
Kryptographie

Vorlesung im WS 2007/8

<http://www.math.tu-berlin.de/~hess/krypto-ws2007>

*Florian Heß / Osmanbey Uzunkol
Technische Universität Berlin*

1

16. Oktober 2007

Zielsetzungen in der Kryptographie

Sichere digitale Kommunikation in Anwesenheit von vertrauensunwürdigen Personen.

Hauptaufgaben:

- Verschlüsselung
- Digitale Signaturen

Spezieller:

- Authentizität, Authentifizierung, Datenintegrität
- Anonymität, Autorisierung, elektronisches Geld
- elektronische Wahlen
- ...

2

16. Oktober 2007

Terminologie

Kryptographie:

- Entwurf und Design von Kryptosystemen, also zum Beispiel Verfahren für die Verschlüsselung und digitale Signaturen.

Kryptoanalyse:

- Versucht, Kryptosysteme zu “knacken”.

Kryptologie:

- Zusammenfassender Begriff für Kryptographie und Kryptoanalyse.
- Wir verwenden “Kryptographie” synonym für “Kryptologie”.

3

16. Oktober 2007

Geschichte der Kryptographie

Alte Disziplin:

- Cäsar, Alexander der Große, ...
- Unsystematische Verwendung bis 20. Jahrhundert.

20. Jahrhundert:

- Systematisierung und Formalisierung.
- Wichtige Rolle im zweiten Weltkrieg (Enigma, A. Turing).
- Bis in die 60er Jahr hauptsächlich Verwendung durch Regierungen und Militär.
- Mit zunehmender Computerisierung verstärkte Verwendung und Anforderungen im wirtschaftlichen (privaten) Bereich.

4

16. Oktober 2007

Geschichte der Kryptographie

20. Jahrhundert (ctd):

- 1976: "New directions in cryptography" von Diffie und Hellman, Geburtsstunde der Kryptographie mit öffentlichem Schlüssel.
- 80er Jahre: Zero-knowledge Protokolle.
- 90er Jahre: Massenhafte Verbreitung kryptographischer Verfahren durch Computer, Internet, Geldautomaten, Mobilfunk, etc.

5

16. Oktober 2007

Kryptographie und andere Wissenschaften

Die Kryptographie ist ausgesprochen **interdisziplinär**:

- **Theoretische und angewandte Informatik** (Komplexitätstheorie, Informationstheorie, Protokolle, formale Methoden, Software Engineering, ...)
- **Mathematik** (Algebra, Zahlentheorie, ...)
- **Elektrotechnik** (Chipdesign, ...)
- **Physik** (Quantenphysik und -computer, ...)
- **Gesellschaftspolitische und rechtliche Aspekte** (DMCA, ...)

Informationssicherheit („Softwaresicherheit“) fällt nicht unter Kryptographie.

6

16. Oktober 2007

Algorithmen

Unter einem Algorithmus verstehen wir einen Text von elementaren Anweisungen, die beispielsweise auf einem Computer oder einer Turing Maschine ausgeführt werden können.

Ein Algorithmus erwartet eine Eingabe, tätigt eine Ausgabe und endet dann.

Ein Algorithmus heißt deterministisch, wenn die auszuführenden Anweisungen eindeutig durch die Eingabe bestimmt sind. Ein solcher Algorithmus verhält sich wie eine Funktion.

Ein Algorithmus heißt probabilistisch, wenn die auszuführenden Anweisungen neben der Eingabe auch von zufälligen Entscheidungen während des Laufs abhängen.

7

16. Oktober 2007

Algorithmen

Zu vorgegebener Eingabe ist die Laufzeit eines Algorithmus die Anzahl der bis zum Ende des Algorithmus ausgeführten Anweisungen, inklusive der Zufallsabfragen. Im Zusammenhang mit Computern werden häufig Bitoperationen gezählt.

Die Laufzeit und die Ausgabe eines probabilistischen Algorithmus hängen damit ebenfalls vom Zufall ab und stellen Zufallsvariablen dar.

Ist A ein probabilistischer Algorithmus, so können wir daraus einen deterministischen Algorithmus A_D machen, indem wir die von A benutzte Zufallsquelle als Eingabe von A_D auffassen.

