

Kryptographie

Boyan Hristov

29. Januar 2018

Claudia Dieckmann

Zusammenfassung

Wir werden einige Konzepte einführen, die man als die Grundbausteine der Kryptographie betrachtet. Wir werden dabei sehen, unter welchen Annahmen sichere Kryptographie existieren kann. Weiter wird der Zusammenhang mit den Klassen P und NP erläutert, als auch werden einigen interessanten Schlussfolgerungen gemacht. Am Ende werden wir auch die Funktion hinter den berühmten RSA Algorithmus sehen.

1 Motivation

1.1 Secret Codes & One-way Pads

Die naive Methode verschlüsselte Konversation zu haben ist, wenn Sender und Empfänger der gleiche Schlüssel benutzen, um Nachrichten zu verschlüsseln und entschlüsseln. Dabei existiert das Problem, dass Sender und Empfänger sich auf einen Schlüssel einigen müssen. Das ist aber schwierig, da bevor sie das gemacht haben, können sie auch keine sicheren Nachrichten zwischen einander senden. Weiter ist das keine gute Lösung, da für je Gesprächspaar ein Schlüssel existieren muss, d.h. wenn jemand mit vielen Leuten verschlüsselte Nachrichten austauschen will, muss diese Person auch viele Schlüssel speichern.

Laut Theorie ist ein Schlüssel nur dann sicher, wenn er mindestens so lang ist wie alle Nachrichten, die damit verschlüsselt werden sollen. Deswegen sind die sogenannte “One-way Pads” entstanden. Dabei wird je Nachricht mit einem Teil des Schlüssels verschlüsselt und dieses Teil wird nachher gelöscht. So garantiert man, dass ein Schlüssel durch “Brute-Force” schwierig zu finden ist. Wie wir aber später sehen werden, reicht es auch wenn der Schlüssel relativ lang ist, solange es keine andere Methode außer Brute-Force gibt, den Schlüssel leichter zu finden.

So kommen wir zu den Konzepten der sicheren Hashfunktionen und der asymmetrischen Verschlüsselung, wobei eine Nachricht mit einem Schlüssel verschlüsselt wird und mit einem anderen entschlüsselt.

1.2 Ziele der Public-Key Kryptosysteme

Hier werden wir einige Notationen einführen.

- $M \in \Sigma^*$ - eine Nachricht
- $E : \Sigma^* \rightarrow \Sigma^*$ - Funktion, die eine Nachricht verschlüsselt
- $D : \Sigma^* \rightarrow \Sigma^*$ - Funktion, die eine Nachricht entschlüsselt

Jedes “Public-Key“ Kryptosystem muss die folgenden Eigenschaften haben. Wir werden später sehen, was für Annahmen gemacht werden müssen, um diese Eigenschaften zu sichern.

1. E und D sind Polynomialzeit berechenbar
2. Man muss die originelle von verschlüsselten Nachrichten generieren können und zwar mit dem Gegenschlüssel.
Formal: $D(E(M)) = M$
3. Mann muss eine Nachricht erstmal entschlüsseln und dann verschlüsseln können, wobei wieder die originelle Nachricht entsteht.
Formal: $E(D(M)) = M$
4. Wenn ein Nutzer E veröffentlicht, veröffentlicht er damit nicht D und auch kein Weg, D leichter (in polynomialer Zeit) zu berechnen

2 Erinnerung

Die meisten Leser können dieses Teil überspringen, es ist aber wichtig zu verstehen, was links- und rechtsinvertierbarkeit bedeuten und welche Folgen diese für die Kryptographie haben.

2.1 Injektivität

Definition 2.1. Eine Funktion $f : X \rightarrow Y$ ist injektiv
 $\Leftrightarrow (f(a) = f(b) \Leftrightarrow a = b)$

2.2 Surjektivität

Definition 2.2. Eine Funktion $f : X \longrightarrow Y$ ist surjektiv
 $\Leftrightarrow \forall y \in Y \exists x \in X : f(x) = y$

2.3 Linksinvertierbarkeit

Hier ist I die Identitätsfunktion und \circ die Verkettung von Funktionen.

