Moderne Kryptographie

Eine kurze Einführung im Rahmen des Proseminars Theoretische Informatik

William Gu, WS14/15

Definition 1. Als ein **Verschlüsselungsverfahren** bezeichnet man ein 5-Tupel der Form $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D)$, wobei gilt:

$\mathcal{P}$ der Klartextraum, $\mathcal{C}$ der Chiffreraum, $\mathcal{K}$ der Schluesselraum,
$E : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ die Verschlüsselungsfunktion und
$D : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$ die Entschlüsselungsfunktion ist.
$\forall k \in \mathcal{K}, m \in \mathcal{P} : D(E(m, k), k) = m$

1 Symmetrische Verfahren

1.1 Historische Chiffriersysteme

Zwei relativ bekannte Chiffren aus der Historie sind zum einen das Caesarchiffre als Beispiel einer monoalphabetischen Substitution.

Zum anderen ist es das Vigenèrechiffre als Beispiel für eine polyalphabetische Substitution, das lange Zeit als „unknackbar“ galt. Das Vigenèrechiffre nutzt das „tabula recta“ und ist eine abgewandelte Mehrfachanwendung des Caesarchiffres.

1.2 Blockchiffren

Definition 2. Unter einer **Blockchiffre** versteht man ein Verschlüsselungsverfahren, wo Klartext- und Schlüsseltextraum die Menge Σ^n aller Wörter der Länge n über dem Alphabet Σ ist. Für ein einzelnes Zeichen, also $n = 1$, nennt man das Chiffre auch Substitutionschiffre.

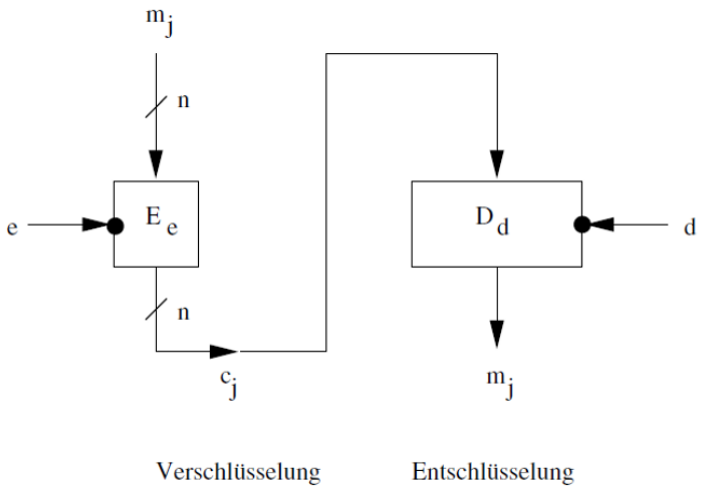

Abbildung 1: Verschlüsselungsmodi der Blockchiffren: ECB (*electronic codebook mode*)

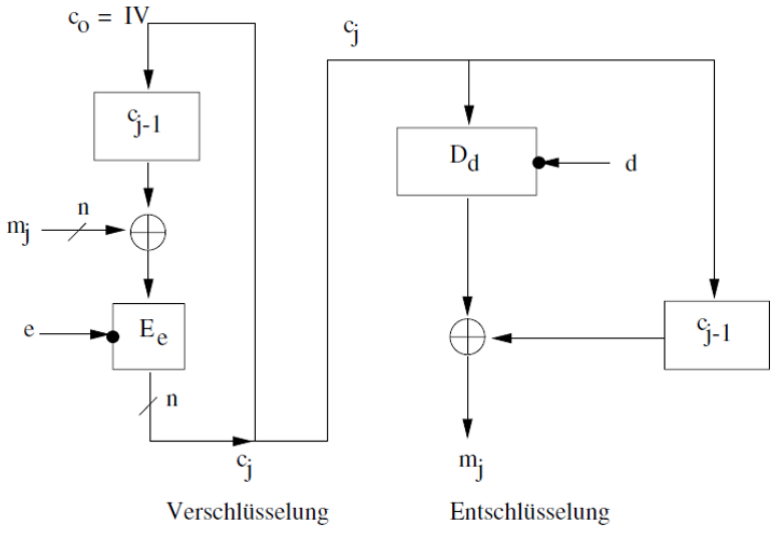

Abbildung 2: Verschlüsselungsmodi der Blockchiffren: CBC (*cipherblock chaining mode*)

2 Public-key Kryptosysteme

Um den Begriff *computationally secure* zu erfassen, benötigen wir ein passendes Rechenmodell:

Definition 3. Eine **probabilistische TM** (PTM) M ist eine NTM, wobei jeder nichtdeterministische Berechnungsschritt *coin-flip step* genannt wird und genau zwei gültige Bewegungen hat.

