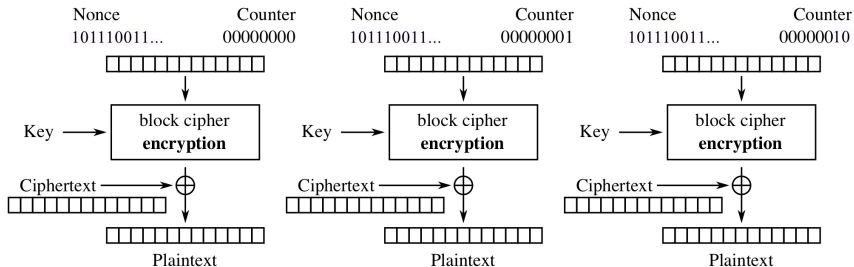
- Erzeuge Werte bestehend aus Nonce (Number Only Used Once) und Zähler
- Daraus wird ein Schlüsselstrom erzeugt und mit dem Klartext addiert (Die Blockchiffre wird also als Pseudozufallszahlengenerator genutzt)



Counter (CTR) mode encryption

Betriebsart: Counter Mode

- Wie bei Stromchiffren üblich, erhalten wir Klartext zurück, indem wir den Schlüsselstrom auf den Ciphertext addieren (Schlüsselstrom \oplus Schlüsselstrom = (0, 0, 0, ...))



Counter (CTR) mode decryption

Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Der Counter Mode nutzt die Blockchiffre als Pseudozufallszahlengenerator wie folgt:



Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

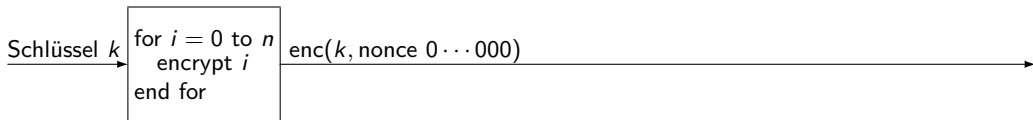
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Der Counter Mode nutzt die Blockchiffre als Pseudozufallszahlengenerator wie folgt:



Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

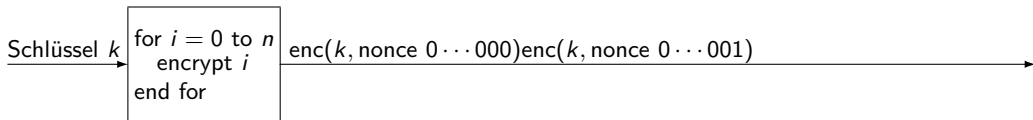
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Der Counter Mode nutzt die Blockchiffre als Pseudozufallszahlengenerator wie folgt:



Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

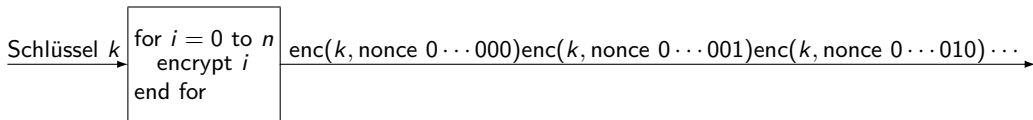
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Der Counter Mode nutzt die Blockchiffre als Pseudozufallszahlengenerator wie folgt:



Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

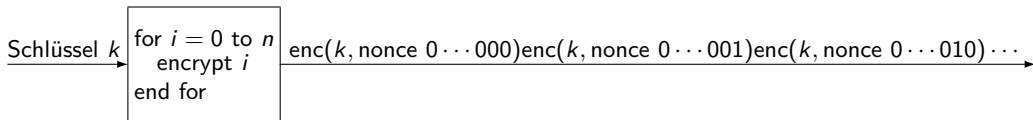
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Der Counter Mode nutzt die Blockchiffre als Pseudozufallszahlengenerator wie folgt:



- Auf Folie 107 haben wir zwei Bedingungen für die Sicherheit formuliert:
 - Aus Teilen des Schlüsselstroms dürfen keine Nachfolger bestimmt werden können
 - Aus Teilen des Schlüsselstroms dürfen keine Vorgänger bestimmt werden können
- Wenn die Blockchiffre sicher ist (aus bekanntem Chiffertext kann der Schlüssel nicht berechnet werden), dann sind diese beiden Bedingungen erfüllt (Hausaufgabe!)

Sicherheit Counter Mode

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

NONCE: Number Only Used Once

- Die Nonce darf bei gleichem Schlüssel nicht mehrfach verwendet werden
 - Ansonsten wird der selbe Schlüsselstrom generiert und der Angreifer kann erkennen, ob die selben Klartexte verschlüsselt wurden
- Die Nonce muss nicht geheim gehalten werden
Sicherheit liegt allein an der Geheimhaltung des Schlüssels

ECB versus CBC und CTR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

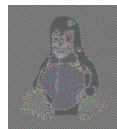
Sichere
Software-
entwicklung

- ECB: Ciphertext lässt Struktur des Klartextes erkennen (Folie 144):



Klartext

ECB Mode



Chiffretext

ECB versus CBC und CTR

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

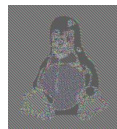
Sichere
Software-
entwicklung

- ECB: Ciphertext lässt Struktur des Klartextes erkennen (Folie 144):



Klartext

ECB Mode



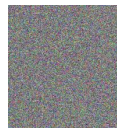
Chiffretext

- Nutzung zusätzlicher Parameter (vorheriger Ciphertext (CBC), Zähler (CTR)):



Klartext

CBC, CTR



Chiffretext

Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel: Integritätsschutz (erkennen, ob Daten verändert wurden)

Hashfunktionen bilden Bitstrings beliebiger Länge auf Bitstrings festen Länge ab

- Hashfunktion: $H : \{0, 1\}^* \longrightarrow \{0, 1\}^l$
- Menge der Bitstrings beliebiger Länge: $\{0, 1\}^*$ (Definitionsbereich von H)
- Menge der Bitstrings der Länge $n \in \mathbb{N}$: $\{0, 1\}^l$ (Bildbereich von H)

Wie bei Verschlüsselungsverfahren werden häufig große Datenmengen verarbeitet

- Die Berechnung muss effizient sein, d.h.
für gegebenes $m \in \{0, 1\}^*$ muss $H(m)$ schnell berechnet werden können

Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Hashfunktionen werden für viele kryptographische Verfahren benötigt:

- Integritätsschutz,
- Daten- und Instanzauthentisierung
- elektronische Signatur
- Pseudozufallszahlengeneratoren

Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Definition kryptographische Hashfunktion

Wir nennen eine Hashfunktion $H : \{0, 1\}^* \longrightarrow \{0, 1\}^l$ **kryptographisch stark**, wenn sie die folgenden zwei Bedingungen erfüllt:

Preimage resistance: Für gegebenes $h \in \{0, 1\}^l$ ist es praktisch nicht möglich einen Wert $m \in \{0, 1\}^*$ mit $H(m) = h$ zu finden.

Collision resistance: Es ist praktisch nicht möglich zwei Werte $m, m' \in \{0, 1\}^*$ so zu finden, dass $m \neq m'$ und $H(m) = H(m')$ gilt.

Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Preimage resistance: Für gegebenes $h \in \{0,1\}^l$ ist es praktisch nicht möglich einen Wert $m \in \{0,1\}^*$ mit $H(m) = h$ zu finden.

Collision resistance: Es ist praktisch nicht möglich zwei Werte $m, m' \in \{0,1\}^*$ so zu finden, dass $m \neq m'$ und $H(m) = H(m')$ gilt.

Praktisch unmöglich:

- Bei einem geforderten Sicherheitsniveau von 100 Bit:
Ein Angreifer benötigt ca. 2^{100} Versuche
 - einen Wert m mit $H(m) = h$ zu finden, oder
 - zwei Werte $m' \neq m$ mit $H(m) = H(m')$ zu finden

Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Preimage resistance: Für gegebenes $h \in \{0, 1\}^l$ ist es praktisch nicht möglich einen Wert $m \in \{0, 1\}^*$ mit $H(m) = h$ zu finden.

H soll effizient berechenbar sein, die Umkehrabbildung

(finde zu $h \in \{0, 1\}^l$ Urbild $m \in \{0, 1\}^*$ mit $H(m) = h$)

aber praktisch nicht berechenbar sein

Wir nennen solche Abbildungen auch Einwegfunktionen

Sicherheit von Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Collision resistance: Es ist praktisch nicht möglich zwei Werte $m, m' \in \{0,1\}^*$ so zu finden, dass $m \neq m'$ und $H(m) = H(m')$ gilt.

Zwei Werte $m, m' \in \{0,1\}^*$ mit $H(m) = H(m')$ nennen wir eine Kollision von H

Sicherheit von Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

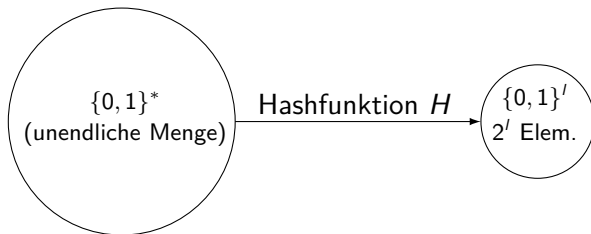
IT-Forensik

Sichere
Software-
entwicklung

Collision resistance: Es ist praktisch nicht möglich zwei Werte $m, m' \in \{0, 1\}^*$ so zu finden, dass $m \neq m'$ und $H(m) = H(m')$ gilt.

