Diffie–Hellman-Problem
Unter welchen Voraussetzungen ist das Diffie–Hellman-Problem besonders schwer zu lösen?

19. September 2021

SEMINAR ZAHLENTHEORIE AN DER UNIVERSITÄT KONSTANZ BEI
PROF. DR. SALMA KUHLMANN
AUTORIN: TAMARA EDINBOROUGH
DATUM DES VORTRAGS: 07.07.2021

SUPERVISOR
MICHELE SERRA

Abstract

Dieser Vortrag thematisiert das Diffie–Hellman-Problem und setzt sich mit der Leitfrage auseinander, unter welchen Voraussetzungen dieses Problem besonders schwer zu lösen ist. Dazu gehen wir auf ein paar Grundlagen der Kryptographie, wie z.B. die Einwegfunktionen, ein. Außerdem definieren wir das diskrete Logarithmus-Problem, welches in vielen Kryptoverfahren für das Ver- und Entschlüsseln von Nachrichten genutzt wird. Danach schauen wir uns das Diffie–Hellman-Verfahren an und betrachten, wie das diskrete Logarithmus Problem bei diesem Verfahren implementiert wird. Wir definieren anschließend das Diffie–Hellman-Problem und untersuchen die Leitfrage, indem wir uns eine Behauptung überlegen, aufstellen und beweisen. Insbesondere wird dabei der Satz von Lagrange thematisiert. Zum Schluss beantworten wir die Leitfrage und schauen uns noch einmal die Einwegfunktionen an.

Inhaltsverzeichnis

1 Einführung: Das Diffie–Hellman-Verfahren

1.1 Kryptosysteme

In der Kryptografie versucht man, eine sichere Kommunikation zwischen zwei oder mehreren Teilnehmern zu gewährleisten. Dazu macht man sich Einwegfunktionen zu Nutze. Einwegfunktionen sind Funktionen, die in der Hinrichtung einfach und in der Rückrichtung schwierig zu berechnen sind. Man implementiert solche Funktionen für das Ver- und Entschlüsseln von Nachrichten. Das Verschlüsseln entspricht dann der Hinrichtung und das Entschlüsseln entspricht der Rückrichtung. Die Einweg-Funktion, die wir beim Diffie–Hellman-Verfahren brauchen, ist die diskrete Exponentialfunktion.

Bevor wir uns die diskrete Exponentialfunktion anschauen, definieren wir zyklische Gruppen und Primitivwurzeln, außerdem schauen wir uns den Satz von Gauß an.

1.2 Diskreter Logarithmus

Definition 1.2.1. *In der Gruppentheorie ist eine zyklische Gruppe eine Gruppe G, die von einem einzelnen Element $a \in G$ erzeugt wird:*

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} = G.$$

Das Element a wird als Erzeuger von G bezeichnet.

Satz 1.2.2. (Satz von Gauß) *Ist n eine natürliche Zahl, dann ist $(\mathbb{Z}/n\mathbb{Z})^\times$ genau dann zyklisch, wenn*

$$n \in \{1, 2, 4, p^k, 2p^k \mid p > 2 \text{ ist eine Primzahl}, k \in \mathbb{N}\}.$$

Vergleiche [3, S.48].

Definition 1.2.3. *Sei $m \in \{1, 2, 4, p^k, 2p^k \mid$ für eine Primzahl $p > 2$, $k \in \mathbb{N}\}$. Dann ist $(\mathbb{Z}/m\mathbb{Z})^\times$ nach dem Satz von Gauß eine zyklische Gruppe. Einen Erzeuger g von $(\mathbb{Z}/m\mathbb{Z})^\times$ bezeichnet man als eine Primitivwurzel modulo m.*

Definition 1.2.4. *Sei p eine Primzahl und $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ erzeugend, d.h. g ist eine Primitivwurzel modulo p. Dann ist $(\mathbb{Z}/p\mathbb{Z})^\times$ eine zyklische Gruppe und wir definieren:*

$$\begin{aligned} \exp_g \colon \mathbb{Z}_p &\to \mathbb{Z}_p^\times \\ x &\mapsto g^x \qquad \mod p \end{aligned}$$

als die diskrete Exponentialfunktion.

Wir schauen uns nun die Definition der Umkehrfunktion an.
Definition 1.2.5. *Sei p eine Primzahl und $g \in \mathbb{Z}_p$. Der diskrete Logarithmus von einer Zahl $y \in \mathbb{Z}_p^\times$ zur Basis g ist definiert als die kleinste natürliche Zahl x mit $y = g^x \mod p$. Bezeichnet mit:*

$$\log_g y =: x$$

Das Bestimmen von x bezeichnet man auch als das diskrete Logarithmus-Problem, da es schwer ist, x zu bestimmen.
ACHTUNG: Wenn $\mathbb{Z}_p^\times$ keine zyklische Gruppe ist oder g kein erzeugendes Element ist, muss keine Lösung x existieren.

Wir schauen uns nun das Diffie–Hellman-Verfahren an und gehen darauf ein, wie das diskrete Logarithmus-Problem bei diesem Verfahren implementiert wird.

1.3 Das Diffie–Hellman-Verfahren

Das Problem, welches man beim Diffie–Hellman-Verfahren löst, ist folgendes:

Alice und Bob wollen einen Schlüssel (eine Zahl) teilen, ohne, dass Charlie dies mitbekommt.

Wir schauen uns an, wie man so einen Schlüssel erstellt:

Schritt 1:
Bob und Alice einigen sich am besten auf eine sehr große Primzahl p und eine Zahl $1 < g < p-1$. Die Zahlen g und p sind öffentlich.

