Kryptographie
Rivest-Shamir-Adleman-Kryptosystem

Niklas Simandi

18. März 2022

Zusammenfassung

Nach einer Einführung in Public-Key-Kryptosysteme ist das Rivest-Shamir-Adleman-Kryptosystem exemplarisch hinsichtlich der Chiffrierung, der Dechiffrierung und dem Schlüsselaustausch dargelegt.

Inhaltsverzeichnis

1 Kryptographie

Kryptographie ist die Lehre von Geheimschriften zur Wahrung vertraulicher Informationen vor Unbefugten. Das Ausgangsproblem der Kryptographie ist die Kommunikation über einen von Natur aus unsicheren Kanal. Die zu versendende Information heißt **Klartext**. Durch den Prozess der **Chiffrierung** erzeugt der Sender aus einem Klartext einen **Geheimtext**, der im Idealfall nur für den Empfänger reversibel ist. Für die Chiffrierung und Dechiffrierung ist jeweils ein **Schlüssel** nötig. Die nachfolgende Definition präzisiert die Beziehung zwischen diesen Begriffen.

Definition 1.1: Sei $\mathcal{P}$ eine Menge von Klartexten, $\mathcal{C}$ eine Menge von Geheimtexten und $\mathcal{K}$ eine Menge von Schlüsseln. Ein **Kryptosystem** $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ definiert für alle $k \in \mathcal{K}$ eine **Chiffrierungsregel** $e_k : \mathcal{P} \to \mathcal{C}$ und eine zugehörige **Dechiffrierungsregel** $d_j : \mathcal{C} \to \mathcal{P}$ für ein $j \in \mathcal{K}$, sodass $d_j(e_k(p)) = p$ für alle $p \in \mathcal{P}$ gilt.

Der Kommunikationsablauf ist nun im Allgemeinen wie folgt:

1. Zu Beginn einigen sich Sender und Empfänger auf ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ und ein **Schlüsselpaar** $(k, j) \in \mathcal{K} \times \mathcal{K}$ mit $d_j(e_k(p)) = p$ für alle $p \in \mathcal{P}$.

2. Der Sender sendet den Geheimtext $c \coloneqq e_k(p)$ für den Klartext $p \in \mathcal{P}$ über einen Kanal an den Empfänger.

3. Der Empfänger dechiffriert den empfangenen Geheimtext c, um den Klartext p aus $d_j(c)$ zu erhalten.

Zu beachten ist allerdings, dass dieser Ablauf eine Einigung zwischen Sender und Empfänger auf das Schlüsselpaar (k, j) voraussetzt. Dies ist in der Realität nur selten der Fall. In der Regel geschieht der **Schlüsselaustausch** stattdessen über den Kommunikationskanal selbst.

Vorweg ist dies zum Beispiel beim Rivest-Shamir-Adleman-Kryptosystem gegeben, dessen Schlüsselaustausch auf dem Diffie-Hellman-Protokoll basiert [1], das k als den **öffentlichen Schlüssel** und j als den **privaten Schlüssel** bezeichnet [2].

Ziel der Facharbeit ist das Zusammenspiel zwischen öffentlichem und privatem Schlüssel konkret für das Rivest-Shamir-Adleman-Kryptosystem darzustellen. Das heißt, die Chiffrierungsregel und Dechiffrierungsregel zu bestimmen.

1.1 Codierungen

Der Austausch von Informationen, auch Kommunikation, basiert auf vordefinierten Regeln und Vereinbarungen. In der Kryptographie dient ein **Code** als System zur Kommunikation zwischen Sender und Empfänger. Besonders für Kryptosysteme ist die Etablierung eines Codes zur numerischen Betrachtung von Nachrichten unabdingbar.

Definition 1.2: Sei $n \in \mathbb{N}$. Eine Menge $\Sigma \coloneqq \{a_1, \ldots, a_n\}$ heißt **Alphabet**, falls jedes **Zeichen** a_i mit $1 \leq i \leq n$ einzigartig in Σ ist. Eine Zeichenfolge $\mathbf{w} \coloneqq w_1 w_2 \ldots w_l$ mit $l \in \mathbb{N}$ heißt **Wort**, wobei $w_j \in \Sigma$ für alle $1 \leq j \leq l$ ist.