Zwei Werte $m, m' \in \{0, 1\}^*$ mit $H(m) = H(m')$ nennen wir eine Kollision von H

- Kollisionen lassen sich nicht vermeiden:
 - H bildet $\{0, 1\}^*$ (unendliche Menge) auf $\{0, 1\}^l$ (endliche Menge, 2^l Elemente) ab
 - Damit muss es (sogar unendlich viele) Kollisionen geben



Sicherheit von Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Zwei Werte $m, m' \in \{0, 1\}^*$ mit $H(m) = H(m')$ nennen wir eine Kollision von H

- Möglicher Angriff (Brute Force):
 - Wähle n zufällige Werte $m_1, \dots, m_n \in \{0, 1\}^*$
 - Prüfe, ob darunter zwei Werte sind, die eine Kollision von H bilden
- Praktisch nicht möglich (d.h. Sicherheitsniveau ≥ 100 Bit) bedeutet:
 - Ein Angreifer benötigt $\geq 2^{100}$ Versuche, bis er eine Kollision gefunden hat (mit hoher Wahrscheinlichkeit)
 - d.h. muss mindestens 2^{100} Werte $m_1, \dots, m_{2^{100}}$ wählen
- Um diesen Angriff auszuschließen, muss der Bildbereich von H groß sein
 - Mindestens 2^{200} Elemente, d.h. $H : \{0, 1\}^* \rightarrow \{0, 1\}^I$ mit $I \geq 200$ (Beweis in der Vorlesung Kryptologie)

Konstruktion von Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

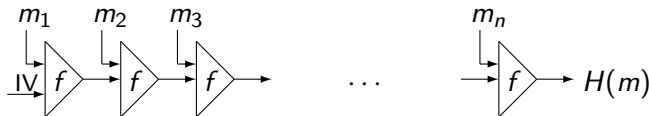
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Merkle-Damgard-Konstruktion:



- Nutze eine Kompressionsfunktion $f : \{0, 1\}^l \times \{0, 1\}^l \rightarrow \{0, 1\}^l$
Diese muss sowohl eine Einwegfunktion, als auch kollisionsresistent sein
- Die Nachricht m wird in Blöcke m_1, \dots, m_n der Länge l aufgeteilt
- Jeder Block wird zusammen mit dem vorherigen Ergebnis mittels f verarbeitet
- Für den ersten Schritt wird ein Initialisierungsvektor (IV) benötigt

Konstruktion von Hashfunktionen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beispiel für sichere Kompressionsfunktionen:

- Basierend auf einer Blockchiffre enc :
 - Im ersten Schritt: $f_1 := f(\text{IV}, m_1) = \text{enc}(\text{IV}, m_1) \oplus m_1$
 - Im zweiten Schritt: $f_2 := f(f_1, m_2) = \text{enc}(f_1, m_2) \oplus m_2$
 - ...
 - Im letzten Schritt: $H(m) = f_n := f(f_{n-1}, m_n) = \text{enc}(f_{n-1}, m_n) \oplus m_n$

Hashfunktionen und Integritätsschutz

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel von Hashfunktionen: Integritätsschutz

- Speichern von Nachricht m und Hashwert $H(m)$ (auf verschiedenen Systemen)
- Prüfung, ob Nachricht m verändert wurde: Berechne Hashwert und vergleiche
- Hierfür wichtig: Kollisionsresistenz
Ein Angreifer darf keine zweite Nachricht mit dem selben Hashwert erzeugen

Einsatzbeispiele:

- Download von Software, z.B. OpenOffice von der Seite
<http://www.openoffice.org/de/downloads/index.html>
 - SHA256-Hashwert für Apache_OpenOffice_4.1.1_MacOS_x86-64_install_de.dmg:
b905925d0d5bfb22e65910031cc1a17efce29498c4408a9deb368825ae8b236c

Hashfunktionen und Integritätsschutz

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Es lässt sich aber nicht feststellen, wer die Nachricht erzeugt hat

- Hashfunktionen sind öffentlich
- Es wird kein kryptographischer Schlüssel verwendet

Hashfunktionen erfüllen also nicht das Schutzziel Datenauthentizität

Message Authentication Codes (MAC)

Schutzziel: Datenauthentizität

(B kann zweifelsfrei feststellen, dass die Nachricht von A stammt)

A Schlüssel: k

compute Prüfsumme $t := \text{mac}(k, m)$

$\xrightarrow{m, t}$

B Schlüssel: k

compute $t' := \text{mac}(k, m)$

if $t' = t$ then accept

else reject

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Message Authentication Codes (MAC)

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schutzziel: Datenauthentizität

- Nur die Inhaber des Schlüssels k können korrekte Prüfsummen berechnen
- Erfüllen also das Schutzziel Datenauthentizität (wenn nur A und B den Schlüssel kennen)
- Erfüllen nicht das Schutzziel Nichtabstreitbarkeit
 - Beide kennen Schlüssel k , also können auch beide Prüfsumme berechnen
 - Gegenüber Dritten (z.B. einem Richter) kann B also nicht beweisen, dass nicht er, sondern A die Prüfsumme berechnet hat
 - Hierfür benötigen wir Signaturen (asymmetrische Verfahren), siehe Folie 202

Message Authentication Codes (MAC)

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wie schon Verschlüsselungsverfahren und Hashfunktionen, müssen auch MAC-Verfahren zum Teil sehr große Datenmengen effizient verarbeiten können. Heutige Verfahren basieren auf

- Blockchiffren (z.B. CBC-MAC, XOR-MAC)
- Kryptographisch starken Hashfunktionen (z.B. HMAC)

CBC-MAC

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Cipher Block Chaining Message Authentication Code (CBC-MAC)

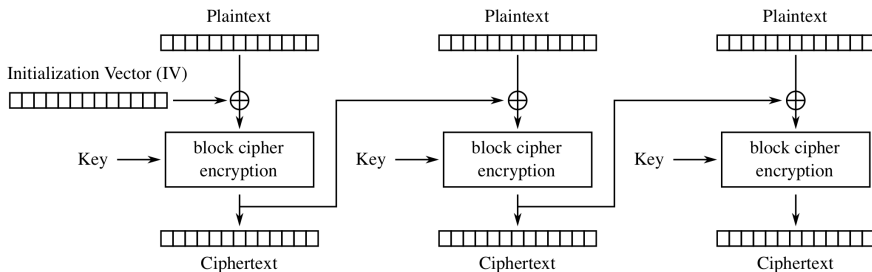
- Basiert auf einer sicheren Blockchiffre
- Nachricht m wird zunächst in Blöcke m_1, \dots, m_n zerlegt

CBC-MAC

Cipher Block Chaining Message Authentication Code (CBC-MAC)

- Basiert auf einer sicheren Blockchiffre
- Nachricht m wird zunächst in Blöcke m_1, \dots, m_n zerlegt

Erinnerung Betriebsmode Cipher Block Chaining (CBC):



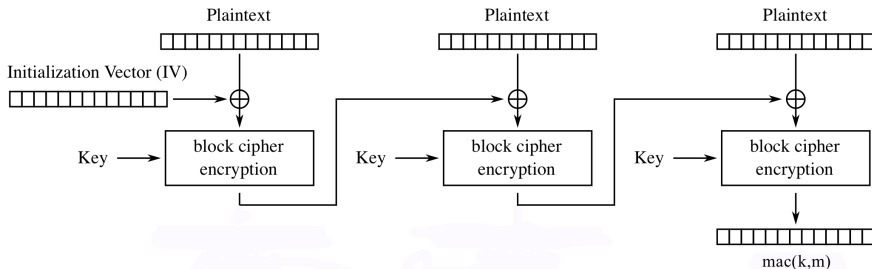
Cipher Block Chaining (CBC) mode encryption

CBC-MAC

Cipher Block Chaining Message Authentication Code (CBC-MAC)

- Basiert auf einer sicheren Blockchiffre
- Nachricht m wird zunächst in Blöcke m_1, \dots, m_n zerlegt

Prüfsumme ist der letzte Ciphertext



Cipher Block Chaining Message Authentication Code (CBC-MAC)

HMAC

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

MAC-Verfahren basierend auf Hashfunktionen $H : \{0, 1\}^* \longrightarrow \{0, 1\}^l$

$$\text{HMAC}(k, m) := H((k \oplus \text{opad}) || H((k \oplus \text{ipad}) || m))$$

Dabei sind

- $\text{opad} := 0x5C \cdots 0x5C$
- $\text{ipad} := 0x36 \cdots 0x36$

Konstanten (die Sicherheit hängt nicht von der konkreten Wahl der Konstanten ab)

Secure Messaging

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel: Sicherer Kanal zwischen Alice und Bob (vertraulich und authentisch)

- Mehrere Umsetzungen denkbar:
 - 1) Verschlüsseln des Klartextes und MAC über den Geheimtext (z.B. bei IPsec)
 - 2) MAC über den Klartext und danach Verschlüsseln des Klartextes (z.B. bei SSH)
 - 3) MAC über den Klartext und Verschlüsseln von Klartext und MAC (z.B. bei SSL)
- Nur Umsetzung 1) ist sicher

Secure Messaging

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Erst Klartext verschlüsseln, dann MAC über den Geheimtext