Definition 2.3. Eine Funktion $f : X \longrightarrow Y$ ist linksinvertierbar
 $\Leftrightarrow \exists g : Y \longrightarrow X : g \circ f = I_x$
 $\Leftrightarrow f$ ist injektiv

2.4 Rechtsinvertierbarkeit

Hier ist I die Identitätsfunktion und \circ die Verkettung von Funktionen.

Definition 2.4. Eine Funktion $f : X \longrightarrow Y$ ist rechtsinvertierbar
 $\Leftrightarrow \exists g : Y \longrightarrow X : f \circ g = I_x$
 $\Leftrightarrow f$ ist surjektiv

3 One way functions (Einwegfunktionen)

In diesem Abschnitt werden die Einwegfunktionen in starke und schwache unterteilt. Es wird auch gezeigt, dass die Existenz von schwachen Einwegfunktionen diese von starken impliziert. Weiter werden wir sehen, dass eine längenerhaltende Funktion aus einer nicht längenerhaltenden konstruiert werden kann. Die starken Einwegfunktionen sind ein grundlegender Baustein für die Kryptographie, Ziel ist aber hier auch alle Annahmen zu verstehen, die dazu führen.

Da die meisten Definitionen auf probabilistische Algorithmen basieren, werden wir erstmal definieren, was vernachlässigbare Erfolgswahrscheinlichkeit bedeutet, um besser die folgenden Konzepte erklären zu können.

3.1 Vernachlässigbare Erfolgswahrscheinlichkeit

Definition 3.1. Vernachlässigbare Erfolgswahrscheinlichkeit

- Funktion abhängig von der Eingabegröße
- Die Erfolgswahrscheinlichkeit eines Algorithmus ist genau dann vernachlässigbar, wenn es eine asymptotische obere Schranke gibt, die polynomial ist

- D.h, auch wenn man polynomial lange den Algorithmus wiederholt, ist die Erfolgswahrscheinlichkeit immer noch vernachlässig
- Damit ist vernachlässige Erfolgswahrscheinlichkeit \equiv nicht Polynomialzeit berechenbar mit einer nicht vernachlässigen Erfolgswahrscheinlichkeit

3.2 Starke und Schwache Einwegfunktionen

Definition 3.2. Eine Funktion $f : 0, 1^* \rightarrow 0, 1^*$ ist eine starke one-way Funktion \Leftrightarrow

1. f ist Polynomialzeit berechenbar
2. Für jeden in polynomialer Zeit berechenbaren Algorithmus A , für jedes Polynom p und für große n gilt:

$$\Pr(A(f(w), 1^n) \in f^{-1}(f(w))) \leq \frac{1}{p(n)}$$

Damit hat A per Definition eine vernachlässigbare Erfolgswahrscheinlichkeit. 1^n wird als Parameter übergeben um zu garantieren, dass die inverse Funktion echt Polynomialzeit unberechenbar ist. Wenn man das weglässt, könnte es sein, dass die Eingabegröße von f exponentiell größer ist als die Ausgabegröße und damit f nur deswegen nicht invertierbar ist, weil kein Algorithmus in polynomialer Zeit das Ergebnis auf dem Band schreiben kann.

Definition 3.3. Eine Funktion $f : 0, 1^* \rightarrow 0, 1^*$ ist eine schwache one-way Funktion \Leftrightarrow

1. f ist Polynomialzeit berechenbar
2. Es existiert ein Polynom p , so dass für alle polynomialzeit berechenbare Algorithmen A und große n :

$$\Pr(A(f(w), 1^n) \notin f^{-1}f(w)) > \frac{1}{p(n)}$$

Merke, dass f invertierbar sein kann, nur nicht in polynomialer Zeit. Weiter steht in der Definition nicht fest, ob f injektiv oder surjektiv ist, da hier f nicht unbedingt in mathematischem Sinne invertierbar ist. D.h. auch $f(x) = 2$ ist laut dieser Definition keine Einwegfunktion, da $g(x) = 1$ schon als zu f inverse Funktion gilt. Surjektivität werden wir für "Public-Key" Kryptosysteme auf jeden Fall brauchen. Ohne Injektivität kann man schon eine Hashingfunktion erstellen (es existieren viele solche), aber keine mathematisch sichere, da mehrere unterschiedliche $w \in \Sigma^*$ dieselbe Hashwerte bekommen werden.