Ein Algorithmus ist polynomiell, wenn es ein Polynom $f \in \mathbb{Z}[t]$ gibt, so daß seine Laufzeit für die Eingabe x durch $f(|x|)$ beschränkt ist.

($|x|$ ist die Wort- oder spezieller Bitlänge von x , siehe Folie 10)

8

16. Oktober 2007

Algorithmen

Beispiel:

Aufgabe ist, eine 6 zu würfeln. Lösung ist, einfach wiederholt zu würfeln, bis eine 6 erscheint. Die erwartete Laufzeit dieses probabilistischen Algorithmus ist dann 6 mal Würfeln.

In vielen Fällen sind probabilistische Algorithmen deterministischen Algorithmen zur Lösung der gleichen Probleme überlegen (einfacher und schneller).

9

16. Oktober 2007

Alphabete und Worte

Ein Alphabet A ist eine nicht-leere Menge.

Die Wortmenge A^* über A ist $A^* = \bigcup_{i=0}^{\infty} A^i$.

Beispiel:

- $A = \{A, \dots, Z\}$, HALLO $\in A^*$
- $A = \{0, 1\}$, 101101 $\in A^*$.
- $1^k = 11 \dots 1$, k Einsen.

Leeres Wort: ε .

Aneinanderhängen von Worten: $m_1, m_2 \in A^* \rightarrow m_1 m_2 \in A^*$.

Länge $|m|$ eines Worts $m \in A^*$: $|m|$ ist minimal mit $m \in A^{|m|}$.

Schreibweise in einigen Programmiersprachen: 'A', "HALLO", ""

10

16. Oktober 2007

Konzepte der Verschlüsselung

Klartexte sind aus Klartextrraum: $m \in M \subseteq A_1^*$.

Chiffretexte sind aus Chiffretextrraum: $c \in C \subseteq A_2^*$.

Schlüssel sind aus Schlüsselräumen: $e \in K_1 \subseteq A_3^*$, $d \in K_2 \subseteq A_4^*$.

Verschlüsselungsverfahren $\mathcal{E} : K_1 \times M \rightsquigarrow C$.

Entschlüsselungsverfahren $\mathcal{D} : K_2 \times C \rightarrow M$.

Verschlüsselung von Klartext m mit Schlüssel e : $c \leftarrow \mathcal{E}(e, m)$.

Entschlüsselung von Chiffretext c mit Schlüssel d : $m \leftarrow \mathcal{D}(d, c)$.

\mathcal{E} und \mathcal{D} sind effiziente Verfahren (z.B. Programme).

\mathcal{E} und \mathcal{D} dürfen probabilistisch sein (dürfen den Zufall verwenden).

\mathcal{E} kann mehrdeutig sein (\rightsquigarrow).

11

16. Oktober 2007

Beispiele: Affin-lineare Blockchiffren

$R = \mathbb{Z}/w\mathbb{Z}$ und $M = C = R^n$, $K_1 = K_2 = \text{GL}(n, R) \times R^n$.

Für $A \in \text{GL}(n, R)$ und $b \in R^n$ seien

- $c = \mathcal{E}((A, b), m) = Am + b$,
- $m = \mathcal{D}((A, b), c) = A^{-1}(c - b)$.

Chiffre von Cäsar:

- $w = 26$, $n = 1$, $A = (1)$, $b = 3$.

Chiffre von Vignère:

- $w = 26$, $A = I_n$, $b \in R^n$.
- Nicht jeder Buchstabe wird gleich verschlüsselt.

Chiffre von Hill:

- $w = 26$, A Permutationsmatrix, $b = 0$

12

16. Oktober 2007

Beispiele: Affin-lineare Blockchiffren

Kryptoanalyse:

- Angriff durch Untersuchung der Häufigkeit des Auftretens von Buchstaben in natürlicher Sprache.
- Angriff falls $n + 1$ Klartext- und Chiffretextpaare (m_i, c_i) vorliegen.

Dann $m_i - c_0 = A(m_i - m_0)$. Ist U Matrix mit den Spalten $c_i - c_0$ und V Matrix mit den Spalten $m_i - m_0$, so gilt $U = AV$. Ist V invertierbar, folgt $A = UV^{-1}$ und $b = c_0 - Am_0$.