- Vertraulichkeit ist ein anderes Schutzziel als Datenauthentizität: MAC-Verfahren müssen nicht die Vertraulichkeit garantieren
- Weiterverarbeitung von Daten nur, wenn Sender bekannt ist: Verhindert z.B. Entschlüsselung von Schadsoftware

Weitere Bedingung:

- Für Verschlüsselung und MAC sollten verschiedene Schlüssel genutzt werden
 - Wesentliches kryptographisches Grundprinzip: Trenne wo du trennen kannst
 - Wird der Schlüssel für ein Verfahren kompromittiert, ist nicht automatisch das zweite Verfahren betroffen

Instanzenauthentisierung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

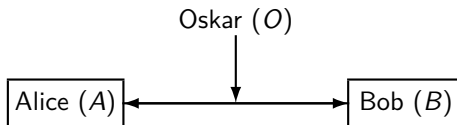
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schutzziel Instanzenauthentisierung: B kann die Identität von A zweifelsfrei feststellen



Verfahren zur Instanzenauthentisierung sind:

- Nachweis eines Geheimnisses (z.B. Benutzername/Passwort)
- Nachweis von Eigenschaften (z.B. biometrische Merkmale wie Fingerabdruck)
- Nachweis eines Geheimnisses, ohne dieses offen legen zu müssen (Challenge-Response Verfahren, siehe nächste Folie)

Wir widmen diesem Aspekt ein eigenes Kapitel (ab Folie 249)

Challenge-Response Verfahren (symmetrisch)

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel: Nachweis eines Geheimnisses (hier Schlüssel k), ohne dieses offen zu legen
Als Basis dienen Message Authentication Codes:

A Schlüssel: k

B Schlüssel: k

choose random c
(challenge)

\xrightarrow{c}

compute $r := \text{mac}(k, c)$
(response)

\xleftarrow{r}

compute $r' := \text{mac}(k, c)$
if $r' = r$ then accept
else reject

Challenge-Response Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel: Nachweis eines Geheimnisses (hier Schlüssel k), ohne dieses offen zu legen

- Nur die Inhaber des Schlüssels k können
 - aus der Challenge c
 - eine korrekte Response rberechnen
- Erfüllen also das Schutzziel Instanzenauthenzität (wenn nur A und B den Schlüssel kennen)

Asymmetrische Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Bei symmetrischen Verfahren wird immer der selbe Schlüssel genutzt

- Schlüssel zum Ver- und Entschlüsseln sind gleich
- Schlüssel für Berechnung und Verifikation von Prüfsummen sind gleich
- Schlüssel zur Berechnung und Verifikation der Response sind gleich

Bei asymmetrischen Verfahren gibt es ein Schlüsselpaar (pk , sk)

pk : Public Key (ist öffentlich), sk : Secret Key (ist geheim)

- Verschlüsselung mit pk : jeder kann verschlüsseln
Entschlüsselung mit sk : nur Inhaber des geheimen Schlüssels kann entschlüsseln
- Berechnung der Prüfsumme mit sk : nur Inhaber von sk kann berechnen
Verifikation der Prüfsumme mit pk : jeder kann prüfen

Asymmetrische Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundidee asymmetrischer Verfahren: Einwegfunktionen mit Falltür

- Einwegfunktion f (Begriff im Abschnitt Hashfunktionen kennen gelernt):
 - f ist effizient berechenbar
 - Umkehrfunktion von f ist praktisch nicht berechenbar
- Falltür:
 - Mit zusätzlichem Wissen lässt sich auch die Umkehrfunktion effizient berechnen

Kandidaten sind:

- Faktorisierungsproblem großer natürlicher Zahlen
Multiplikation ist deutlich einfacher als Faktorisieren
- Das diskrete Logarithmusproblem
Potenzieren ist deutlich einfacher als Logarithmus

Asymmetrische Verschlüsselung: RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

RSA-Verfahren

- publiziert 1977
- benannt nach Rivest, Shamir und Adleman
- gilt als das erste bekannte asymmetrische Verfahren

Sicherheit beruht auf der vermuteten Schwierigkeit des Faktorisierens großer Zahlen

Faktorisierungsproblem:

Gegeben: Zusammengesetzte natürliche Zahl $n = p \cdot q \in \mathbb{N}$, p, q Primzahlen.

Lösung: Finde die beiden Primfaktoren p und q .

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Für das RSA-Verfahren benötigen wir einige mathematische Grundlagen

- Die Menge \mathbb{Z}_n besteht aus allen natürlichen Zahlen $< n$
 $\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$
- Wir rechnen in dieser Menge wie folgt:
 - Für eine natürliche Zahl $t \in \mathbb{N}$ sei $t \bmod n$ diejenige eindeutige Zahl aus \mathbb{Z}_n , die aus t durch (ev. mehrmaliges) Subtrahieren von n entsteht
 - Beispiele: $6 \bmod 4 = 2$ ($6 - 4 = 2$), $10 \bmod 4 = 2$ ($10 - 2 \cdot 4 = 2$)
 - Für Addition und Multiplikation in \mathbb{Z}_n gilt nun:

$$a + b \quad := \quad a + b \bmod n$$

$$a \cdot b \quad := \quad a \cdot b \bmod n$$

- Beispiel in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$: $2 + 3 \bmod 4 = 5 \bmod 4 = 1$

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Weitere Eigenschaften der Menge \mathbb{Z}_n :

Inverse Elemente bzgl. Addition und Multiplikation in \mathbb{Z}_n

- $a \in \mathbb{Z}_n$ heißt additiv invers (modulo n) zu $b \in \mathbb{Z}_n$, wenn

$$a + b = 0 \bmod n$$

- $a \in \mathbb{Z}_n$ heißt multiplikativ invers (modulo n) zu $b \in \mathbb{Z}_n$, wenn

$$a \cdot b = 1 \bmod n$$

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Weitere Eigenschaften der Menge \mathbb{Z}_n :

Inverse Elemente bzgl. Addition und Multiplikation in \mathbb{Z}_n

- $a \in \mathbb{Z}_n$ heißt additiv invers (modulo n) zu $b \in \mathbb{Z}_n$, wenn

$$a + b = 0 \bmod n$$

- $a \in \mathbb{Z}_n$ heißt multiplikativ invers (modulo n) zu $b \in \mathbb{Z}_n$, wenn

$$a \cdot b = 1 \bmod n$$

- Beispiele in \mathbb{Z}_4 :

- $3 + 1 = 4 = 0 \bmod 4$ (1 ist additiv invers zu 3)
- $3 \cdot 3 = 9 = 1 \bmod 4$ (3 ist multiplikativ invers zu sich selbst)

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Elemente in \mathbb{Z}_n haben Inverse?

- Bzgl. Addition alle Elemente: für alle $a \in \mathbb{Z}_n$ gilt mit $b = n - a$:

$$a + b = a + (n - a) = n = 0 \bmod n$$

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Elemente in \mathbb{Z}_n haben Inverse?

- Bzgl. Addition alle Elemente: für alle $a \in \mathbb{Z}_n$ gilt mit $b = n - a$:

$$a + b = a + (n - a) = n = 0 \bmod n$$

- Bzgl. Multiplikation nicht alle Elemente: z.B. in \mathbb{Z}_4
 - 1 ist zu sich selbst invers ($1 \cdot 1 = 1$)
 - 3 ist zu sich selbst invers (hatten wir schon)
 - zu 2 gibt es kein inverses Element
($2 \cdot 1 = 2 \neq 1$, $2 \cdot 2 = 4 = 0 \bmod 4 \neq 1$, $2 \cdot 3 = 6 = 2 \bmod 4 \neq 1$)

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Elemente in \mathbb{Z}_n haben multiplikativ Inverse?

- Für $a \in \mathbb{N}$ heißt $t \in \mathbb{N}$ *Teiler* von a (in Zeichen $t|a$), wenn $\frac{a}{t} \in \mathbb{N}$
1, 2, 3, 4, 6 sind Teiler von 12
- $t \in \mathbb{N}$ heißt *gemeinsamer Teiler* von $a, b \in \mathbb{N}$, wenn $t|a$ und $t|b$
1, 2, 4 sind gemeinsame Teiler von 12 und 20
- $a, b \in \mathbb{N}$ heißen *teilerfremd*, wenn 1 einziger gemeinsamer Teiler von a und b ist
8 und 15 sind teilerfremd

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Elemente in \mathbb{Z}_n haben multiplikativ Inverse?

- Für $a \in \mathbb{N}$ heißt $t \in \mathbb{N}$ *Teiler* von a (in Zeichen $t|a$), wenn $\frac{a}{t} \in \mathbb{N}$
1, 2, 3, 4, 6 sind Teiler von 12
- $t \in \mathbb{N}$ heißt *gemeinsamer Teiler* von $a, b \in \mathbb{N}$, wenn $t|a$ und $t|b$
1, 2, 4 sind gemeinsame Teiler von 12 und 20
- $a, b \in \mathbb{N}$ heißen *teilerfremd*, wenn 1 einziger gemeinsamer Teiler von a und b ist
8 und 15 sind teilerfremd

Ein Element $a \in \mathbb{Z}_n$ besitzt genau dann ein multiplikativ Inverses modulo n , wenn a und n teilerfremd sind

Einschub: Mathematische Grundlagen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Welche Elemente in \mathbb{Z}_n haben multiplikativ Inverse?