Hoffnung für sichere Hashfunktionen gibt es erst mit den Einwegpermutationen, die wir bald sehen werden. Bevor müssen wir aber auch die längenerhaltende Funktionen einführen, die in der Praxis ganz hilfreich sind.

Satz 3.4. *Es existiert eine schwache Einwegfunktion \Leftrightarrow eine starke Einwegfunktion existiert.*

Beweis. Der Beweis dafür ist ziemlich lang und kompliziert, deswegen werden wir hier nur die Schema erläutern. In dem Buch von Oded Goldreich “Foundations of Cryptography - Basic Tools“ kann man im Abschnitt 2.3.2 den vollständigen Beweis finden.

Die Idee ist aus einer schwachen Einwegfunktion f , eine starke Einwegfunktion g folgendermaßen zu konstruieren.

$g(x_1, \dots, x_{t(n)}) = f(x_1), \dots, f(x_{t(n)})$, wobei $|x_1| = |x_{t(n)}|$ und $t(n) = n \cdot p(n)$. Also $n^2 p(n)$ -bit lange Eingabe wird in n Blöcke je mit Länge $t(n)$.

Der Rest des Beweises nimmt an, dass g keine starke Einwegfunktion ist und konstruiert daraus ein Algorithmus, der f in polynomialer Zeit mit vernachlässigbare Fehlerwahrscheinlichkeit invertiert, woraus der Widerspruch entsteht.

Der Beweis ist so konstruiert, da man nicht sicher sein kann, dass ein solcher Algorithmus jeden Block einzeln invertieren wird, was in einer maximalen Erfolgswahrscheinlichkeit von $(1 - \frac{1}{p(n)})^{np(n)}$ resultieren würden. Das zeigt, dass Verstärkung von der Komplexität einer Aufgabe deutlich schwieriger ist als probabilistische Verstärkung. \square

3.3 Längenerhaltende Funktionen

Definition 3.5. Eine Funktion $f : \Sigma^* \rightarrow \Sigma^*$ ist längenerhaltend $\Leftrightarrow \forall w \in \Sigma^* : |f(w)| = |w|$

Satz 3.6. *Wenn eine Einwegfunktion existiert, dann existiert auch eine längenerhaltende Einwegfunktion*

Beweis. Sei $f : \Sigma^* \rightarrow \Sigma^*$ eine starke Einwegfunktion. Da f Polynomialzeit berechenbar ist $\Rightarrow \forall x \in \Sigma^* : |f(x)| \leq p(|x|)$, d.h. die Länge von jeder Abbildung von f ist polynomial in der Länge begrenzt.

Wir konstruieren $g : \Sigma^* \rightarrow \Sigma^*$ und $h : \Sigma^* \rightarrow \Sigma^*$.

$g(x) \stackrel{\text{def}}{=} f(x) 10^{p(|x|) - |f(x)|}$.

Damit haben wir festgelegt, dass jede Abbildung von g die maximale Länge von allen Abbildungen von f haben wird.

$h(x'x'') =_{\text{def}} g(x')$, wobei $|x'x''| = p(|x'|) + 1$.

Damit konstruieren wir h so, dass je Eingabe die gleiche Länge hat. Die Eingabemenge wird wieder künstlich gefüllt, die letzte Zeichen werden aber ignoriert.

Damit ist trivialerweise h eine längenerhaltende Funktion. Jetzt müssen wir nur zeigen, dass diese auch eine starke Einwegfunktion ist. Der Beweis per Widerspruch folgt.

Sei B ein Algorithmus, dass g in polynomialer Zeit mit unvernachlässigbare Erfolgswahrscheinlichkeit invertiert. Wir konstruieren den Algorithmus A , der f in polynomialer Zeit invertiert.