Beispiele: Affin-lineare Blockchiffren

Vernam's One Time Pad:

- Im Chiffre von Vignère den Vektor b gleichverteilt zufällig aus R^n wählen und nur einmal verwenden.
- Dann c ebenfalls völlig zufällig, keine Verbindung zu Klartext. Daher unmöglich, aus c Informationen über m zu bekommen.
- Chiffre aber inpraktikabel (wie b zu Kommunikationspartner bringen?)

Symmetrisch, asymmetrisch

Symmetrisches Verschlüsselungssystem (secret key):

- $d = e$ (oder d leicht aus e berechenbar).
- Sender und Empfänger haben e als gemeinsames Geheimnis.

Asymmetrisches Verschlüsselungssystem (public key):

- d geheim, e öffentlich.
- d schwer oder gar nicht aus e berechenbar.
- Empfänger besitzt e und d .
- Sender verwendet e zum Verschlüsseln.
- Empfänger verwendet d zum Entschlüsseln.

Prinzip von Kerckhoff

Grundlegende Anforderung:

Sicherheit eines Systems sollte sich nicht aus der Geheimhaltung der Algorithmen, sondern nur aus den geheimen Schlüsseln ableiten.

Gründe dafür:

- Geheime Schlüssel lassen sich schneller und häufiger austauschen, größere Flexibilität.
- Geheimhaltung funktioniert nicht lange (siehe COMP128 im GSM Mobilfunk, RC4 von RSA), Umstellung auf neue Algorithmen teuer.
- Öffentliche Algorithmen können von unabhängiger Seite untersucht werden. Dies eliminiert Designfehler und baut Vertrauen bei Benutzern bzw. Kunden auf (siehe GSMK Cryptophone).

Prinzip von Kerckhoff

Gründe dagegen:

- Firmen wollen Geschäftsgeheimnisse bewahren.
- Staatliche Behörden wollen einen verbreiteten Gebrauch (z.B. durch Terroristen) des für eigene Zwecke entwickelten und benutzten, vielleicht sehr sicheren Kryptosystems verhindern.

Im allgemeinen wird die Meinung vertreten, daß das Prinzip von Kerckhoff befolgt werden sollte.

17

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Es werden Angreifer (Algorithmen, Programme, Menschen etc.) betrachtet.

Im wesentlichen drei Aspekte:

- Was ist das Ziel eines Angriffs (wann erfolgreich)?
- Welche Informationen stehen dem Angreifer zur Verfügung?
- Welche Rechenleistung besitzt der Angreifer?

Trifft man für diese Aspekte eine Wahl, so legt man sich auf ein Sicherheitsmodell fest.

Gibt es unter den Aspekten keinen Angreifer, so ist das Kryptosystem sicher (im gewählten Modell).

Maximale Sicherheit, wenn Ziele minimal und Informationen maximal.

18

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Ziele eines Angreifers:

- Chiffretext entschlüsseln.
- Chiffretexte bekannten Nachrichten zuordnen.
- Gegebenen Chiffretext in neuen Chiffretext umwandeln, so daß neuer Klartext mit alten Klartext sinnvoll verbunden ist.
- Irgendeinen Chiffretext erzeugen (ohne Klartext zu kennen).

Die korrespondierenden (negierten) Eigenschaften des Verschlüsselungssystems:

- Einweg-Eigenschaft (onewayness, OW).
- Semantische Sicherheit, Nichtunterscheidbarkeit (indistinguishability, IND).
- Nicht-Modifizierbarkeit (non-malleability, NM).
- Plaintext-awareness (PA).

19

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Informationen (Fähigkeiten) des Angreifers in aufsteigender Reihenfolge:

- Ciphertext-only Angriff: Der Angreifer erhält nur Chiffretexte.
- Known-plaintext Angriff: Der Angreifer erhält Klartexte und die zugehörigen Chiffretexte.
- Chosen-plaintext Angriff (CPA): Der Angreifer kann sich die Klartexte aussuchen und erhält die zugehörigen Chiffretexte.

Zusätzlich bei Public-Key Verschlüsselungssystemen:

- Chosen-ciphertext Angriff (CCA1): Der Angreifer kann sich Chiffretexte aussuchen und erhält die zugehörigen Klartexte.