Sei fortan $\mathbb{L} \coloneqq \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$ das Alphabet der 26 lateinischen Großbuchstaben. Eine Nachricht ist so durch Anpassen von Umlauten, Großbuchstaben, Wortzwischenräumen und Satzzeichen in ein Wort aus $\mathbb{L}$ überführbar und umgekehrt. Des Weiteren ist die Äquivalenz von Alphabeten ausschließlich von der Anzahl der Zeichen abhängig, wie die nachfolgende Definition verdeutlicht.

Definition 1.3: Sei $n \in \mathbb{N}$, und seien $\Sigma_A \coloneqq \{a_1, \ldots, a_n\}, \Sigma_B \coloneqq \{b_1, \ldots, b_n\}$ Alphabete. Eine Funktion der Form $\phi : \Sigma_A \to \Sigma_B, a_i \mapsto b_i$ mit $1 \leq i \leq n$ heißt **Codierung** über Σ_A und Σ_B. Ferner ist ein Wort $\mathbf{x} \coloneqq x_1 x_2 \ldots x_m$ mit $x_i \in \Sigma_A$ genau dann äquivalent zu $\mathbf{y} \coloneqq y_1 y_2 \ldots y_m$ mit $y_i \in \Sigma_B$, falls $\phi(x_i) = y_i$ für alle $1 \leq i \leq m$ gilt.

Sei $\mathbb{Z}_n \coloneqq \{0, \ldots, n-1\}$ mit $n \in \mathbb{N}$ und $n > 1$ ein Alphabet in n Zeichen. Dann ist durch nachfolgende Tabelle eine Codierung ψ über den Alphabeten $\mathbb{L}$ und $\mathbb{Z}_{26}$ gegeben.

Tabelle 1: Jeder Buchstabe entspricht der darunter stehenden Zahl

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Diese willkürlich gewählte Codierung erlaubt nun die numerische Betrachtung beliebiger Nachrichten. Nach Anpassen unzulässiger Zeichen entspricht eine Nachricht wie zum Beispiel „Seebär“ dem Wort $\mathbf{x} \coloneqq \mathtt{S\ E\ E\ B\ A\ E\ R}$. Insbesondere ist $\mathbf{x}$ bezüglich ψ äquivalent zu $\mathbf{y} \coloneqq \mathtt{18\ 4\ 4\ 1\ 0\ 4\ 17}$.

1.2 Public-Key-Kryptosystem

Nach der Festlegung eines Codes folgt nun eine Präzisierung von Definition 1.1 auf bestimmte Kryptosysteme, wo der Schlüsselaustausch über den unsicheren Kommunikationskanal stattfindet.

Definition 1.4: Ein **Public-Key-Kryptosystem** $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ bestimmt einen privaten Schlüssel $j \in \mathcal{K}$ zur Dechiffrierung und einen zugehörigen öffentlichen Schlüssel $k \in \mathcal{K}$ zur Chiffrierung. Die Dechiffrierungsregel $d_j : \mathcal{C} \to \mathcal{P}$ sei invers zur Chiffrierungsregel $e_k : \mathcal{P} \to \mathcal{C}$ mit $d_j(e_k(p)) = p$ für alle $p \in \mathcal{P}$ und $e_k(d_j(c)) = c$ für alle $c \in \mathcal{C}$. Insbesondere sei die Berechnung der inversen Funktion von e_j nur dann durchführbar, falls zusätzlich der private Schlüssel bekannt ist [1].

Eine Funktion mit der beschriebenen Eigenschaft heißt **Falltürfunktion**. Ferner ist die Zusatzinformation dann die **Falltür**. Basierend auf der Annahme, dass Falltürfunktionen existieren, ist der Schlüsselaustausch nun über einen unsicheren Kommunikationskanal realisierbar.

Bemerkung 1.5: Zu Beginn einigen sich Sender und Empfänger auf einen Code zur Nutzung in einem Public-Key-Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K})$. Sei $m \in \mathcal{P}$ die codierte Nachricht, die an den Empfänger zu senden ist.

1. Der Empfänger bestimmt einen privaten Schlüssel $j \in \mathcal{K}$ und einen öffentlichen Schlüssel $k \in \mathcal{K}$ mit $d_j(e_k(p)) = p$ für alle $p \in \mathcal{P}$.

2. Der Sender bestimmt die Chiffrierungsregel e_k durch den öffentlichen Schlüssel k. Nun ist der Sender in der Lage, Klartexte zu chiffrieren und so den Geheimtext $c \coloneqq e_k(m)$ zu versenden.