Bei Eingabe $(y, 1^n)$ hält dann A mit Ausgabe $B(y10^{p(n)-|y|}, 1^{p(n)+1})$.

Damit haben wir gezeigt, dass $B \geq_p A$. Widerspruch, da A in polynomialer Zeit nur mit vernachlässigbare Erfolgswahrscheinlichkeit terminiert.

Analog für h . □

4 One-way Permutationen

Hier wurde die Definition aus “Introduction to the Theory of Computation“ von Michael Sipser benutzt, jedoch etwas angepasst, damit die Konvention weiter ähnlich bleibt.

Definition 4.1. Eine Funktion $f : \Sigma^* \rightarrow \Sigma^*$ ist eine Einwegpermutation \Leftrightarrow

1. f ist eine längenerhaltende Permutation
2. f ist Polynomialzeit berechenbar
3. Für alle probabilistische Algorithmen A , $\forall k \in \mathbb{N}^+$ und für große n , wählen wir ein Wort w mit $|w| = n$ und führen A mit Eingabe w aus
 $Pr_{A,w}(A(f(w)) = w) \leq n^{-k}$

Hier wurde auch die Definition einer starken Einwegpermutation benutzt. $Pr_{A,w}$ notiert die Wahrscheinlichkeit über die beliebige Wahl von w als auch die Münzwürfe von A . Wie würde diese einer schwachen aussehen?

4.1 Bedeutung

Die starke längenerhaltende Einwegpermutationen sind der Grundbaustein der Kryptographie. Wenn solche existieren, kann man sichere Hashingalgorithmen erstellen. Mit solchen werden heutzutage z.B. die Passwörter hashiert, bevor diese in einem Datenbanksystem gespeichert werden. So kann jedes mal das System das von Nutzer eingegebenes Passwort hashieren und mit dem gespeicherten vergleichen. Wenn jemand die Passwörter aus dem Datenbank sehen kann, kann dieser nie die originelle Klartextpasswörter von diesen erstellen.

5 Trapdoor Functions (Falltürfunktionen)

Definition 5.1. Eine Funktion $f : \Sigma^* \rightarrow \Sigma^*$ ist eine indexierte Funktion, für die ein probabilistischer Polynomialzeit Algorithmus A existiert, und eine zu f inverse Funktion $h : \Sigma^* \rightarrow \Sigma^*$. Hier ist A der Algorithmus, der f , h , i und t liefert. A' ist der Algorithmus, der versucht, f zu invertieren. Dabei müssen f , g und h die folgenden Eigenschaften haben.

1. f und h sind Polynomialzeit berechenbar
2. Für alle probabilistische Algorithmen A' , $\forall k \in \mathbb{N}^+$ und für große n , wählen wir eine beliebige Rückgabe (i, t) von A bei Eingabe $(w \in \Sigma^n, 1^n)$
$$\Pr(A'(i, f_i(w)) = y | f_i(y) = f_i(w)) \leq n^{-k}$$
3. $\forall n, \forall w \in \Sigma^n$, für je Rückgabepaar (i, t) von A , dass mit nichtvernachlässigbarer Wahrscheinlichkeit vorkommt, gilt:
$$h(t, f_i(w)) = y, \text{ wobei } f_i(y) = f_i(w)$$

Hier ist t das Geheimnis, womit f leicht invertierbar ist. Die zweite Eigenschaft sagt, dass f ohne t schwer invertierbar ist und die dritte, dass f mit Hilfe von t leicht invertierbar ist und h die entsprechende inverse Funktion ist.

5.1 Bedeutung

Das ist schon alles, was wir brauchen, um ein "Public-Key" Kryptosystem zu konstruieren. Die Funktion f_i können wir veröffentlichen, das wird unser öffentliches Schlüssel sein. Die Funktion h bzw. das Geheimnis t werden wir für uns behalten.

