

2.5 Iterationsangriff

Sei allgemein $E: M \rightarrow M$ eine bijektive Abbildung der endlichen Menge M und $D = E^{-1}$ die Umkehrabbildung; wir stellen uns E als Verschlüsselungsfunktion vor.

Dann ist E in der Permutationsgruppe $\mathfrak{S}(M)$ enthalten, die die (riesige) Ordnung $\#\mathfrak{S}(M) = (\#M)!$ hat. Immerhin ist sie endlich, und somit gibt es ein $s \in \mathbb{N}_1$ mit $E^s = \mathbf{1}_M$, also

$$D = E^{s-1}.$$

Also ist D aus E bestimmbar durch hinreichend häufige Iteration – ein Angriff, der natürlich nur für asymmetrische Verfahren relevant ist. Um sich davor zu schützen, muss man *die Ordnung von E – das kleinste $s \geq 1$ mit $E^s = \mathbf{1}_M$ – möglichst groß wählen.*

Das Beispiel RSA

Hier ist $M = C = \mathbb{Z}/n\mathbb{Z}$, also $\#\mathfrak{S}(M) = n!$, wobei n schon eine sehr große Zahl ist, so dass noch nicht unmittelbar eine Gefahr zu sehen ist – der Angreifer könnte zwar $E^{n!-1}$ bilden, aber das wird er selbst mit dem effizientesten Potenzalgorithmus in diesem Universum nicht schaffen.

Allerdings sind die RSA-Verschlüsselungsfunktionen in einer wesentlich kleineren Untergruppe von $\mathfrak{S}(M)$ enthalten – deren Ordnung der Angreifer glücklicherweise nicht kennt:

Um das herzuleiten, betrachten wir die Abbildung

$$\Phi: \mathbb{N} \rightarrow \text{Abb}(M, M), \quad e \mapsto E_e \quad \text{mit} \quad E_e(a) = a^e \pmod n.$$

Sie hat die folgenden Eigenschaften:

Bemerkungen

1. Für $e, f \in \mathbb{N}$ ist $E_{ef} = E_e \circ E_f$, weil $a^{ef} \equiv (a^f)^e \pmod n$ für alle $a \in M$. Also ist Φ Homomorphismus der multiplikativen Halbgruppe \mathbb{N} .
2. Ist $e \equiv f \pmod{\lambda(n)}$, so ist $E_e = E_f$: Wenn $f = e + k\lambda(n)$, folgt $a^f = a^{e+k\lambda(n)} \equiv a^e \pmod n$ für alle $a \in M$.
3. Ist $e \pmod{\lambda(n)}$ invertierbar, so ist E_e bijektiv: Ist $de \equiv 1 \pmod{\lambda(n)}$, so $E_d \circ E_e = E_1 = \mathbf{1}_M$. Also ist die von Φ induzierte Abbildung,

$$\bar{\Phi}: \mathbb{M}_{\lambda(n)} \rightarrow \mathfrak{S}(M),$$

ein Gruppen-Homomorphismus.

4. $\bar{\Phi}$ ist injektiv: Ist nämlich $\Phi(e) = E_e = \mathbf{1}_M$, so ist $a^e \equiv a \pmod{n}$ für alle $a \in M$, also $a^{e-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{M}_n$, also $\lambda(n) | e - 1$, also $e \equiv 1 \pmod{\lambda(n)}$.

Damit ist bewiesen:

Satz 2 Die RSA-Verschlüsselungsfunktionen E_e bilden eine zu $\mathbb{M}_{\lambda(n)}$ isomorphe Untergruppe $H \leq \mathfrak{S}(M)$ von der Ordnung $\varphi(\lambda(n))$ und vom Exponenten $\lambda(\lambda(n))$.

Die Ordnung einer einzelnen Verschlüsselungsfunktion E_e kann natürlich noch viel kleiner sein; die zyklische Untergruppe $\langle e \rangle \leq \mathbb{M}_{\lambda(n)}$ hat die Ordnung $s := \text{Ord}(e) | \lambda(\lambda(n))$.

Damit sind wir auf folgende Probleme gestossen:

1. Wie groß ist $\lambda(\lambda(n))$?

Antwort (ohne Beweis): „Im allgemeinen“ ist $\lambda(\lambda(n)) \approx \frac{n}{8}$.

Will man sich dessen sicher sein, wählt man p, q speziell, d. h., $p = 2p' + 1$, $q = 2q' + 1$ mit verschiedenen Primzahlen $p', q' \geq 3$. (Solche Primzahlen p', q' heißen **GERMAIN-Primzahlen** nach Sophie GERMAIN, die durch Betrachtung dieser Zahlen einen wesentlichen Fortschritt für das FERMAT-Problem erzielt hatte.) Für $n = pq$ ist dann

$$\lambda(n) = \text{kgV}(2p', 2q') = 2p'q' \approx \frac{n}{2}.$$

Sind weiterhin auch $p' = 2p'' + 1$ und $q' = 2q'' + 1$ speziell, so ist

$$\lambda(\lambda(n)) = 2p''q'' \approx \frac{n}{8}.$$

Der Primzahlsatz lässt erwarten, dass es auch solche Zahlen noch in astronomischen Mengen gibt.

2. Wann ist $\text{Ord}(e) = \lambda(\lambda(n))$? Oder nicht wesentlich kleiner?

Antwort: meistens. (Auch hier existiert eine mathematische Analyse.)

Als Folgerung kann man festhalten: *Bis auf vernachlässigbar unwahrscheinliche Ausnahmen ist s von der gleichen Größenordnung wie n .* Die besten bekannten Ergebnisse dazu finden sich im Kapitel 23 des Buchs von SHPARLINSKI, siehe das Literaturverzeichnis der Vorlesung.

Ergänzend zu Abschnitt 2.2 lässt sich jetzt die Aufgabe

(F) Finden der Ordnung s der Verschlüsselungsfunktion hinzufügen. Es gilt die Komplexitätstheoretische Implikation

$$(F) \longrightarrow (A)$$

(wenn die Ordnung s bekannt ist, ist $D = E^{s-1}$ und daher auch $d = e^{s-1}$ bekannt), aber vielleicht nicht die Umkehrung. *Die Ordnung der Verschlüsselungsfunktion zu finden, ist mindestens so schwierig das Faktorisieren des Moduls.*