Schritt 2:
Alice wählt eine beliebige ganze Zahl $1 < a \leq p-1$ und Bob eine beliebige ganze Zahl $1 < b \leq p-1$.
Die Zahlen a und b sind geheim.
Schritt 3:
Alice berechnet

$$A = g^a \mod p$$

und Bob berechnet

$$B = g^b \mod p.$$

Schritt 4:
Alice sendet die Zahl A an Bob und Bob sendet die Zahl B an Alice. Daher sind A und B öffentlich.
Schritt 5:
Alice berechnet:

$$\tilde{A} = B^a \mod p$$

und Bob berechnet

$$\tilde{B} = A^b \mod p.$$

Es gilt $\tilde{A} = \tilde{B}$, da

$$\tilde{A} \equiv B^a \equiv (g^b)^a \equiv (g^a)^b \equiv A^b \equiv \tilde{B} \mod p.$$

Die Zahl $g^{ab} \equiv \tilde{A} \equiv \tilde{B} \bmod p$ ist der geheime Schlüssel.
Wir bemerken, dass Charlie die Elemente p, g, A und B kennt. Aufgrund des diskreten Logarithmus-Problems kann Charlie a bzw. b aus Schritt 3 nicht so einfach bestimmen, um dann mit dem Wissen über A und b bzw. B und a den geheimen Schlüssel mit $\tilde{A} = B^a \mod p$ bzw. $\tilde{B} = A^b \mod p$ zu bestimmen.

1.3.1 Beispiel

Schritt 1:
Bob und Alice einigen sich auf eine Primzahl $p = 5$ und auf $g = 2$.
Schritt 2:
Alice wählt die Zahl $a = 3$ und Bob die Zahl $b = 2$. Alice berechnet

$$A := g^a \equiv 2^3 \equiv 3 \mod 5$$

und Bob berechnet

$$B := g^b \equiv 2^2 \equiv 4 \mod 5.$$

Schritt 3:
Alice sendet die Zahl $A \equiv 3$ an Bob und Bob sendet die Zahl $B \equiv 4$ an Alice. Alice berechnet:

$$B^a \equiv 4^3 \equiv 4 \mod 5$$

Bob berechnet

$$A^b \equiv 3^2 \equiv 4 \mod 5$$

$B^a \equiv A^b \equiv 4 \mod 5$ ist also der geheime Schlüssel.

Wie kann Charlie den geheimen Schlüssel bestimmen bzw. erraten? Das Problem, das Charlie lösen muss, ist das Diffie–Hellman-Problem:

2 Das Diffie–Hellman-Problem

Definition (Diffie–Hellman-Problem) *Sei p eine Primzahl, g eine ganze Zahl und a, b, A und B wie oben (beim Diffie–Hellman-Verfahren) gegeben. Bestimme*

$$g^{ab}.$$

Wie sollten Alice und Bob g, p, a und b wählen, sodass Charlie es besonders schwer hat, den Schlüssel g^{ab} zu bestimmen, d.h. das Diffie–Hellman-Problem möglichst schwer zu lösen ist?

Wir untersuchen diese Frage unter der Annahme, dass das Wissen über A und B aus Schritt 3 beim Diffie–Hellman-Verfahren Charlie bei der Bestimmung des Schlüssels g^{ab} (für a und b aus Schritt 2 beim Diffie–Hellman-Verfahren) nichts bringt. Später werden wir sehen, dass diese Annahme keinen Einfluss auf die Wahl von p und g hat.

2.1 Wahl von g

Seien p, g, a, b, A, B wie beim Diffie–Hellman-Verfahren. Die Zahl g^{ab} ist der Schlüssel den Charlie erfahren möchte. D.h. die Elemente die g erzeugt sind die möglichen Schlüssel. Charlie kann also durch Ausprobieren der Elemente, die g erzeugt, den Schlüssel g^{ab} bestimmen. Alice und Bob sollten g so auszuwählen, dass g möglichst viele Elemente erzeugt, sodass Charlie umso mehr Elemente aus $\langle g \rangle$ ausprobieren muss, um den Schlüssel zu bestimmen.

Zur Veranschaulichung – ein Beispiel dafür wie man g nicht wählen sollte: Der Extremfall für eine falsche Wahl von g ist $g = 1$. Die von $g = 1$ erzeugte Untergruppe ist $\{1\}$, d.h. als Schlüssel g^{ab} für $a, b \in \mathbb{N}$ ist nur 1 möglich.

Die Zahl g sollte also am besten eine Primitivwurzel in $(\mathbb{Z}/p\mathbb{Z})^\times$ sein. Daher schauen wir uns beim Diffie–Hellman-Verfahren die Primzahlen p an, da $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklische Gruppen sind und somit Primitivwurzeln enthalten. Wir wissen, dass wir g als eine Primitivwurzel in $(\mathbb{Z}/p\mathbb{Z})^\times$ wählen sollten. Wir wissen allerdings nicht, wie man ein solches g findet. Bei der Wahl von der Primzahl p geht es also darum, dass wir p so wählen, dass es möglichst einfach ist, ein g in $(\mathbb{Z}/p\mathbb{Z})^\times$ zu finden.