3. Der Empfänger dechiffriert den empfangen Geheimtext c gemäß $d_j(c)$, um wiederum m zu erhalten.

Da lediglich der Empfänger d_j kennt, ist in der Theorie die Kommunikation zwischen Sender und Empfänger abhörsicher. Allerdings bleibt fraglich, ob Falltürfunktionen wie in Definition 1.4 beschrieben in der Praxis existieren. Die moderne Kryptographie weitet deswegen den Begriff einer Falltürfunktion auch auf Funktionen aus, deren inverse Funktion nur mit einem hohen Rechenaufwand ohne Zusatzinformation zu bestimmen ist, da ein Unbefugter nur über begrenzte Ressourcen und Rechenleistung verfügt, ist diese Neudefinition sinnvoll.

2 Elementare Zahlentheorie

Das Rivest-Shamir-Adleman-Kryptosystem beruht auf etwaigen Überlegungen der elementaren Zahlentheorie, also der Studie der Phänomene ganzer Zahlen. Sei fortan $\mathbb{P}$ die Menge aller Primzahlen.

2.1 Faktorisierungsproblem

Grundlage für die Falltür des Rivest-Shamir-Adleman-Kryptosystems bildet das Faktorisierungsproblem, das auf klassischen Computern vermutlich nur schwer zu lösen ist [3].

Satz 2.1: Sei $n \in \mathbb{N}$ mit $n > 1$. Dann gibt es eindeutig bestimmte Primzahlen $p_1, \ldots, p_m \in \mathbb{P}$ mit $p_1 < \cdots < p_m$ und $e_1, \ldots, e_m \in \mathbb{N}$, sodass

$$n = p_1^{e_1} \cdots p_m^{e_m} = \prod_{k=1}^{m} p_k^{e_k}$$

für ein $m \in \mathbb{N}$ gilt.

Das Faktorisierungsproblem besteht darin, die **kanonische Primfaktorzerlegung** einer beliebigen Zahl effizient zu berechnen. Die Annahme ist nun, dass insbesondere für eine **Semiprimzahl** $N \coloneqq pq$ mit geeignet großen $p, q \in \mathbb{P}$ und $p \neq q$ die Berechnung der kanonischen Primfaktorzerlegung praktisch nicht durchführbar ist, also bei alleiniger Kenntnis von N weder p noch q bestimmbar ist.

Die Berechnung der kanonischen Primfaktorzerlegung einer Semiprimzahl mit 250 Dezimalstellen erforderte umgerechnet auf einem einzelnen 2,1 GHz Prozessor circa 2700 Jahre [4]. Heutzutage besitzen Semiprimzahlen in kryptographischen Anwendungen typischerweise 617 Dezimalstellen.

2.2 Euler'sche Funktion

Als Nächstes ist basierend auf der Annahme, dass das Faktorisierungsproblem für Semiprimzahlen mit exorbitanten Primfaktoren nahezu unlösbar ist, eine Falltür zu finden.

Definition 2.2: Für alle $n \in \mathbb{N}$ entspricht die **Euler'sche Funktion** $\varphi(n)$ der Anzahl der zu n teilerfremden Zahlen in $\mathbb{Z}_n$, also $\varphi : \mathbb{N} \to \mathbb{N}, n \mapsto \varphi(n) \coloneqq |\{z \in \mathbb{Z}_n \mid \mathrm{ggT}(n, z) = 1\}|$.