Jedem Berechnungslauf b wird bei Eingabe $w \in \Sigma^*$ die folgende Wahrscheinlichkeit zugewiesen:

$$\Pr(b) = 2^{-k}$$

Demnach ergibt sich aus der Summenregel der Wahrscheinlichkeitstheorie für die Definition der Wortakzeptanz:

$$\Pr(M \text{ akzeptiert } w) = \sum_{b \text{ akzeptierend}} \Pr(b)$$

M akzeptiert $L \subseteq \Sigma^*$ mit Fehlerrate $\epsilon \Leftrightarrow w \in L \Rightarrow \Pr(M \text{ akzeptiert } w) \geq 1 - \epsilon \wedge w \notin L \Rightarrow \Pr(M \text{ verwirft } w) \geq 1 - \epsilon$.

Die Komplexitätsklasse BPP (*engl. bounded-error probabilistic polynomial time*) stellt die Klasse derjenigen Sprachen da, die von einer PTM mit Fehlerrate $\epsilon = \frac{1}{3}$ akzeptiert werden:

$$\forall w \in L : \Pr(M \text{ akzeptiert } w) \geq \frac{2}{3}$$

Durch die Nachteile eines symmetrischen Kryptosystems motiviert, fingen Mitte des 20.Jahrhunderts Wissenschaftler an, nach einer Alternative zu forschen. Das Schlüsseltauschverfahren von Diffie-Hellman war eines der ersten Publikationen zur Public-key Kryptographie. Es zeigte erstmals, wie es möglich ist, geheime Schlüssel über unsichere Kanäle zu tauschen ohne eine vorherige geheime Absprache benötigt wird.

2.1 Einweg- und Falltürfunktionen

Mathematische Grundlage eines solchen Public-key bzw.*asymmetrischen* Kryptosystems bilden spezielle Funktionen, die sogenannten Einwegfunktionen.

Definition 4. Eine Funktion der Form $f : \Sigma^* \to \Sigma^*$ bezeichnet man als **längenerhaltend**, falls gilt:

$$\forall w \in \Sigma^* : |w| = |f(w)|$$

Definition 5. Sei M nun eine PTM. Eine längenerhaltende Funktion f wird als **Einwegfunktion** bezeichnet, falls gilt:

1. f ist in polynomieller Zeit berechenbar *(einfach berechenbar)*
2. $\forall M, k \exists$ genügend großes n : $\Pr(M(f(w)) = y \text{ mit } f(w) = f(y)) \leq n^{-k}$ (*schwer* zu invertieren)

Definition 6. Sei $\{f_i\}$ eine Familie von Funktionen mit $i \in \Sigma^*$ und die Funktionen seien

$$f_i(w) = f(i, w) \quad \forall i, w \in \Sigma^*$$

dann wird die Funktion $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ eine **Indizierungsfunktion** genannt. Sie ist längenerhaltend, wenn alle Funktionen in der Familie längenerhaltend sind.

Sei f im folgenden eine längenerhaltende Indizierungsfunktion, $h : \Sigma^* \times \Sigma^* \to \Sigma^*$ eine Hilfsfunktion und G eine PTM, dann wird f als eine **Falltürfunktion** (*engl. trapdoor function*) bezeichnet, falls gilt:

1. f, h sind in polynomieller Zeit berechenbar
2. Für ein zufälliges $w \in \Sigma^*$ und E als PTM gilt:

   $$\forall E, k \exists \text{ genügend großes } n : \Pr(E(i, f_i(w)) = y \text{ mit } f_i(y) = f_i(w)) \leq n^{-k}$$

   Hierbei dient G als ein Generator, der die Tupel (i, t) ausgibt.
3. Für alle Ausgaben (i, t) von G, die mit einer Wahrscheinlichkeit > 0 auftreten, gilt:

   $$\forall n, w \text{ mit } |w| = n : h(t, f_i(w)) = y \text{ mit } f_i(y) = f_i(w)$$

2.2 RSA-Kryptosystem

Unter dem Titel *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* veröffentlichten R. Rivest, A. Shamir und L. Adleman 1978 erstmals ein konkretes Public-key Verfahren. Hat man