Eine Überlegung wäre, dass man die Primzahl p so wählt, dass der Anteil an Elementen in $(\mathbb{Z}/p\mathbb{Z})^\times$, die Primitivwurzeln sind, möglichst hoch ist, da wir keine Formel kennen um eine

Primitivwurzel zu bestimmen. Dann würde man durch Ausprobieren schnell eine Primitivwurzel finden.
Frage: *Wie hängt die „Form“ der Primzahl p von dem Anteil der Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$, welche Primitivwurzeln sind, ab?*

Wir brauchen eine Behauptung über diesen Zusammenhang, um diese dann zu überprüfen. Um eine Behauptung aufzustellen müssen wir etwas Vorarbeit leisten und Grundlagen wiederholen, insbesondere wird uns der Satz von Lagrange dabei helfen:

2.2 Aufstellung einer Behauptung über die Wahl von p

Definition 2.2.1. (Euler´sche Phi-Funktion) *Sei $n \in \mathbb{N}$ und $\varphi(n) := |\{d \in [0,n] \cap \mathbb{N} \mid \mathrm{ggT}(d,n) = 1\}|$. Die Abbildung*

$$\varphi \colon \mathbb{N}^+ \to \mathbb{N}^+$$

heißt Euler´sche Phi-Funktion und ist für $n \in \mathbb{N}^+$ gleich der Anzahl an Elementen aus $[0,n]$, die teilerfremd zu n sind.

Satz 2.2.2. (Kleiner Satz von Fermat) *Sei p eine Primzahl und $a \in \mathbb{Z}$.*

(a) Falls $p \nmid a$, dann ist $a^{p-1} \equiv 1 \mod p$.

(b) Für alle p und a gilt $a^p \equiv a \mod p$.

Vergleiche [1, S.22].

Satz 2.2.3. (Satz von Euler) *Für alle a, $n \in \mathbb{N}$ mit $\mathrm{ggT}(a,n) = 1$ gilt:*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Vergleiche [1, S.21].

Wir führen nun eine neue Definition ein:
Defintion 2.2.4. *Sei $m \in \mathbb{N}$ und $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Die Ordnung von a modulo m ist die kleinste positive Zahl r, sodass $a^r \equiv 1 \mod m$ gilt:*

$$r = \mathrm{ord}_m(a)$$

Bemerkung 2.2.5. *Sei $m \in \mathbb{N}$, dann ist $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ genau dann eine Primitivwurzel modulo m, wenn $\mathrm{ord}_m(a) = \varphi(m)$ gilt.*

Bemerkung 2.2.6. *Sei $m \in \mathbb{N}$, $1 \leq a \leq m-1$ und $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ die von a erzeugte Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$. Dann gilt:*

$$|\langle a \rangle| = \mathrm{ord}_m(a)$$

Sei p eine Primzahl. In den noch folgenden Beweisen verwenden wir die Definition einer Primitivwurzel $g \in \mathbb{Z}/p\mathbb{Z}^\times$ als ein Element g mit $\mathrm{ord}_p(g) = p-1$.

Das folgende Lemma wird uns dabei helfen, eine Behauptung über die „Form“ von p aufzustellen:

Lemma 2.2.7.(Satz von Lagrange) *Sei $m \in \mathbb{N}$ und $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Die Ordnung von a modulo m ist ein Teiler von $\varphi(m)$.*

Beweis. Wir geben den Beweis aus [1, S.22]. Sei $r = \mathrm{ord}_m(a)$, also $a^r \equiv 1 \mod m$. Der Satz von Euler impliziert, dass auch $a^{\varphi(m)} \equiv 1 \mod m$.
Nach dem Lemma von Bézout existieren $x, y \in \mathbb{Z}$ mit $g := \mathrm{ggT}(r, \varphi(m)) = xr + y\varphi(m)$. Es folgt, dass $a^g \equiv a^{rx} \cdot a^{y\varphi(m)} \equiv 1 \mod m$. Da die Ordnung die kleinste positive Zahl mit dieser Eigenschaft ist, folgt $r = g$. Wir schließen, dass r ein Teiler von $\varphi(m)$ ist. *q.e.d.*

Wir schauen uns an, was das Lemma 2.2.7. für die Wahl von p bedeutet:
Sei p eine Primzahl und seien $d_1, ..., d_{k-1}$ und $d_k = p-1$ die Teiler von $p-1$ für ein $k \in \mathbb{N}$. Wir definieren

$$C_d := \{1 \leq a \leq p-1 |\ \mathrm{ord}_p(a) = d\}$$

für alle $d \in \{d_1, ...d_k, p-1\}$. Dann gilt mit Lemma 2.2.7. und wegen $C_{d_i} \cap C_{d_j} = \emptyset$ für $1 \leq i \neq j \leq k$:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \dot{\bigcup_{d|p-1}} C_d = C_{d_1} \dot{\cup} \cdots \dot{\cup} C_{d_{k-1}} \dot{\cup} C_{p-1}$$

Wir bemerken, dass C_{p-1} die Menge der Primitivwurzeln ist. Zur Erinnerung: wir wollten p so wählen, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ möglichst viele Primitivwurzeln enthält.
Überlegung: Wir wissen, dass die Elemente aus $(\mathbb{Z}/p\mathbb{Z})^\times$ auf die Mengen C_{d_i} und C_{p-1} für alle $i = 1, ..., k-1$ aufgeteilt werden. Man kann sich also fragen; ob ein größerer Anteil der Elemente aus $(\mathbb{Z}/p\mathbb{Z})^\times$ auf C_{p-1} verteilt wird, wenn es weniger Mengen C_{d_i} mit $i = 1, ..., k-1$ gibt, auf welche die Elemente aus $(\mathbb{Z}/p\mathbb{Z})^\times$ aufgeteilt werden können.