6 Beispiel

6.1 Konstruktion der Trapdoor Funktion hinter RSA

1. Wähle 2 (echt) große Primzahlen p und q
2. Berechne $N = pq$
3. Berechne $\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$
4. Wähle $\phi(N) < e < N$ zufällig, so dass es semiprim zu $\phi(N)$ ist. Je Primzahl $> \phi(N)$ ist möglich.
5. Berechne d , so dass $ed \equiv 1 \pmod{\phi(N)}$. Das ist immer möglich, da alle Zahlen zwischen 1 und $\phi(N)$ formen eine Gruppe, die abgeschlossen bezüglich Multiplikation Modulo $\phi(N)$ ist. Dazu bietet sich das euclidische Algorithmus für die Suche nach $GGT(\phi(N), e)$.

6.2 Anwendung von RSA

Aus dem oben beschriebenen Algorithmus werden wir e und N veröffentlichen und d für uns behalten. Damit gilt:

- $E(M) = M^e \pmod{N}$
- $D(M) = M^d \pmod{N}$
- Damit $D(E(M)) = (M^e \pmod{N})^d \pmod{N} = M^{ed} \pmod{N} = M$
- Und $E(D(M)) = M^{ed} \pmod{N} = M$ analog

So können wir Nachrichten beides verschlüsseln (mit dem öffentlichen Schlüssel von jemandem, nur diese Person kann das öffnen), oder signieren, wobei wir eine Nachricht mit unserem privaten Schlüssel verschlüsseln. Wenn die Nachricht sich mit unserem öffentlichen Schlüssel sich entschlüsseln lässt, dann wurde diese sicherlich mit unserem privaten Schlüssel verschlüsselt und wurde damit sicherlich von uns geschrieben.

7 Konsequenzen von der Existenz der Einwegfunktionen

Obwohl es eine starke Vermutung gibt, dass $P \neq NP$, macht es immer Sinn nachzudenken, was für Bedeutung $P = NP$ für die Kryptographie hat, bzw. wie sicher wir sind, wenn $P \neq NP$ bewiesen wird.

Satz 7.1. $P = NP \Rightarrow$ es existieren keine Einwegfunktionen

Beweis. Sei $f : \Sigma^* \rightarrow \Sigma^*$, $\Sigma = 0, 1$, eine Einwegfunktion.

Sei L eine Sprache von Paaren, so dass $(x^*, y) \in L \Leftrightarrow \exists x : f(x) = y$ und x^* ist ein Präfix von x .

$L \in NP$, da bei einer Eingabe (x^*, y) und Zeugen (x, y) können wir in polynomialer Zeit überprüfen, ob $f(x) = y$ (da f Polynomialzeit berechenbar ist, nach der Definition einer Einwegfunktion) und ob x^* ein Präfix von x ist.

Da aber nach Annahme $P = NP \Rightarrow L \in P$. Sei A das Algorithmus, dass L in polynomialer Zeit entscheidet. Damit können wir L benutzen um f in polynomialer Zeit zu invertieren, also um aus je Ausgabe y das entsprechende Eingabewert x zu generieren.

Wir fangen mit (ϵ, y) . Dann raten wir das nächste Zeichen von x und benutzen A um zu überprüfen, ob wir richtig geraten haben. Da A in polynomialer Zeit läuft, haben wir am Ende eine Laufzeit von $O(|y|p)$, wobei p ein Polynom ist. Damit haben wir in polynomialer Zeit f invertiert, deswegen ist per Definition f keine Einwegfunktion. Widerspruch! \square

8 Literatur

- Introduction To The Theory Of Computation, Michael Sipser
- Foundations of Cryptography - Basic Tools, Oded Goldreich
- <https://crypto.stackexchange.com/questions/39878/how-to-show-that-a-one-way-function-proves-that-p>
 - Beweis für $P = NP \Rightarrow$ Einwegfunktionen existieren nicht
- Construct a length preserving one way function, Stackexchange
 - <https://cs.stackexchange.com/questions/10639/length-preserving-one-way-functions>
 - Oben wurde den Beweis von Oded Goldreich benutzt, das war aber für das Verständniss hilfreich
- A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir, und L. Adleman
 - Wie die Namen der Autoren schon zeigt, ist das das Paper zu RSA

- https://en.wikipedia.org/wiki/One-way_function