20

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Chosen-plaintext und Chosen-ciphertext Angriffe gibt es auch in adaptiver und kombinierter Form:

Der Angreifer darf Klar- und Chiffretexte in Abhängigkeit zuvor erhaltener Chiffre- bzw. Klartexte und den Ergebnissen von Zwischenrechnungen wählen.

CCA1 wird dann zu CCA2.

21

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Rechenleistung eines Angreifers:

- Vergleichbar der von \mathcal{E} und \mathcal{D} (polynomiell).
- Unbeschränkt.

Die korrespondierenden (negierten) Eigenschaften des Verschlüsselungssystems:

- Komplexitätstheoretische Sicherheit (computational security).
- Perfekte Sicherheit (unconditional security, perfect secrecy).

Im allgemeinen betrachtet man nur komplexitätstheoretische Sicherheit.

22

16. Oktober 2007

Angriffe und Sicherheitsmodelle

Beispiel:

Das für Public-Key Systeme stärkste Sicherheitsmodell ist Nichtunterscheidbarkeit unter einem adaptiven Chosen-ciphertext Angriff (IND-CCA2).

Hier versucht ein Angreifer die Chiffretexte zweier von ihm vorgegebener Nachrichten den Nachrichten zuzuordnen.

Gelingt dies mit Wahrscheinlichkeit signifikant besser als $1/2$, so gilt der Angriff als erfolgreich.

NM ist sicherer als IND ist sicherer als OW.

CCA2 ist sicherer als CCA1 ist sicherer als CPA.

NM-CCA2 = IND-CCA2

(In spezieller Situation: PA ist sicherer als IND-CCA2, NM-CCA2)

23

16. Oktober 2007

Konzepte der Signatur

Nachrichten aus Nachrichtenraum: $m \in M \subseteq A_1^*$.

Signaturen aus Signaturenraum: $\sigma \in S \subseteq A_2^*$.

Schlüssel sind aus Schlüsselräumen: $d \in K_1 \subseteq A_3^*$, $e \in K_2 \subseteq A_4^*$.

Signierungsverfahren $s : K_1 \times M \rightsquigarrow S$.

Verifizierungsverfahren $v : K_2 \times M \times S \rightarrow \{0, 1\}$.

Signatur von Nachricht m mit Schlüssel d : $\sigma \leftarrow s(d, m)$.

Verifizierung von m, σ mit Schlüssel e : $f \leftarrow v(e, m, \sigma)$.

s und v sind effiziente Verfahren (z.B. Programme).

s und v dürfen probabilistisch sein (dürfen den Zufall verwenden).

s kann mehrdeutig sein (\rightsquigarrow).

24

16. Oktober 2007

Symmetrisch

Symmetrisches Signatursystem (secret key, MAC):

- $d = e$ (oder d leicht aus e berechenbar).
- Sender und Empfänger haben e als gemeinsames Geheimnis.
- Gemeinhin als Message Authentication Code (MAC) bezeichnet, meistens deterministisch.

Erweiterte Nachrichten werden verschickt: (m, σ) wo $\sigma \leftarrow S(d, m)$.

Integrität der erweiterten Nachrichten (m, σ) wird von \mathcal{V} mit $S(d, m) = \sigma$ überprüft.

Hashfunktion: MAC ohne geheimen Schlüssel.

Asymmetrisch

(Asymmetrisches, public key) Signatursystem:

- d geheim, e öffentlich.
- d schwer oder gar nicht aus e berechenbar.
- Signierer besitzt e und d .
- Signierer verwendet d zum Signieren.
- Empfänger verwendet e zum Verifizieren.

Angriffe und Sicherheitsmodelle

Das Prinzip von Kerckhoff soll gelten
(vielleicht ein Grund dagegen weniger hier).

Ziele des Angreifers:

- Existentielle Fälschung. Der Angreifer berechnet eine Signatur für eine Nachricht.
- Universelle Fälschung: Der Angreifer kann Signaturen für jede beliebige Nachricht berechnen.
- Total break: Der Angreifer berechnet den geheimen Schlüssel des Signierers.

Angriffe und Sicherheitsmodelle

Informationen (Fähigkeiten) des Angreifers in aufsteigender Reihenfolge:

- Key-only Angriff: Der Angreifer kennt nur den öffentlichen Schlüssel des Signierers.
- Known-Signature Angriff: Der Angreifer erhält Nachrichten und die zugehörigen Signaturen.
- Chosen-Message Angriff: Der Angreifer kann sich die Nachrichten aussuchen und erhält die zugehörigen Signaturen.