Frage: Für welche Primzahlen p ist die Anzahl der Mengen C_d minimal?
Wir sehen, dass die Anzahl der Mengen C_d der Anzahl der Teiler von $p-1$ entspricht:

$$\#C_d = |\{d_1, ...d_k, p-1\}| = \#\text{Teiler von } p-1$$

Wir wollen also wissen für welche p die Anzahl der Teiler von $p-1$ minimal ist. Es gilt:

$$p - 1 = 2q$$

für ein $q \in \mathbb{N}$, da p eine große Primzahl, also ungerade ist. Die Anzahl der Teiler von $p-1$ ist also genau dann minimal, wenn q eine Primzahl ist.

Damit ist die Anzahl der Mengen C_d genau dann minimal, wenn sich $p-1$ in genau zwei

Primfaktoren zerlegen lässt.

Die Behauptung über die Wahl von p lautet somit:
Behauptung 2.2.8. *Sei p eine Primzahl. Der Anteil der Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$, welche Primitivwurzeln sind, ist am größten, wenn $p-1$ sich in genau zwei Primfaktoren zerlegen lässt.*

2.3 Beweis der Behauptung 2.2.8. über die Wahl von p

Um die Behauptung zu überprüfen, d.h. den Anteil an Primitivwurzeln in $(\mathbb{Z}/p\mathbb{Z})^\times$ für eine Primzahl p zu berechnen, brauchen wir eine Formel um die Anzahl der Primitivwurzeln in $(\mathbb{Z}/p\mathbb{Z})^\times$ zu bestimmen. Deshalb werden wir uns zwei Lemmata und zwei Sätze anschauen und beweisen. Mit diesen Sätzen und Lemmata können wir dann die Anzahl der Primitivwurzeln in $(\mathbb{Z}/p\mathbb{Z})^\times$ berechnen.

Satz 2.3.1. *Sei p eine Primzahl und d ein Teiler von $p-1$. Die Kongruenz*

$$x^d \equiv 1 \mod p$$

besitzt genau d Lösungen.

Beweis. Wir geben den Beweis aus [1, S.52]. Sei d ein Teiler von $p-1$. Wir schreiben $p-1 = d\cdot e$ für ein $e \in \mathbb{N}$, da $d \mid p-1$. Dann gilt:

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + ... + x^d + 1) =: (x^d - 1)g(x).$$

Der kleine Satz von Fermat impliziert, dass die Kongruenz $x^{p-1} \equiv 1 \pmod m$ genau $p-1$ Lösungen besitzt, nämlich die Elemente von $\mathbb{Z}/p\mathbb{Z}^\times$. Die Kongruenz $g(x) \equiv 0 \mod p$ besitzt höchstens $\mathrm{Grad}(g) = d(e-1) = p-1-d$ Lösungen. Es gibt also mindestens d Zahlen $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$ mit $g(\alpha) \not\equiv 0 \mod p$. Diese Zahlen erfüllen also $\alpha^d \equiv 1 \mod p$. Da die Kongruenz $x^d \equiv 1 \mod p$ höchstens d Lösungen besitzt, schließen wir, dass genau d Zahlen $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$ mit $a^d \equiv 1 \mod p$ existieren. *q.e.d.*

Lemma 2.3.2. *Sei $n \in \mathbb{N}$. Es gilt, dass*

$$\sum_{d|n} \varphi(d) = n.$$

Beweis. Wir geben den Beweis aus [1, S.23]. Sei $n \in \mathbb{N}$ und $M := \{1, ..., n\}$. Wir definieren

$$\varphi_d(n) = |\{a \in M \mid \mathrm{ggT}(a, n) = d\}|.$$

So ist $\sum_{d|n} \varphi_d(n) = n$. Sei d ein Teiler von n und $1 \le a \le n$. Dann gilt

$$\mathrm{ggT}(a, n) = d \quad \Leftrightarrow \quad \mathrm{ggT}\left(\frac{a}{d}, \frac{n}{d}\right) = 1.$$

Somit gilt $\varphi_d(n) = \varphi\left(\frac{n}{d}\right)$ und damit

$$\sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi_d(n) = n.$$

Somit folgt die Behauptung. *q.e.d.*

Lemma 2.3.3. Vergleiche [1, S.52]. *Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $\mathrm{ggT}(a, m) = 1$. Für alle $k \in \mathbb{N}$ gilt, dass*

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\mathrm{ggT}(\mathrm{ord}_m(a), k)}$$

ist.

Bemerkung 2.3.4. *Sei $\mathrm{ord}_m(a) = d$. Dann gilt:*

$$\mathrm{ord}_m(a^k) = d \Leftrightarrow \frac{\mathrm{ord}_m(a)}{\mathrm{ggT}(\mathrm{ord}_m(a), k)} = \frac{d}{\mathrm{ggT}(d, k)} = d \Leftrightarrow \mathrm{ggT}(d, k) = 1$$

Diese Folgerung ist für den nachfolgenden Beweis wichtig.