---

1: **function** RSAKEY( )
2: $p \leftarrow$ gen( ), $q \leftarrow$ gen( ) ▷ generiere zwei zufällige Primzahlen
3: $N \leftarrow pq$ ▷ RSA-Modul
4: wähle eine kleinere Zahl $1 < e < \varphi(N)$, die relativ prim zu $\varphi(N)$ ist ▷ e ist stets ungerade
5: $d \leftarrow e^{-1}$ als multiplikative Inverse von e: $de \equiv 1 \mod \varphi(N)$
6: **return** $P = (e, N)$ als **öffentlicher Schlüssel** und $S = (d, N)$ als **privaten Schlüssel**

---

nun ein Schlüsselpaar generiert, so kann man über die folgende Gleichung verschlüsseln

$$E = f(w, (e, N)) = w^e \mod N$$

bzw. über die folgende Funktion wiederum entschlüsseln:

$$D = h(x, (d, N)) = x^d \mod N$$

Wieso funktioniert dieser Algorithmus? Jedes Verschlüsselungsverfahren muss korrekt ver- und dann auch wieder entschlüsseln können.

Satz (Korrektheit von RSA)**.**

$$\forall w \in \mathbb{Z}_n : D(E(w, (e, N)), (d, N)) = w^{ed} \mod N = w$$

Beweis. Für den Beweis dieses Satzes verwenden wir Sätze aus der Zahlentheorie, u.a. den chinesischen Restsatz (CRT) und den kleinen Satz von Fermat:
z.z.: $D(E(w,(e,N)),(d,N)) = (w^e \mod N)^d \mod N = w^{ed} \mod N = w$.

Die zentrale Kongruenzgleichung in der RSA-Schlüsselgenerierung sagt uns

$$de \equiv 1 \mod \varphi(N) \Leftrightarrow ed \equiv 1 \mod (p-1)(q-1) \Leftrightarrow ed \equiv 1 + k(p-1)(q-1)$$

d.h. also für w^{ed} gilt:

$$w^{ed} \mod N \equiv w^{1+k(p-1)(q-1)} \mod N$$

Aufgrund von $N = pq$ müssen wir jeweils eine Gleichung $\mod p$ und $\mod q$ betrachten - hier beispielhaft nur mit p:

$$\begin{aligned} w^{ed} &\equiv w(w^{p-1})^{k(q-1)} \mod p \\ &\equiv w(w^{p-1} \mod p)^{k(q-1)} \mod p \\ &\equiv w(1)^{k(q-1)} \mod p \qquad \text{wegen Fermat} \\ &\equiv w \mod p \end{aligned}$$

Da für q dies hier analog gilt, haben wir jetzt gezeigt, dass $w^{ed} \equiv w \mod p \wedge w^{ed} \equiv w \mod q$ und nach dem CRT gilt jetzt $w^{ed} \equiv w \mod N$. □

RSAP bezeichne hier das Problem aus einem gegebenen öffentlichen Schlüssel und einem Chiffretext den Klartext wieder zu entschlüsseln. RSAP* wiederum das Problem, aus dem öffentlichen Schlüssel den privaten Schlüssel über $de \equiv 1 \mod \varphi(N)$ zu berechnen. FACT sei das Faktorisierungsproblem der Zahlentheorie. Die Sicherheit des RSA-Verfahrens beruht darauf, dass man zeigen kann: Es ist genauso schwer, den privaten Schlüssel aus dem öffentlichen Schlüssel zu generieren, wie das RSA-Modul zu faktorisieren:

$$\text{RSAP} \leq_p \text{RSAP}^* =_p \text{FACT}$$

Literatur

[1] Johannes Buchmann: *Einführung in die Kryptographie*, 2010, Springer-Verlag.

[2] Thomas H. Cormen et al.: *Introduction to Algorithms*, 2009, MIT Press.

[3] Gerd Fischer: *Lehrbuch der Algebra*, 2013, Springer Spektrum.

[4] Jonathan Katz, Yehuda Lindell: *Introduction to Modern Cryptography*, 2008, Chapman & Hall.

[5] Michael Sipser: *Introduction to the Theory of Computation*, 2012, Cengage Learning.

[6] Angelika Steger: *Diskrete Strukturen - Band 1: Kombinatorik, Graphentheorie, Algebra.*, 2007, Springer.