Den letzte Variante gibt es auch in adaptiver Form.

Stärkstes Sicherheitsmodell: Sicherheit bezüglich existenzieller Fälschung unter adaptiven Chosen-Message Angriffen.

Verwendung von Hashfunktionen

Hashfunktion $H : M \rightarrow \{0,1\}^*$.

Im allgemeinen wird nur ein Hashwert $H(m)$ und nicht m selbst signiert.

- Effizienter, da $H(m)$ viel kürzer als m ist.
- Beweisbare Sicherheit von in der Praxis relevanten Verfahren (allerdings im Zufallsorakelmodell, RO).

Offenbar muß H kollisionsfrei sein, man kann keine zwei Nachrichten m_1, m_2 mit $H(m_1) = H(m_2)$ berechnen.

Brute-Force (exhaustive search) Angriff

Dieser Angriff kann bei Kryptosystemen mit komplexitätstheoretischer Sicherheit immer ausgeführt werden.

Für Verschlüsselungsverfahren zum Beispiel:

1. Alle Entschlüsselungsschlüssel ausprobieren.
2. Schauen, ob das Entschlüsselte Sinn macht (d.h. Ausnutzen von Redundanz in beispielsweise geschriebener Sprache etc.) oder ob der Schlüssel zu evtl. bekannten Klartext- und Chiffretextpaaren paßt.

Gegenmaßnahme im allgemeinen:

- Ausreichend großen Schlüsselraum haben, somit Aufwand für Angriff groß genug machen.

Bemerkungen

Die meisten heute verwendeten Kryptosysteme sind **unsicher**,

- wenn ein Angreifer unbegrenzte Rechenleistung hat.

Darüberhinaus sind die meisten heute verwendeten Public-Key Verfahren bereits **unsicher**,

- wenn ein Angreifer auch nur gewisse Operationen besonders schnell ausführen kann (Quantencomputer).

Es gibt keine Kryptosysteme mit komplexitätstheoretischer Sicherheit, deren Sicherheit mathematisch bewiesen wurde (dies würde im Endeffekt $P \neq \mathcal{N}P$ implizieren).

Vergleich Public-Key und Secret-Key Kryptographie

Public-Key:

- größere Funktionalität, z.B. Schlüsselaustausch, Signaturen, etc.
- basiert auf mathematischen Problemen (aus der Zahlentheorie).

Secret-Key:

- effizienter in Verschlüsselung (ebenso MAC und Hashfunktionen).

Hybridverfahren:

- Austausch geheimer, sogenannter Sitzungsschlüssel (Session Keys) mittels Public-Key Kryptographie.
- Danach Verwendung symmetrischer Verfahren.

Protokolle

Sind definierte Abfolgen von Kommunikations- und Berechnungsschritten zwischen mindestens zwei Teilnehmern zum Lösen kryptographischer Aufgaben.

Beispiel: Challenge-Response Protokoll zur Identifikation.

- Alice besitzt öffentlichen Schlüssel e und geheimen Schlüssel d eines Signaturverfahrens.
- Bob soll überzeugt werden, daß Alice d kennt, ohne daß d an Bob geschickt wird.

1. Bob wählt zufällige Nachricht m und schickt sie an Alice.
2. Alice schickt Bob ihre Signatur der Nachricht m unter d .
3. Bob ist überzeugt, wenn die Signatur bzgl. e gültig ist.

Protokolle

Eine Angreiferin Eve ohne Kenntnis von d müßte Signaturen von m fälschen, um Bob zu überzeugen.

Angreifer können aktiv oder passiv sein (substitute, replay, insertion attacks).

Sicherheitsbeweis eines Protokolls:

- Mit Hilfe eines Widerspruchs ...
- Man zeigt, daß man mit Hilfe eines Angreifers zugrunde liegende kryptographische Primitive angreifen kann beziehungsweise daß man damit ein zugrundeliegendes, "schwieriges" mathematisches Berechnungsproblem lösen kann.
- Da das Problem aber schwierig ist, kann es keinen Angreifer geben.