Nun kommen wir zu dem Satz, den wir brauchen, um die Anzahl der Primitivwurzel in $(\mathbb{Z}/p\mathbb{Z})^\times$ für eine Primzahl p zu berechnen:
Satz 2.3.5. *Sei p eine Primzahl und d ein Teiler von $p - 1$. Wir definieren*

$$\psi(d) = |\{1 \leq a \leq p - 1 \mid \mathrm{ord}_p(a) = d\}|.$$

Es gilt, dass

$$\psi(d) = \varphi(d).$$

Beweis. Wir geben den Beweis aus [1, S.53]. Sei p eine Primzahl und d ein Teiler von $p - 1$. Wir nehmen zuerst an, dass $\psi(d) > 0$. Dann existiert eine Zahl $1 \leq a \leq p - 1$ mit $\mathrm{ord}_p(a) = d$. Insbesondere sind die Zahlen $a, a^2, ..., a^d$ nicht kongruent modulo p. Außerdem gilt für $i = 1, ..., d$, dass

$$(a^i)^d \equiv (a^d)^i \equiv 1^i \equiv 1 \mod p.$$

Also ist a^i eine Lösung der Kongruenz $x^d \equiv 1 \mod p$ für $i = 1, ..., d$. Wir haben in Lemma 2.3.1 gezeigt, dass die Kongruenz $x^d \equiv 1 \mod p$ genau d Lösungen modulo p besitzt. Diese Lösungen sind daher $a, a^2, ..., a^d$. Nun impliziert die Bemerkung 2.3.4, dass $\mathrm{ord}_p(a^i) = d$ genau dann gilt, wenn $\mathrm{ggT}(i, d) = 1$ ist, also wenn $i \in \mathbb{Z}/d\mathbb{Z}^\times$ ist. Die Anzahl solcher i ist $\varphi(d)$. Wir haben daher gezeigt, dass falls $\psi(d) > 0$, so ist $\psi(d) = \varphi(d)$. Wir müssen jetzt nur noch zeigen, dass der Fall $\psi(d) = 0$ nicht eintreten kann. Wir wissen aus Lemma 2.2.7, dass die Ordnung $\mathrm{ord}_p(a)$ jeder Zahl $0 < a < p$ ein Teiler von $p - 1$ ist. Daher gilt, dass

$$\sum_{d|p-1} \psi(d) = p - 1.$$

Außerdem gilt:

$$\sum_{d|p-1} \varphi(d) = p - 1.$$

nach Lemma 2.3.2. Für jedes d gilt, dass $\psi(d) \leq \varphi(d)$ ist. Falls $\psi(d) = 0$ gilt, so ist dies offensichtlich. Falls $\psi(d) > 0$ ist, so haben wir gezeigt, dass $\psi(d) = \varphi(d)$. Daher gilt, dass

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) = p - 1.$$

Aber dies ist nur möglich falls $\psi(d) = \varphi(d)$ für alle $d \mid (p-1)$. *q.e.d.*

Nun können wir endlich unsere Behauptung 2.2.8 über die Wahlvon p beweisen.

Behauptung 2.2.8. *Sei p eine Primzahl. Der Anteil der Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$, welche Primitivwurzeln sind, ist am größten, wenn sich $p-1$ in genau 2 Primfaktoren zerlegen lässt.*

Beweis. Mit dem Satz 2.3.5, den wir gerade gezeigt haben, können wir die Anzahl der Primitivwurzeln in $(\mathbb{Z}/p\mathbb{Z})^\times$ für eine Primzahl p ausrechnen. Es gilt nämlich laut dem Satz 2.3.5, dass wenn wir $d = p - 1$ wählen, dass $\psi(p-1)$, also die Anzahl der Primitivwurzeln von $(\mathbb{Z}/p\mathbb{Z})^\times$ mit $\varphi(p-1)$ übereinstimmt.

Wir schauen uns zuerst den Anteil der Primitivwurzeln an, wenn p eine Primzahl ist, wobei $p - 1 = 2p_1$ sich in genau 2 Primfaktoren mit einer Primzahl p_1 zerlegen lässt. Es gelten:

$$\begin{aligned}\psi(1) =& \varphi(1) = 1\\ \psi(2) =& \varphi(2) = 1\\ \psi(p_1) =& \varphi(p_1) = p_1 - 1,\end{aligned}$$

da 2 und p_1 Primzahlen sind. Nun gilt, wegen $p - 1 = 2p_1$ bereits $p_1 = \dfrac{p-1}{2} = \dfrac{p}{2} - \dfrac{1}{2}$.
Aus Lemma 2.3.2. und Satz 2.3.5. folgt $\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d) = p - 1$ und wir erhalten:

$$\begin{aligned}\psi(p-1) =& \psi(1) + \psi(2) + \psi(p_1) + \psi(p-1) - \psi(1) - \psi(2) - \psi(p_1)\\ =& \sum_{d|p-1} \psi(d) - \psi(1) - \psi(2) - \psi(p_1)\\ =& p - 1 - 1 - 1 - (p_1 - 1)\\ =& p - 3 - (\frac{p}{2} - \frac{1}{2} - 1)\\ =& \frac{p-3}{2}\end{aligned}$$

Da 1 und $p-1$ keine gute Wahl für g sind(, da $\langle g\rangle = \{1\}$ für $g = 1$ und $\langle g\rangle = \{1, p-1\}$ für $g = p-1$) , gilt $1 < g < p-1$, d.h. es kommen $p-3$ Elemente für g infrage.

Somit sind die „Hälfte“ der Elemente in $\{2, ..., p-2\} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ Primitivwurzeln.
Um die Behauptung zu beweisen müssen wir zeigen, dass der Anteil der Primitivwurzeln in $\{2, ..., p-2\} \subset \mathbb{Z}/p\mathbb{Z}^\times$, wenn p sich in mehr als 2 Primfaktoren zerlegen lässt, kleiner als die Hälfte ist.