- Für $a \in \mathbb{N}$ heißt $t \in \mathbb{N}$ *Teiler* von a (in Zeichen $t|a$), wenn $\frac{a}{t} \in \mathbb{N}$
1, 2, 3, 4, 6 sind Teiler von 12
- $t \in \mathbb{N}$ heißt *gemeinsamer Teiler* von $a, b \in \mathbb{N}$, wenn $t|a$ und $t|b$
1, 2, 4 sind gemeinsame Teiler von 12 und 20
- $a, b \in \mathbb{N}$ heißen *teilerfremd*, wenn 1 einziger gemeinsamer Teiler von a und b ist
8 und 15 sind teilerfremd

Ein Element $a \in \mathbb{Z}_n$ besitzt genau dann ein multiplikativ Inverses modulo n , wenn a und n teilerfremd sind

Vgl. auch Untersuchung von \mathbb{Z}_4 auf Folie 188:

- 1 und 3 teilerfremd zu 4
- 2 ist nicht teilerfremd zu 4

RSA-Verschlüsselungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüsselgenerierung:

- Wähle zwei Primzahlen: p, q . Wir nennen $n = p \cdot q$ das *Modul*
- $\phi(n) = (p - 1) \cdot (q - 1)$ heißt auch *Euler-Zahl* von n
- Verschlüsselungsschlüssel (pk): Wähle e teilerfremd zu $\phi(n)$
- Entschlüsselungsschlüssel (sk): Wähle d so, dass $e \cdot d = 1 \bmod \phi(n)$
(Solch ein d existiert, da e teilerfremd zu $\phi(n)$ ist)

Verschlüsselung einer Nachricht $m \in \mathbb{Z}_n$

- Berechne $c = m^e \bmod n$

Entschlüsselung des Ciphertextes c

- Berechne $c^d \bmod n$

RSA-Verschlüsselungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Verschlüsselung: $c = m^e \bmod n$, Entschlüsselung: $c^d \bmod n$

- Warum gilt $m = c^d \bmod n$
 - Hängt mit der Wahl von e und d zusammen: $e \cdot d = 1 \bmod \phi(n)$
 - Daher gilt (etwas unformal):

$$\begin{aligned}c^d &= (m^e \bmod n)^d \\&= (m^e)^d \bmod n \\&= m^{e \cdot d} \bmod n \\&(\Rightarrow) m^{1 \bmod \phi(n)} \bmod n \\&(\Rightarrow) m^1 \bmod n\end{aligned}$$

- Gleichungen 4 und 5 benötigen einen formalen Beweis (siehe Vorlesung Kryptologie)

RSA Beispiel

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüsselgenerierung:

- Primzahlen: $p = 3, q = 5$
- Modul: $n = p \cdot q = 15$, Eulerzahl: $\phi(n) = (p - 1) \cdot (q - 1) = 8$
- Verschlüsselungsschlüssel: $e = 3$ (ist teilerfremd zu $\phi(n)$)
- Entschlüsselungsschlüssel: $d = 3$ (es gilt $e \cdot d = 9 = 1 \bmod 8$)

Verschlüsselung der Nachricht $m = 7$:

- $c = m^e \bmod n = 7^3 \bmod 15 = 343 \bmod 15 = 13$

Entschlüsselung des Ciphertextes $c = 13$

- $c^d \bmod n = 13^3 \bmod 15 = 2197 \bmod 15 = 7$.

Sicherheit RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Angreifer kennt
 - den öffentlichen Verschlüsselungsschlüssel e und
 - das Modul n (also die Menge \mathbb{Z}_n , in der gerechnet wird)
- Ziel des Angreifers: Bestimme den Klartext m zum Ciphertext $c = m^e \bmod n$
- Einziger Angriff heute: Bestimme den geheimen Entschlüsselungsschlüssel d
 - Zusammenhang zwischen e und d : es gilt $e \cdot d = 1 \bmod \phi(n)$
Erinnerung: Für $n = p \cdot q$, p, q Primzahlen, gilt $\phi(n) = (p - 1) \cdot (q - 1)$
- Aber: Der Angreifer kennt $\phi(n)$ nicht, kann also d nicht aus e berechnen
- Um $\phi(n)$ zu bestimmen, kann er versuchen, p, q zu berechnen (n faktorisieren)

Faktorisierungsproblem:

Gegeben: Zusammengesetzte natürliche Zahl $n = p \cdot q \in \mathbb{N}$, p, q Primzahlen.

Lösung: Finde die beiden Primfaktoren p und q .

- Erste Idee: Probedivision:

Faktorisierungsproblem:

Gegeben: Zusammengesetzte natürliche Zahl $n = p \cdot q \in \mathbb{N}$, p, q Primzahlen.

Lösung: Finde die beiden Primfaktoren p und q .

- Erste Idee: Probedivision:

- for $i = 1$ to \sqrt{n}
- if $n/i \in \mathbb{N}$ stopp
- return $i, n/i$

Faktorisierungsproblem:

Gegeben: Zusammengesetzte natürliche Zahl $n = p \cdot q \in \mathbb{N}$, p, q Primzahlen.

Lösung: Finde die beiden Primfaktoren p und q .

- Erste Idee: Probedivision:
 - for $i = 1$ to \sqrt{n}
 - if $n/i \in \mathbb{N}$ stopp
 - return $i, n/i$
- Aber: Es gibt bessere Algorithmen zum Faktorisieren:
 - Für Sicherheitsniveau 100 Bit werden Primzahlen der Größe ca. 2^{1000} benötigt
 - Nachweis in der Vorlesung Kryptologie

Asymmetrische Verschlüsselungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Weitere bekannte Verfahren

- Rabin-Verfahren (basiert auch auf Schwierigkeit des Faktorisierungsproblems)
- ElGamal-Verfahren (basiert auf Schwierigkeit des Logarithmusproblems)
- Merkle-Hellman und McEliece (basieren auf Schwierigkeit anderer Probleme)

Nachteil von asymmetrischen Verschlüsselungsverfahren:

- Sind deutlich ineffizienter als symmetrische Verschlüsselungsverfahren
- Verwendung daher in der Praxis nur für den Austausch symmetrischer Schlüssel

Hybridverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Kombination von asymmetrischen (für Schlüsselaustausch) und symmetrischen (für die eigentliche Verschlüsselung) Verschlüsselungsverfahren

- A will B eine vertrauliche Nachricht m übermitteln
- B besitzt ein Schlüsselpaar (pk, sk) (z.B. für das RSA-Verfahren)
- A vertraut dem öffentlichen Schlüssel pk (weiß, dass dieser B gehört)

A öffentlicher Schlüssel: $pk = e$

B geheimer Schlüssel: $sk = d$

choose random key k
compute $k' = k^e \bmod n$

and $c = \text{enc}(k, m)$

$\xrightarrow{k', c}$ compute $k = k'^d \bmod n$
and $m = \text{dec}(k, c)$

Signaturverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schutzziel: Nichtabstreitbarkeit

(B kann auch gegenüber Dritten nachweisen, dass die Nachricht von A stammt)

A geheimer Schlüssel: sk

B öffentlicher Schlüssel: pk

compute Signatur $s := \text{sig}(sk, m) \xrightarrow{m, s}$

compute $b := \text{verify}(pk, m, s)$
if $b = \text{true}$ then accept
else reject

Wir benötigen Verfahren:

- sig : Signieren von Nachrichten m mit einem geheimen Schlüssel sk
- verify : Prüfen von Signaturen mit dem zugehörigen öffentlichen Schlüssel pk

Signaturverfahren RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüsselgenerierung: (ähnlich dem RSA-Verschlüsselungsverfahren)

- Wähle zwei Primzahlen: p, q , setze $n = p \cdot q$ und $\phi(n) = (p - 1) \cdot (q - 1)$
- Verifikationsschlüssel (pk): Wähle e teilerfremd zu $\phi(n)$
- Signaturschlüssel (sk): Wähle d so, dass $e \cdot d = 1 \bmod \phi(n)$
- Zusätzlich benötigen wir eine Hashfunktion H

Signaturverfahren RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüsselgenerierung: (ähnlich dem RSA-Verschlüsselungsverfahren)

- Wähle zwei Primzahlen: p, q , setze $n = p \cdot q$ und $\phi(n) = (p - 1) \cdot (q - 1)$
- Verifikationsschlüssel (pk): Wähle e teilerfremd zu $\phi(n)$
- Signaturschlüssel (sk): Wähle d so, dass $e \cdot d = 1 \bmod \phi(n)$
- Zusätzlich benötigen wir eine Hashfunktion H

Signatur einer Nachricht $m \in \mathbb{Z}_n$ (**Signaturfunktion sig**)

- Berechne $h = H(m)$
- Berechne $s = h^d \bmod n$ (Verschl. von $h = H(m)$ mit dem geheimen Schlüssel)

Signaturverfahren RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüsselgenerierung: (ähnlich dem RSA-Verschlüsselungsverfahren)

- Wähle zwei Primzahlen: p, q , setze $n = p \cdot q$ und $\phi(n) = (p - 1) \cdot (q - 1)$
- Verifikationsschlüssel (pk): Wähle e teilerfremd zu $\phi(n)$
- Signaturschlüssel (sk): Wähle d so, dass $e \cdot d = 1 \bmod \phi(n)$
- Zusätzlich benötigen wir eine Hashfunktion H