Sei p eine Primzahl, wobei $p-1 = 2p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j}$ für ein $j \in \mathbb{N}$ und $k_i \in \mathbb{N}$ für alle $i = 1, ..., j$. Die Primzahlen p_1 bis p_k sind außerdem paarweise verschieden. Wir bemerken, dass für die Euler´sche Phi Funktion $\varphi(uv) = \varphi(u)\varphi(v)$ für $u, v \in \mathbb{Z}$ gilt, falls $ggT(u, v) = 1$ und $\varphi(p_i^{k_i}) = (p_i^{k_i} - p_i^{k_i-1})$ für alle $i = 1, ..., j$ gilt. Wir erhalten also:

$$\sum_{\substack{d|p-1\\ d\neq p-1}} \psi(d) \geq \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_1=0}^{k_1-1} \psi(p_1^{k_1-l_1}p_2^{k_2-l_2}\cdots p_j^{k_j-l_j}) \tag{1}$$

$$= \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_1=0}^{k_1-1} \varphi(p_1^{k_1-l_1}p_2^{k_2-l_2}\cdots p_j^{k_j-l_j}) \tag{2}$$

$$= \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_1=0}^{k_1-1} \varphi(p_1^{k_1-l_1})\varphi(p_2^{k_2-l_2})\cdots\varphi(p_j^{k_j-l_j}) \tag{3}$$

$$= \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_1=0}^{k_1-1} (p_1^{k_1-l_1} - p_1^{k_1-l_1-1})(p_2^{k_2-l_2} - p_2^{k_2-l_2-1})\cdots(p_j^{k_j-l_j} - p_j^{k_j-l_j-1}) \tag{4}$$

$$= \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_2=0}^{k_2-1} (p_1^{k_1} - 1)(p_2^{k_2-l_2} - p_2^{k_2-l_2-1})\cdots(p_j^{k_j-l_j} - p_j^{k_j-l_j-1}) \tag{5}$$

$$= (p_1^{k_1} - 1) \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_2=0}^{k_2-1} (p_2^{k_2-l_2} - p_2^{k_2-l_2-1})\cdots(p_j^{k_j-l_j} - p_j^{k_j-l_j-1}) \tag{6}$$

$$= (p_1^{k_1} - 1)(p_2^{k_2} - 1) \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_3=0}^{k_3-1} (p_3^{k_3-l_3} - p_3^{k_3-l_3-1})\cdots(p_j^{k_j-l_j} - p_j^{k_j-l_j-1}) \tag{7}$$

$$= (p_1^{k_1} - 1)(p_2^{k_2} - 1)\cdots(p_j^{k_j} - 1) \tag{8}$$

Wenn wir den Faktor $p_1^{k_1-l_1}$ für alle $l_2 = 1, .., k_2 - 1$ in der Abschätzung (1) weglassen erhalten wir eine Abschätzung mit Teilern von $p-1$ die paarweise verschieden zu den Teilern von $p-1$ in der Abschätzung (1) sind und erhalten anstelle von der Abschätzung (8):

$$\sum_{\substack{d|p-1\\ d\neq p-1}} \psi(d) \geq \sum_{l_j=0}^{k_j-1} \cdots \sum_{l_2=0}^{k_2-1} \psi(p_2^{k_2-l_2}\cdots p_j^{k_j-l_j}) \tag{9}$$

$$= (p_2^{k_2} - 1)\cdots(p_j^{k_j} - 1) \tag{10}$$

Da die Teiler von $p-1$ in der Abschätzung (9) paarweise verschieden zu den Teilern von $p-1$ in der Abschätzung (1) sind, können wir $\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d)$ mit der Summe aus (8) und (10) nach oben abschätzen und erhalten :

$$\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d) \geq (p_1^{k_1}-1)(p_2^{k_2}-1)\cdots(p_j^{k_j}-1) + (p_2^{k_2}-1)\cdots(p_j^{k_j}-1) \tag{11}$$

$$= p_1^{k_1}(p_2^{k_2}-1)\cdots(p_j^{k_j}-1) \tag{12}$$

Wenn wir bei den Abschätzungen (1) und (9) die Teiler $p_2^{k_2-l_2}$ für alle $l_2 = 1,..,k_2-1$ weglassen, erhalten wir anstelle von der Abschätzung (12):

$$\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d) \geq p_1^{k_1}(p_3^{k_3}-1)\cdots(p_j^{k_j}-1) \tag{13}$$

Da die Teiler von $p-1$ in der Abschätzung (13) paarweise verschieden zu den Teilern von $p-1$ in der Abschätzung (1) und (9) und somit auch zu den Teilern von $p-1$ in der Abschätzung (12) sind, können wir $\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d)$ mit der Summe aus (12) und (13) nach oben abschätzen und erhalten:

$$\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d) \geq p_1^{k_1}(p_2^{k_2}-1)(p_3^{k_3}-1)\cdots(p_j^{k_j}-1) + p_1^{k}(p_3^{k_3}-1)\cdots(p_j^{k_j}-1) \tag{14}$$

$$= p_1^{k_1}p_2^{k_2}(p_3^{k_3}-1)\cdots(p_j^{k_j}-1) \tag{15}$$

Lassen wir nun nacheinander die Teiler $p_i^{k_i-l_i}$ für alle $l_i = 1,..,k_i-1$ und für alle $i = 3,...,j$ in allen vorhergehenden Abschätzungen weg und addieren (nach jedem Weglassen) die letzte vorhergehende Abschätzung mit der Abschätzung, die wir anstelle der letzten vorhergehenden Abschätzung (wegen dem Weglassen) erhalten, erhalten wir anstelle von (15) induktiv:

$$\sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d) \geq p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j} \tag{16}$$

Es gilt $\sum_{i=1}^{j}\sum_{l_i=0}^{k_i-1}\varphi(2p_i^{k_i-l_i}) \geq 2$, da $\varphi(2p_i^{k_i-l_i}) \geq 1$ für alle $l_i = 1,..,k_i-1$ und für alle $i = 1,...,j$ gilt und $p-1$ sich in mindestens 3 Primfaktoren zerlegen lässt. Da wir bei der Abschätzung (16) die Teiler 2 und $2p_i^{k_i-l_i}$ von $p-1$ für alle $l_i = 1,..,k_i-1$ und für alle $i = 1,...,j$ nicht verwendet haben, erhalten wir mit $p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j} = \frac{p-1}{2} = \frac{p}{2} - \frac{1}{2}$ und $\sum_{i=1}^{j}\sum_{l_i=0}^{k_i-1}\varphi(2p_i^{k_i-l_i}) \geq 2$:

$$\psi(p-1) = \sum_{d|p-1} \psi(d) - \sum_{\substack{d|p-1 \\ d\neq p-1}} \psi(d) \tag{17}$$

$$\leq p-1-p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j} - \psi(2) - \sum_{i=1}^{j}\sum_{l_i=0}^{k_i-1} \psi(2p_i^{k_i-l_i}) \tag{18}$$

$$= p-1-p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j} - \varphi(2) - \sum_{i=1}^{j}\sum_{l_i=0}^{k_i-1} \varphi(2p_i^{k_i-l_i}) \tag{19}$$

$$\leq p-1-(\frac{p}{2}-\frac{1}{2}) - 1 - 2 \tag{20}$$

$$\leq \frac{p-7}{2} \tag{21}$$

Weniger als die „Hälfte“ der Elemente in $\{2,...,p-2\} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ sind Primitivwurzeln. Für eine Primzahl p ist der Anteil der Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$, welche Primitivwurzeln sind, also am größten, wenn $p-1$ sich in genau 2 Primfaktoren zerlegen lässt.$_{q.e.d.}$

Wir sollten also die Primzahl p mit der „Form“ $p-1=2q$ wählen, wobei q eine Primzahl ist. Eine Primzahl p mit dieser „Form“ wird als starke Primzahl bezeichnet.

2.4 Wahl von a und b

Sei p eine starke Primzahl, d.h. es gilt $p-1=2q$ für eine Primzahl q und g eine Primitivwurzel in $(\mathbb{Z}/p\mathbb{Z})^\times$, außerdem wählen wir a, b, A und B wie beim Diffie–Hellman-Verfahren.

Zur Erinnerung, wir haben die Wahl von g und p unter der Annahme bestimmt, dass Charlie mit dem Wissen über A und B den geheimen Schlüssel g^{ab} nicht effizienter als ohne das Wissen über A und B bestimmen kann. Wir zeigen die Annahme nun für die Wahl von p und g.
Seien $\langle A\rangle$ und $\langle B\rangle$, die von A und B erzeugten Untergruppen in $(\mathbb{Z}/p\mathbb{Z})^\times$. Es gilt für den geheimen Schlüssel g^{ab}:

$$g^{ab} \in \langle g\rangle \cap \langle A\rangle \cap \langle B\rangle \subset \langle g\rangle,$$

Wenn Alice a so wählt, dass $A \in \{1, p-1\}$ gilt, dann gilt $\langle A\rangle = \{1\}$ für $A=1$ und $\langle A\rangle = \{1, p-1\}$ für $A=p-1$. Somit muss Charlie maximal 2 Elemente aus $\langle A\rangle$ ausprobieren um den Schlüssel zu finden. Das Gleiche gilt auch für Bob für die Wahl von b.

Alice und Bob wählen also a und b, so dass $A, B \notin \{1, p-1\}$ gilt. Seien nun a und b so gewählt, dass $A, B \notin \{1, p-1\}$ gilt und sei die ψ-Funktion wie aus Satz 2.3.5.. Da $\mathrm{ord}_p(1)=1$, $\mathrm{ord}_p(p-1)=2$ und nach Satz 2.3.5. $\psi(1)=\phi(1)=1$ und $\psi(2)=\phi(2)=1$ gelten, folgt nach Lemma 2.2.7., dass $\mathrm{ord}_p(A), \mathrm{ord}_p(B) \in \{q, p-1\}$ gilt.

Fall 1: Es gilt $\mathrm{ggT}_p(A)=q$ und $\mathrm{ord}_p(B)=p-1$. Also gilt nach Bemerkung 2.2.6. bereits $2|\langle A\rangle| = 2q = p-1 = |\langle g\rangle|$. D.h. die Wahrscheinlichkeit, dass Charlie den Schlüssel g^{ab} durch