Signatur einer Nachricht $m \in \mathbb{Z}_n$ (**Signaturfunktion** **sig**)

- Berechne $h = H(m)$
- Berechne $s = h^d \bmod n$ (Verschl. von $h = H(m)$ mit dem geheimen Schlüssel)

Signaturverifikation (**Verifikationsfunktion** **verify**)

- Berechne $h = H(m)$
- Berechne $v = s^e \bmod n$ (Entschl. von s mit dem öffentlichen Schlüssel)
- Wenn $h = v$, akzeptiere die Signatur, sonst nicht

Signaturverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Signaturverfahren erfüllen auch das Schutzziel Nichtabstreitbarkeit

- Die Signatur wird mit dem geheimen Schlüssel erzeugt
- Also kann nur der Inhaber des geheimen Schlüssels die Signatur berechnet haben

Weitere Signaturverfahren

- Digital Signature Algorithm (DSA), El-Gamal, Schnorr-Signatur: basieren auf dem diskreten Logarithmusproblem
- Merkle-Signatur: basiert auf Hashbäume
- McEliece-Niederreiter-Signatur: basiert auf lineare Codes

Challenge-Response Verfahren (asymmetrisch)

Ziel: Nachweis eines Geheimnisses (hier Schlüssel sk), ohne dieses offen zu legen
Als Basis können auch Signaturverfahren dienen
(ein symmetrisches Verfahren haben wir bereits auf Folie 180 gesehen)

A Bs öff. Schlüssel: pk

B Schlüsselpaar: (pk, sk)

choose random c
(challenge)

\xrightarrow{c}

compute $r := \text{sig}(sk, c)$
(response)

\xleftarrow{r}

compute $b := \text{verify}(pk, c, r)$
if $b = \text{true}$ then accept
else reject

Zusammenfassung RSA

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ein RSA-Schlüsselpaar kann genutzt werden für

- Verschlüsselung
- Datenauthentisierung (Signaturverfahren)
- Instanzauthentisierung (Challenge-Response-Verfahren)

Für alle drei Verfahren müssen verschiedene Schlüssel eingesetzt werden

- Wichtiges kryptographisches Grundprinzip: Trenne wo du trennen kannst
- Es gib auch Angriffe, wenn die selben Schlüssel genutzt werden (nächste Folie)

Schlüsseltrennung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Schlüssel für Daten- und Instanzauthentisierung müssen verschieden sein

Andernfalls ist folgender Angriff möglich:

- Angreifer erzeugt Nachricht m und bildet $H(m) = c$ (challenge)
- Angreifer fordert B zur Authentisierung auf und sendet c
- B berechnet Prüfsumme r
(B sieht nicht, ob c Zufall oder der Hashwert einer Nachricht ist)
- Dem Angreifer liegt eine von B korrekt signierte Nachricht vor

Schlüsseleinigungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziel: Sicherer Austausch von Schlüsseln über einen unsicheren Kanal

- Diffie-Hellman-Schlüsseleinigungsverfahren
(Entwickelt von Diffie, Hellman und Merkle 1976)
- Bekannt seit 1997: Ähnliches Verfahren entwickelt Anfang 1970 vom britischen Geheimdienst (Ellis, Cocks, Williamson)
- Sicherheit beruht auf der vermuteten Schwierigkeit des Diskreten Logarithmusproblems

Problem Diskreter Logarithmus (DL):

Eingabe: Zwei Zahlen g, h

Ausgabe: $\log_g h$, d.h. $x \in \mathbb{N}$ mit $g^x = h$

Problem Diskreter Logarithmus (DL):

Eingabe: Zwei Zahlen g, h

Ausgabe: $\log_g h$, d.h. $x \in \mathbb{N}$ mit $g^x = h$

Wann ist das DL-Problem praktisch nicht lösbar (Sicherheitsniveau 100 Bit)?

Wir betrachten wieder $\mathbb{Z}_p := \{0, 1, 2, \dots, p-1\}$ (Multiplikation modulo p)

Eigenschaften:

- Ist p eine Primzahl, so sind alle $x \in \mathbb{Z}_p \setminus \{0\}$ teilerfremd zu p (Def. Primzahl)
- Also besitzen alle $x \in \mathbb{Z}_p \setminus \{0\}$ multiplikativ Inverse in \mathbb{Z}_p (vgl. Folie 190)
- Sei $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, \dots, p-1\}$
(Menge aller multiplikativ invertierbaren Elemente in \mathbb{Z}_p)

Eigenschaften (Fortsetzung):

- \mathbb{Z}_p^* ist zyklisch, d.h. es gibt $g \in \mathbb{Z}_p^*$ mit $\{g^n \bmod p; n \in \mathbb{N}\} = \{1, 2, \dots, p-1\}$
 - g heißt dann Erzeuger der Gruppe
 - Insbesondere gilt also $\mathbb{Z}_p^* = \{g^n \bmod p; 1 \leq n \leq p-1\}$
- Beispiel $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$:
 - 3 ist Erzeuger: $3^1 = 3 \bmod 5, 3^2 = 9 = 4 \bmod 5,$
 $3^3 = 27 = 2 \bmod 5, 3^4 = 81 = 1 \bmod 5.$
 - 4 nicht: $4^1 = 4, 4^2 = 16 = 1 \bmod 5, 4^3 = 64 = 4 \bmod 5, \dots$
Also $\{4^n; n \in \mathbb{N}\} = \{1, 4\}.$
- Ist $g \in \mathbb{Z}_p^*$ Erzeuger, dann existiert für alle $h \in \mathbb{Z}_p^*$ ein $x \in \mathbb{N}$ mit $g^x = h$.
D.h. $\log_g h$ ist lösbar ($= x$)
- $\log_4 3$ ist nicht lösbar in \mathbb{Z}_5^*

Diffie-Hellman-Schlüsseleinigungsverfahren

- Wir rechnen in \mathbb{Z}_p^* , p sehr große Primzahl (siehe Folie 215)
- Wir benötigen einen Erzeuger $g \in \mathbb{Z}_p^*$

A Parameter (g, p)

choose random x

compute $X = g^x \bmod p$

comp. $Y^x = (g^y)^x = g^{xy} \bmod p$

B Parameter (g, p)

choose random y

compute $Y = g^y \bmod p$

comp. $X^y = (g^x)^y = g^{xy} \bmod p$

Abbildung: Diffie-Hellman-Schlüsseleinigungsverfahren (DH)

Diffie-Hellman-Schlüsseleinigungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Aus g^{xy} lassen sich z.B. Schlüssel für Secure Messaging ableiten:

- $k_E := \text{Hash}(g^{xy} || 0x00)$ Schlüssel für Verschlüsselung
- $k_A := \text{Hash}(g^{xy} || 0x01)$ Schlüssel für MAC

Sicherheit des Diffie-Hellman-Schlüsseleinigungsverfahrens

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Angreifer kennt Parameter (g, p) und sieht $g^x \bmod p$ und $g^y \bmod p$

Ziel: Bestimmung von g^{xy} (das gemeinsame Geheimnis)

- Einzige derzeit bekannte Möglichkeit: Bestimme x oder y (d.h. berechne $\log_g g^x$ oder $\log_g g^y$)
- Erste Idee hierfür: Probepotenzieren
 - Wähle x' , berechne $g^{x'}$ und vergleiche: $g^x \stackrel{?}{=} g^{x'}$.
 - Für $p > 2^{100}$ ist $|\mathbb{Z}_p^*| > 2^{100}$, also W'keit für Gleichheit: $1/2^{100}$.
 - D.h. ca. 2^{100} Versuche, x zu finden (Sicherheitsniveau 100 Bit)
- Aber: Es gibt bessere Algorithmen zum Bestimmen des Logarithmus
 - Für Sicherheitsniveau von 100 Bit werden deutlich größere Zahlen benötigt
 - Nachweis in der Vorlesung Kryptologie

Man-in-the-Middle Angriff

Aber folgender Angriff möglich:

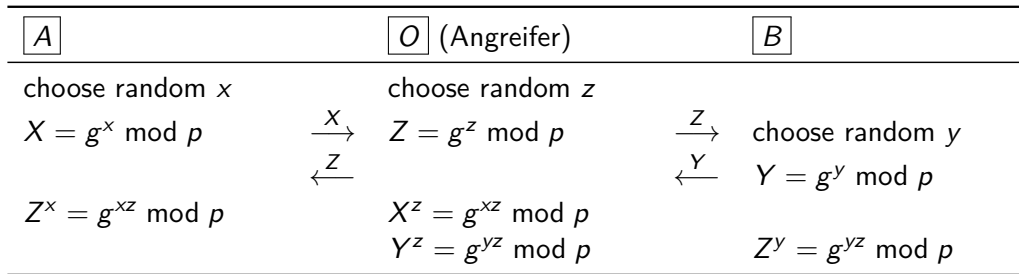


Abbildung: Man-in-the-Middle Angriff

- Nicht A und B einigen sich auf ein Geheimnis, sondern A mit O und B mit O
- Nachfolgend kann O durch Umschlüsselung die Kommunikation zwischen A und B belauschen, ohne das dies auffällt

Diffie-Hellman-Schlüsseleinigungsverfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Die Schlüsselanteile $g^x \bmod p$ und $g^y \bmod p$ müssen den jeweiligen Kommunikationspartnern zugeordnet werden können

- Mögliche Lösungen sind:
 - Authentisierung der Schlüsselanteile (MAC oder Signatur)
 - Authentisierung der Kommunikationspartner (Instanzauthentisierung)
- In jedem Fall benötigen A und B vorab einen Vertrauensanker, z.B.:
 - öffentlicher Schlüssel des jeweils anderen
 - gemeinsamer symmetrischer Schlüssel
- Dieser Vertrauensanker muss vorab sicher ausgetauscht werden:
 - öffentliche Schlüssel: authentisch
 - symmetrischer Schlüssel: vertraulich und authentisch

Problem: Zuordnung eines Schlüssels zum Schlüsselinhaber (wem gehört der Schlüssel)

- Beispiel 1: Verschlüsselung mit öffentlichem Schlüssel, Entschlüsselung mit geheimem Schlüssel:
 - Bei Nutzung des öffentlichen Schlüssels einer falschen Person kann diese die Nachricht entschlüsseln (Verlust der Vertraulichkeit)
- Beispiel 2: Signaturerzeugung mit geheimem Schlüssel, Verifikation mit öffentlichem Schlüssel:
 - Bei falscher Zuordnung des öffentlichen Schlüssels zu einer Person vertraue ich fälschlicherweise auf die Authentizität der Daten (Verlust der Datenauthentizität)

Vertrauensmodelle

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Wir unterscheiden drei Vertrauensmodelle

- Direct Trust: Nutzer erhält den öff. Schlüssel direkt vom Schlüsselinhaber
 - kleine Virtual Private Networks
- Web of Trust: Nutzer signieren gegenseitig ihre öff. Schlüssel
 - PGP, GNU-PG
- Hierarchical Trust: Öff. Schlüssel werden von einer zentralen Instanz verwaltet
 - Qualifizierte elektronische Zertifikate nach Signaturgesetz
 - Public Key Infrastruktur des Deutschen Forschungsnetzwerkes
 - Server-Authentisierung via https

Direct Trust

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Direct Trust ist nur für kleine Gruppen anwendbar
(Paarweiser Schlüsselaustausch notwendig)

- 2 Personen: ein Austausch
- 3 Personen: 3
- 4 Personen: 6
- n Personen: $n(n-1)/2$
- Kommt neuer Partner hinzu: Austausch mit n Personen

Web of Trust

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Idee: Nutzer signieren öffentliche Schlüssel andere Nutzer (und garantieren so für die Authentizität des Schlüssels).

- Beispiel (Alice, Bob und Carl):
 - Alice signiert Bobs öffentlichen Schlüssel
 - Bob signiert Carls öffentlichen Schlüssel
 - Alice vertraut Carls öffentlichem Schlüssel
- Warum vertraut Alice Carls Schlüssel?
 - Alice prüft mit Bobs öff. Schlüssel Bobs Signatur von Carls öff. Schlüssel (Ist aber nur dann sicher, wenn Alice Bob vertraut, nur authentische Schlüssel zu signieren, also vor der Signierung die Bindung zwischen Schlüssel und Schlüsselinhaber zu prüfen (z.B. über Direct Trust))

Web of Trust

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Jeder Nutzer hat einen Schlüsselbund (key ring) mit öff. Schlüsseln anderer Nutzer

- Jedem öffentlichen Schlüssel sind zugeordnet
 - Name des Schlüsselinhabers
 - Owner Trust (5 Stufen, Grad des Vertrauens in die Prüffähigkeit des Schlüsselinhabers)
 - Key Legitimacy (3 Stufen, Grad des Vertrauens in den öffentlichen Schlüssel)
leitet sich ab aus den Owner Trusts der Signierer und der Anzahl der Signaturen
 - Signaturen des öffentlichen Schlüssels
- Vorgehen in RFC 2440 (OpenPGP Message Format) beschrieben

Web of Trust: Owner Trust

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Wert für Owner Trust legt jeder Nutzer selbst fest.
- Gibt an, wie der Schlüsselinhaber öffentliche Schlüssel anderer Nutzer prüft
- Fünf Level:
 - unbekannt (unknown) für Nutzer, über die man keine weiteren Informationen hat
 - kein Vertrauen (not trusted) für Nutzer, denen nicht vertraut wird
 - geringes Vertrauen (marginal) für Nutzer, denen nicht voll vertraut wird
 - volles Vertrauen (complete) für Nutzer, denen voll vertraut wird
 - absolutes Vertrauen (ultimate) für Nutzer, deren privater Schlüssel sich im privaten Schlüsselbund befindet (üblicherweise nur die eigenen privaten Schlüssel)

Web of Trust: Key Legitimacy

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Vertrauen in Authentizität eines öffentlichen Schlüssels

- x = Anzahl von Signaturen von Nutzern, deren Owner Trust marginal ist
- X = Anzahl von Signaturen mit einem Owner Trust marginal, die erforderlich ist, damit ein Schlüssel als authentisch eingestuft wird
- y = Anzahl von Signaturen von Nutzern, deren Owner Trust complete ist
- Y = Anzahl von Signaturen mit einem Owner Trust complete, die erforderlich ist, damit ein Schlüssel als authentisch eingestuft wird
- Vertrauenslevel $L := x/X + y/Y$. Man unterscheidet drei Level:
 - nicht authentisch ($L = 0$), teilweise authentisch ($0 < L < 1$), authentisch ($L \geq 1$)
- Üblich sind die Werte $X = 2$ und $Y = 1$, d.h., Schlüssel ist authentisch, wenn
 - der Schlüssel von einer vertrauenswürdigen (complete) Person, oder
 - von zwei teilweise vertrauenswürdigen (marginal) Personen signiert wurde

Web of Trust: Eigenschaften

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Nachteile:

- Einstufung (Owner Trust) erfordert hohes Wissen der Nutzer
- Die Signaturen sind juristisch nicht bindend (vgl. Signaturgesetz)
- Zurückziehen von Zertifikaten nicht einfach umsetzbar

Vorteile:

- Gegenüber Direct Trust eine deutliche Verbesserung
- Umgesetzt in PGP (Pretty Good Privacy) und GnuPG (Open Source)
- Es gibt zahlreiche Schlüsselservers, auf denen öffentliche Schlüssel und zugehörige Signaturen hochgeladen werden können
- Einige Institutionen bieten einen Certification Service für PGP- und GPG-Schlüssel an (z.B. c't)

Hierarchical Trust

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ziele:

- Zuordnung eines öffentlichen Schlüssels zum Schlüsselinhaber
- Festlegung der Schlüsselnutzung (Verschlüsselung, Authentisierung, Signatur)
- Etablierung einer gemeinsamen Sicherheitsinfrastruktur
 - Wie sicher sind die Schlüssel gelagert, erzeugt usw.
 - Wie stark ist die Bindung zwischen Schlüssel und Schlüsselinhaber (z.B. wie wird geprüft)

Hierarchical Trust

Public Key Infrastrukturen

- Öffentliche Schlüssel werden von einer vertrauenswürdigen Instanz verwaltet
- Nutzer erhalten Zertifikate C_i für ihren öffentlichen Schlüssel pk_i
- Vertrauensanker bildet der öffentliche Schlüssel pk_{CA} der CA

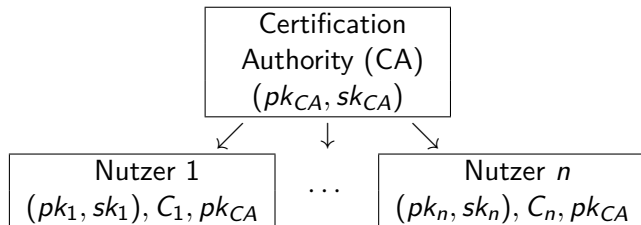


Abbildung: Schematischer Aufbau einer Public Key Infrastruktur

Public Key Infrastrukturen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

$C_i = (\text{Inhalt, Signatur}) =$

Angaben zum Nutzer

Name, Organisation, usw.

öffentlicher Schlüssel pk_i

Verwendeter Algorithmus

z.B. RSA, DSA

Gültigkeitszeitraum

Angaben zur Certification Authority

Name, Kontaktdaten usw.