ausprobieren der Elemente in $\langle A\rangle$ bestimmt, ist doppelt so groß, wie den Schlüssel g^{ab} durch ausprobieren der Elemente in $\langle g\rangle$ zu bestimmen. Allerdings muss Charlie, bevor sie ein Element aus $\langle A\rangle$ als Schlüssel ausprobiert, ein Element aus $\langle A\rangle$ berechnen bzw. bestimmen. Das heißt Charlie, braucht zwei Rechenschritte um zu bestimmen, ob ein Element aus $\langle A\rangle$ der Schlüssel g^{ab} ist. Dahingegen braucht man nur einen Rechenschritt um zu bestimmen, ob ein Element aus $\langle g\rangle$ der Schlüssel g^{ab} ist, da man die Elemente aus $\langle g\rangle$ nicht bestimmen muss. Daher kann Charlie mit zwei Rechenschritten zwei Elemente aus $\langle g\rangle$ als Schlüssel ausprobieren. Sei $1 \leq n \leq \frac{p-1}{2}$. Die Wahrscheinlichkeit, dass Charlie mit $2n$ Rechenschritten den Schlüssel durch ausprobieren von n Elementen in $\langle A\rangle$ findet, beträgt $\sum_{i=1}^{n} \frac{1}{\frac{p-1}{2}-i+1} = \sum_{i=1}^{n} \frac{2}{p+1-2i}$. Die Wahrscheinlichkeit, dass Charlie mit $2n$ Rechenschritten den Schlüssel g^{ab} durch ausprobieren von $2n$ Elementen in $\langle g\rangle$ findet, beträgt $\sum_{i=1}^{2n} \frac{1}{p-1-i+1} = \sum_{i=1}^{2n} \frac{1}{p-i} > \sum_{i=1}^{n} \frac{2}{p+1-2i}$ (kann man einfach durch Induktion zeigen). Somit kann Charlie den Schlüssel g^{ab} effizienter finden, wenn sie ihr Wissen über A nicht nutzt. Das Wissen über B bringt Charlie nichts, da nach Bemerkung 2.2.6. $|\langle A\rangle| = p-1 = |\langle g\rangle|$, also $\langle A\rangle = \langle g\rangle$ gilt.
Fall 2: Es gilt $\mathrm{ord}_p(B) = q$ und $\mathrm{ord}_p(A) = p-1$. Es folgt die gleiche Argumentation wie bei Fall 1 für B anstelle von A.
Fall 3: Es gilt $\mathrm{ord}_p(A) = \mathrm{ord}_p(B) = q$. Dies folgt trivialerweise aus Fall 1 und Fall 2.
Fall 4: $\mathrm{ord}_p(A) = p-1 = \mathrm{ord}_p(B)$. Dann gilt mit Bemerkung 2.2.6. $|\langle g\rangle| = p-1 = |\langle A\rangle| = |\langle B\rangle|$ und somit $\langle g\rangle \cap \langle A\rangle \cap \langle B\rangle = \langle g\rangle$, d.h. Charlies Wissen über A und B spielt keine Rolle dabei, wie viele Elemente Charlie aus $\langle g\rangle$ als Schlüssel ausprobieren muss.

$\Rightarrow$Wir schließen daraus, dass Charlie mit dem Wissen über A und B den Schlüssel g^{ab} nicht effizienter finden kann(als ohne dem Wissen) und dass wir auch ohne die Annahme(über das Wissen von A und B) auf die gleiche Wahl von p und g gekommen wären.

2.5 Beantwortung der Leitfrage

Nun können wir endlich die Leitfrage beantworten unter welchen Voraussetzungen das Diffie–Hellman-Problem besonders schwer zu lösen ist.

Antwort:

- p sollte eine starke Primzahl sein. D.h.:

$$p - 1 = 2q,$$

  wobei q eine Primzahl ist.

- g sollte eine Primitivwurzel in $(\mathbb{Z}/p\mathbb{Z})^\times$ sein.
- Alice und Bob sollten $1 < a, b \leq p - 1$ so wählen, dass $A, B \notin \{1, p - 1\}$ gilt.

3 Ausblick

Wie wir gesehen haben, beruht das Diffie–Hellman-Verfahren und die gesamte Präsentation unter der Annahme, dass die diskrete Exponentialfunktion eine Einweg-Funktion ist. Man weiß allerdings nicht, ob Einweg-Funktionen existieren. Dies bezeichnet man auch als PNP-Problem, welches als eines der wichtigsten ungelösten Probleme der Mathematik und Informatik gilt. Dabei ist die Frage, ob die Menge aller Probleme, die schnell lösbar sind (P) und die Menge aller Probleme, bei der man eine vorgeschlagene Lösung schnell auf Korrektheit überprüfen kann (NP), identisch sind.
Könnte für mindestens ein Problem aus NP gezeigt werden, dass dieses prinzipiell nicht schnell lösbar ist, wäre P$\neq$ NP bewiesen. Wenn man also beim Diskreten Logarithmus-Problem zeigt, dass kein Verfahren existiert, um das Problem schnell lösen zu können, haben wir P$\neq$ NP bewiesen. Wenn allerdings P=NP gilt, dann existieren Einwegfunktionen nicht und das Diffie–Hellman-Verfahren wäre nicht mehr sicher, da die diskrete Exponentialfunktion keine Einweg-Funktion mehr wäre. Damit wären sämtliche Kryptoverfahren nicht mehr sicher, da diese auf der Existenz von Einweg-Funktionen basieren.
Die Antwort auf die Leitfrage beruht also auch auf der Vermutung, dass es keinen effizienten Algorithmus gibt um das Problem Diffie–Hellman-Problem oder das diskrete Logarithmus Problem zu lösen.

Literatur

[1] Irene I. Bouw: *Elementare Zahlentheorie, Vorlesungsskript*, 2008, Universität Ulm. http://www.mathematik.uni-ulm.de/ReineMath/mitarbeiter/bouw/ss08/files/skriptez.pdf [Online; accessed 07-July-2021]

[2] Jeffrey Hoffstein, Jill Pipher und Joseph H. Silverman: *An Introduction to Mathematical Cryptography*. Springer-Verlag, New York, Second Edition, 2014, ISBN 978-1-4939-1710-5

[3] Steffen Roch: *Zahlentheorie, Vorlesungsskript*, 2016, Technische Universität Darmstadt. https://www.mathematik.tu-darmstadt.de/media/analysis/lehrmaterial_anapde/roch/Zahlentheorie.pdf [Online; accessed 07-July-2021]

[4] Wikipedia contributors: P-NP-Problem — Wikipedia, The Free Encyclopedia, 2021. https://de.wikipedia.org/wiki/P-NP-Problem, [Online; accessed 29-June-2021].