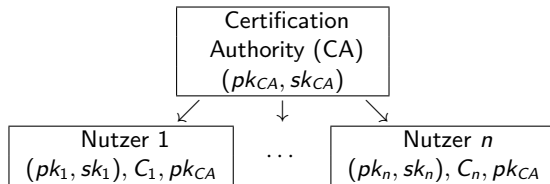
Schlüsselnutzung

z.B. Signatur, Authentisierung, Verschlüsselung

Signatur der CA (mit sk_{CA})

Abbildung: Zertifikat für Nutzer i (ausgestellt von der Certification Authority)

Public Key Infrastrukturen: Beispiel Signatur



Nutzer 1 signiert Dokument m , Nutzer 2 prüft Signatur

Nutzer 1 Schlüssel: $(pk_1, sk_1), C_1$

Nutzer 2 Schlüssel: pk_{CA}

compute $s := \text{sig}(sk_1, m)$

s, C_1, m
 \longrightarrow

verify($pk_{CA}, \underbrace{\text{inhalt, signatur}}_{=C_1}$)

verify(pk_1, m, s)

Public Key Infrastrukturen

Häufig weitere Aufteilung:

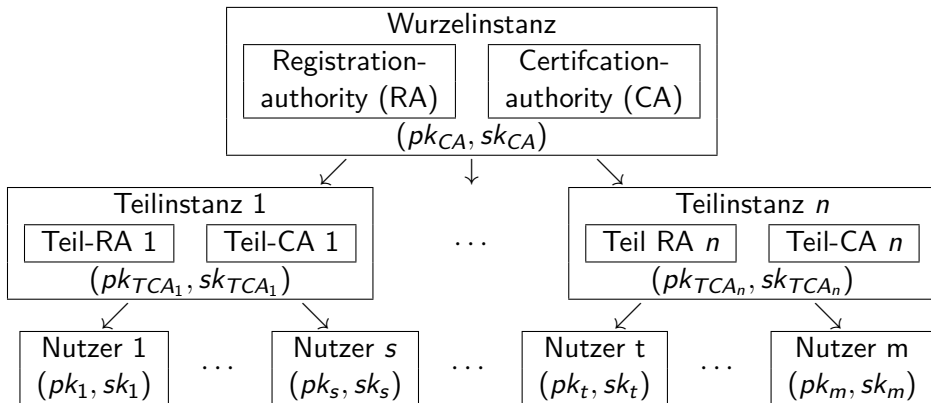


Abbildung: Schematische Darstellung einer 3-stufigen Public Key Infrastruktur

Public Key Infrastrukturen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Aufgabenverteilung:

- Registration Authority
 - Legt Sicherheitsrichtlinien fest
 - Prüft Zertifizierungsanträge
 - Legt Inhalte der Zertifikate fest
 - Leitet Anträge an Certification Authority weiter
- Certification Authority:
 - Stellt die eigentlichen Zertifikate aus

Zurückziehen von Zertifikaten:

- Bei Sicherheitsvorfällen (z.B. Schlüsselkompromittierung, Alg. werden unsicher)
- Eine Instanz hält sich nicht an Sicherheitsvorgaben
- Hierzu: Führen von Certificate Revocation Lists (CRLs)
- Zusätzlich: Prüfung, ob Zertifikate in CRL enthalten ist

Public Key Infrastrukturen

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Alle Instanzen einer PKI (Root-CA, Teil-CAs, Endnutzer) müssen ein definiertes Maß an Sicherheitsstandards einhalten.

Sicherheitsvorgaben werden in zwei Dokumenten festgelegt:

- Certificate Policy: welche Sicherheitsvorgaben müssen eingehalten werden
- Certificate Practise Statement: wie werden die Sicherheitsvorgaben umgesetzt
- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practise Framework
(beschreibt wird Aufbau und Inhalt beider Dokumente im Detail)

Public Key Infrastrukturen: RFC 3647

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Allgemeines

- Teilnehmer der PKI
- Zertifikatsnutzung
- Genutzte Algorithmen
- Schlüssellängen
- Datenfelder in den Zertifikaten

- Initialisierung

- Registrierung der Teilnehmer
- Generierung der Schlüsselpaare
- Generierung der Zertifikate
- Schlüssel- und Zertifikatsverteilung
- Schlüssel-Backup

- Nutzung

- Zertifikatsneuausstellung
- Zertifikatsvalidierung
- Schlüsselupdate
- Schlüssel-Recovery

- Aufhebung

- Ablauf des Zertifikates
- Zurückziehen des Zertifikates
- Archivierung

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Zertifikate müssen:

- Inhaber eindeutig identifizieren,
- Schlüsselnutzung festlegen,
- Ausstellende CA identifizieren
(hieraus folgen u.a. die Sicherheitsvorgaben für die PKI)

Es existieren zwei Standards für Zertifikate:

- X509: Eingesetzt zur sicheren Kommunikation im Internet (https)
- Card Verifiable Certificates (cvc): Eingesetzt zur sicheren Kommunikation zwischen/zu Smartcards

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

X509-Zertifikate: Kodiert nach ASN.1 (Abstract Syntax Notation Nr. 1)

```
Certificate ::= SEQUENCE {  
    tbsCertificate      TBSCertificate,      TBS: To Be Signed  
    signatureAlgorithm  AlgorithmIdentifier,  Signaturalgorithmus  
    signatureValue      BITSTRING }          Signatur über TBSCert.
```

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

```
TBSCertificate ::= SEQUENCE {  
    version                EXPLICIT Version DEFAULT v1,  
    serialNumber            CertificateSerialNumber,  
    signature               AlgorithmIdentifier,  
    issuer                  Name,  
    validity                Validity,  
    subject                 Name,  
    subjectPublicKeyInfo    SubjectPublicKeyInfo,  
    extensions              EXPLICIT Extensions OPTIONAL  
                           --If present, version MUST be v3 }
```

Erweiterungen (extensions) gibt es erst ab Version 3

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

`Version ::= INTEGER { v1(0), v2(1), v3(2) }`

Aktuell v3, v1, v2 aber weiterhin nutzbar

`CertificateSerialNumber ::= INTEGER`

Unterschiedlich für alle Zertifikate, die von einer CA (issuer) ausgestellt werden:
Meist Zähler oder Hashwert über Public Key.

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

```
AlgorithmIdentifier ::= SEQUENCE {  
    algorithm      OBJECT IDENTIFIER,  
    parameters    ANY DEFINED BY algorithm OPTIONAL }
```

Legt Signaturalgorithmus zum Signieren des Zertifikats über eine OID fest

Selber Wert wie unter `signatureAlgorithm`

Einschub OID

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

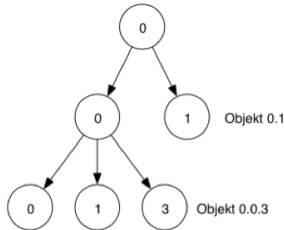
IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Object Identifier (OID) bezeichnen Informationsobjekte (weltweit eindeutig)

- Eine OID ist ein Knoten in einem hierarchisch zugewiesenen Namensraum Folge von Nummern, die seine Position, beginnend an der Wurzel, angibt
- Drei Wurzeln: ITU-T (0), ISO (1), joint-iso-itu-t (2)
 - ITU-T: International Telecommunication Union-Telecommunication Standardization Sector
 - ISO: International Organization for Standardization
- ISO/IEC 9834, DIN 66334: Regeln für Vergabe und Registrierung von OIDs



Einschub OID

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Beispiel:

- Signaturalgorithmus sha1-with-rsa-signature: 1.2.840.113549.1.1.5
iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha1-with-rsa-signature(5)
- Auflösen der OIDs in OID-Respositories:
 - Z.B.: <http://www.oid-info.com>

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

issuer, subject beschreiben Aussteller, Inhaber eindeutig über Name
Enthält Anzahl von Attributen, z.B.

- country: DE
- organization: HDA
- organizational unit: FBI
- common name: Marian Margraf
- serial number: 1,2,...

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

```
Validity ::= SEQUENCE {  
    notBefore    Time,  
    notAfter     Time }
```

Zeitraum, in dem der geheime Schlüssel genutzt werden kann

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

```
SubjectPublicKeyInfo ::= SEQUENCE {  
    algorithm           AlgorithmIdentifier,  
    subjectPublicKey     BIT STRING }
```

Enthält den öffentlichen Schlüssel

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ab Version v3 sind Extensions erlaubt, z.B. für

- Informationen über Schlüsselnutzung
- Informationen über Sicherheitsrichtlinien (wo findet man CP und CPS)
- Erweiterte Attribute für issuer und subject:
mögliche Kontaktdaten für Rückfragen (E-Mailadresse, Fax, Telefon)
- Einschränkungen des Zertifikatspfades, z.B. maximale Pfadkette, d.h. wie viele Zertifikate müssen maximal bis zum Root-Zertifikat geprüft werden

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

`Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension`

```
Extension ::= SEQUENCE {  
    extnID      OBJECT IDENTIFIER,  
    critical    BOOLEAN DEFAULT FALSE,  
    extnValue   OCTET STRING }
```

`extnID`: Identifier der Extension

`critical`: gibt an, ob eine bestimmte Angabe geprüft werden muss oder das Zertifikat auch ohne die Überprüfung dieser Angabe als gültig akzeptiert werden kann

`extnValue`: Inhalt der Extension

Public Key Infrastrukturen: Zertifikate

Extension Schlüsselnutzung (OID: 2.5.29.15)

joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15)

```
KeyUsage ::= BIT STRING {  
    digitalSignature      (0),  
    nonRepudiation       (1),  
    keyEncipherment      (2),  
    dataEncipherment     (3),  
    keyAgreement          (4),  
    keyCertSign          (5),  
    cRLSign              (6),  
    encipherOnly         (7),  
    decipherOnly         (8) }
```

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Weitere Schlüsselnutzungen:

- Code signing
- OCSP signing
- Timestamping

Public Key Infrastrukturen: Zertifikate

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Weitere mögliche Erweiterungen sind:

- Extended Key Usage
- Certificate Policies
- CRLDistributionPoints
- Freshest CRL

Authentisierung: Einführung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

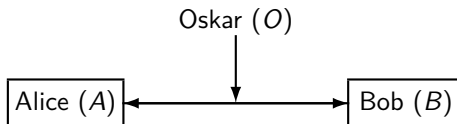
Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

B (Prüfer) kann die Identität von A (Beweisender) zweifelsfrei feststellen
Angreifer O versucht, Identität von A zu übernehmen



Feststellung der Identität z.B. über:

- eindeutige Merkmale
- charakteristische Eigenschaften

Authentisierung: Einführung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Grundlage für alle kryptographischen Verfahren:

- Mit wem führe ich einen Schlüsselaustausch durch (vgl. MitM-Angriff, Folie 216)
- Wem schicke ich vertrauliche Nachrichten
- Wer schickt mir vertrauliche Nachrichten
- Wer hat eine Nachricht signiert

Authentisierung: Einführung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Faktoren für die Überprüfung:

- Wissen (z.B. ein Passwort, eine PIN (Personal Identification Number))
- Besitz (z.B. ein Schlüssel in einer Chipkarte)
- Eigenschaften (z.B. ein biometrisches Merkmal)

n –Faktor-Authentisierung:

- 1-Faktor-Authentisierung: Nutzt nur einen Faktor
z.B. Abrufen von E-Mails: Benutzername/Passwort (Wissen)
- 2-Faktor-Authentisierung: Nutzt zwei verschiedene Faktoren
z.B. Auszahlung am Geldautomaten: Bankkarte (Besitz) und PIN (Wissen)

Typisches Beispiel: Benutzername/Passwort

- Anmeldung am Client
- Anmeldung an Webdiensten (E-Mail, Forum, Online-Banking)

Nachteile: Anfällig gegen

- Ausspähen (z.B. über Phishing, Keylogging, Abhören der Verbindung)
Replay-Attacken: Abhören der Verbindung und Wiedereinspielen
- Man-in-the-Middle Attacken: klar

Einmalpasswörter

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Verbesserung: Einmalpasswörter

- Jedes Passwort wird nur einmal verwendet
- Verhindert somit Replay-Attacken

Problem: Beide Seiten müssen die Passwörter kennen

Zwei Möglichkeiten:

- Passwortlisten
- Passwortgeneratoren

Einmalpasswörter: Passwortlisten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Typischer Anwendungsfall: Transaktionsnummern (TAN) im Online-Banking
z.B. zur Bestätigung von Überweisungen

- Beide Kommunikationspartner erhalten eine Liste mit Passwörtern
- Passwörter werden wie folgt verwendet:
 - Sequentielle Auswahl: von oben nach unten
 - Indizierte Auswahl: Prüfer gibt an, welches Passwort verwendet wird (z.B. Nummer in der Liste)
 - Beliebige Auswahl: Beweisender sucht ein Passwort aus
Nachteil hier: Raten des Passwortes wird vereinfacht (mehrere Passwörter möglich)

Einmalpasswörter: Passwortlisten

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Indizierte Auswahl ist ein Challenge-Response Protokoll (vgl. Folie 180)

B Prüfer (Liste L)

A Beweisender (Liste L)

wähle Index i
(challenge)

\xrightarrow{i}

suche i -tes Passwort p_i
(response)

$\xleftarrow{p_i}$

vergleiche

Einmalpasswörter: Passwortgeneratoren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Ableitung verschiedener Passwörter aus einem vorab ausgetauschten Geheimnis g

Wir unterscheiden:

- zeitgesteuerte Generatoren
- ereignisgesteuerte Generatoren
- Challenge-Response-Generatoren

Zeitgesteuerte Generatoren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Hauptideen:

- Generierung der Einmalpasswörter aus
 - g (vorab ausgetauschtes Geheimnis) und
 - t (Zeitpunkt der Authentisierung)
- Beide Parteien (Prüfer und Beweisender) generieren das Einmalpasswort
- Prüfer vergleicht sein Einmalpasswort mit dem vom Beweisenden

Problem:

- Zeit beim Prüfer und Beweisenden nicht exakt gleich
- Man benötigt also einen Toleranzbereich (z.B. 30 Sekunden)

Zeitgesteuerte Generatoren: Google Authenticator

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicherheit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- $\text{key} = g$ (vorab ausgetauschtes Geheimnis)
- $t = \text{time}$ (in sec (Zeitpunkt der Authentisierung))
- $\text{message} = t/30$ (Zeitintervall von 30 Sekunden)
- $p = \text{mac}(\text{key}, \text{message})$ (Einmalpasswort für Zeit t)
Message Authentication Codes (MAC), z.B. HMAC, siehe Folie 147

Ereignisgesteuerte Generatoren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Hauptideen:

- Generierung der Einmalpasswörter aus
 - g (vorab ausgetauschtes Geheimnis) und
 - t (Zähler, Anzahl der bereits durchgeführten Authentisierungen)
- Beide Parteien (Prüfer und Beweisender) generieren das Einmalpasswort
- Prüfer vergleicht sein Einmalpasswort mit dem vom Beweisenden

Ereignisgesteuerte Generatoren: Lamport-Hash

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Basiert auf einer kryptographischen Hashfunktion H (benötigt: nicht rückrechenbar)

- g (vorab ausgetauschtes Geheimnis)
- Zufallszahl r (muss nicht geheim gehalten werden)
- Startwert $S = H(r||g)$ ($r||g = r$ und g hintereinander geschrieben)
- Generierung der Einmalpasswörter:
 - Erstes Passwort: $p_1 = H^N(S)$ (N mal Anwenden von H)
 - Zweites Passwort: $p_2 = H^{N-1}(S)$ ($N - 1$ mal Anwenden von H)
 - t -tes Passwort: $p_t = H^{N-(t-1)}(S)$
- Aus $p_t = H^{N-(t-1)}(S)$ lässt sich nicht $p_{t+1} = H^{N-(t-2)}(S)$ berechnen
 $H^{N-(t-1)}(S) \mapsto H^{N-(t-2)}(S)$ ist die Umkehrung von H auf $H^{N-(t-1)}(S)$

Ereignisgesteuerte Generatoren: Lamport-Hash

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Problem: Irgendwann wurden N Passwörter erzeugt

- Reinitialisierung: Wähle einen neuen Zufallswert r
- Bilde neuen Startwert $S = H(r||g)$

Challenge-Response gesteuerte Verfahren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Kennen wir schon (z.B. auf Basis von Message Authentication Codes)
Vorab ausgetauschtes Geheimnis: Der symmetrische Schlüssel k

B (Prüfer) Schlüssel: k

A (Beweisender) Schlüssel: k

choose random c
(challenge)

\xrightarrow{c}

compute $r := \text{mac}(k, c)$
(Einmalpasswort, response)

\xleftarrow{r}

compute $r' := \text{mac}(k, c)$
if $r' = r$ then accept
else reject

Einmalpasswörter: Zusammenfassung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Vorteile:

- Sicher gegen passive Angriffe (Ausspähen): Jedes Mal ein neues Passwort
- Verfahren verhindert somit Replay-Attacken

Weiterhin möglich: Man-in-the-Middle-Angriff (aktiver Angriff)

- Angreifer O gibt sich al Prüfer B aus und erhält das Einmalpasswort von A
- O kann sich gegen über B als A ausgeben
- Verhinderung des Angriffs: Gegenseitige Authentisierung:
 - Nicht nur A muss sich gegenüber B authentisieren,
 - sondern auch B gegenüber A

Faktoren

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- Wissen (erledigt)
- Besitz (kommt jetzt)
- Eigenschaften (kommt nach Besitz)

Faktor Besitz

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

- A (Beweisender) besitzt einen geheimen Schlüssel k
 - Für symmetrische Verfahren: Schlüssellänge ≥ 100 Bit
 - Für asymmetrisches Verfahren RSA: Schlüssellänge ≥ 4000 Bit
- Schlüssel ist irgendwo gespeichert
- Ziel: Sichere Speicherung des Schlüssels
 - Schlüssel soll von keinem Unbefugten ausgelesen werden können
 - Schlüssel soll von keinem Unbefugten genutzt werden können

Sicherheitselemente

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Nutzung sicherer Hardware (Sicherheitschips)

Microprozessoren, die gegen Angriffe geschützt sind, z.B. gegen

- physikalische Attacken (bohren, fräsen, ...)
- elektrische Angriffe (mehr Strom, als Spezifikation erlaubt)
- Angriffe mit Licht und Laser

Detektoren erkennen Angriffe, Schlüsselspeicher wird gelöscht

2-Faktor-Authentisierung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

2-Faktor-Authentisierung basierend auf

- Besitz (Sicherheitselement) und
- Wissen (PIN)

Umsetzung

- Speicherung von Schlüssel und PIN im nicht-auslesbaren Bereich des Chips
- Authentisierung:
 - über Challenge-Response Verfahren
 - Nutzung des Schlüssels wird über PIN freigegeben

2-Faktor-Authentisierung

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Anwendungsbeispiele:

- Bankkarten (Geldabheben an Bankautomaten)
- Kreditkarten (Bezahlen am Point of Sale)
- Personalausweis (Authentisieren mit der Online-Ausweisfunktion)

Angriffe

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

**Netzwerk- und
Internetsicher-
heit**

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Angriffe

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

**Sicherheit für
Ubiquitous
Computing**

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Angriffe

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

**Bewertungs-
kriterien**

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Netzwerksicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

**IT-Sicherheits-
management**

IT-Forensik

Sichere
Software-
entwicklung

Netzwerksicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

Sichere
Software-
entwicklung

Netzwerksicherheit

Einleitung

Grundlegende
Begriffe

Kryptologie

Authentisierung

Netzwerk- und
Internetsicher-
heit

Sicherheit für
Ubiquitous
Computing

Bewertungs-
kriterien

IT-Sicherheits-
management

IT-Forensik

**Sichere
Software-
entwicklung**