Abbildung 1: Graph der Euler'schen Funktion

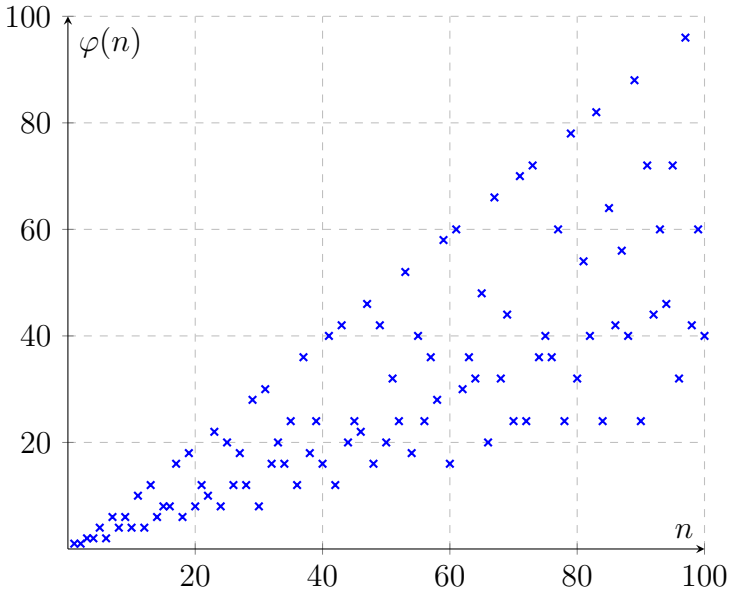


Abbildung 1 offenbart, dass die Euler'sche Funktion in der Regel keineswegs trivial zu berechnen ist. Doch diese Funktion besitzt auch einige besonders schöne Eigenschaften, die die Rechenkomplexität immens verringern: so gilt zum Beispiel $\varphi(p) = |\mathbb{Z}_p| = p-1$ für alle $p \in \mathbb{P}$ wie leicht anhand von Definition 2.2 zu verifizieren ist. Für Semiprimzahlen existiert ein ähnliches Resultat, wie die nachfolgende Bemerkung darlegt.

Bemerkung 2.3: Sei $N := pq$ eine Semiprimzahl mit $p, q \in \mathbb{P}$ und $p \neq q$. Dann gilt $\varphi(N) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Beweis: Sei $P := \{z \in \mathbb{Z}_N \mid \text{ggT}(pq, z) = p\} = \{p, 2p, \ldots, (q-1)p\}$, und sei $Q := \{z \in \mathbb{Z}_N \mid \text{ggT}(pq, z) = q\} = \{q, 2q, \ldots, (p-1)q\}$. Dann gilt

$$\begin{aligned}
\varphi(N) &= |\{z \in \mathbb{Z}_N \mid \text{ggT}(N, z) = 1\}| \\
&= |\mathbb{Z}_N| - |P| - |Q| \\
&= (pq - 1) - (q - 1) - (p - 1) \\
&= pq - p - q + 1 \\
&= (p - 1)(q - 1),
\end{aligned}$$

da $P \cap Q = \emptyset$ und $\text{ggT}(N, z) = 1$ für alle $z \in \mathbb{Z}_N \setminus (P \cup Q)$ ist. □

Für Semiprimzahlen ist die Euler'sche Funktion dann leicht kalkulierbar, wenn die kanonische Primfaktorzerlegung bekannt ist. Doch für Semiprimzahlen mit zu enormen Primfaktoren ist nach Annahme das Faktorisierungsproblem schwer zu lösen, was wiederum die Berechnung praktisch unmöglich macht.

Demnach ist die Euler'sche Funktion in diesen Fällen eine Falltür. Abschließend ist noch eine zentrale Eigenschaft der Euler'schen Funktion im weiteren Sinne von Interesse.

Satz 2.4: Sei $n \in \mathbb{N}$ mit $n > 1$, und sei $a \in \mathbb{Z}$ teilerfremd zu n. Dann gilt $a^{\varphi(n)} \bmod n = 1$.

Vorweg basiert die Korrektheit des Rivest-Shamir-Adleman-Kryptosystems auf diesem Satz. Eine weitere Konsequenz ist das effiziente Berechnen modularer Inverse, wie die nachfolgende Bemerkung beweist.

Bemerkung 2.5: Sei $n \in \mathbb{N}$ mit $n > 1$, und sei $a \in \mathbb{Z}$ teilerfremd zu n. Dann gibt es ein $a^{-1} \in \mathbb{Z}$ mit $aa^{-1} \bmod n = 1$.

Beweis: Nach Satz 2.4 gilt $a^{\varphi(n)} \bmod n = 1 \Leftrightarrow aa^{\varphi(n)-1} \bmod n = 1$. Folglich ist $a^{-1} \coloneqq a^{\varphi(n)-1} \bmod n$ dann invers zu a.

Der Zusammenhang zwischen öffentlichem und privatem Schlüssel des Rivest-Shamir-Adleman-Kryptosystems entspricht genau dieser Bemerkung.

3 Rivest-Shamir-Adleman-Kryptosystem

Mithilfe der zahlentheoretischen Überlegungen folgt nun eine präzise Definition des Rivest-Shamir-Adleman-Kryptosystems.

Definition 3.1: Sei $N \coloneqq pq$ eine Semiprimzahl mit $p, q \in \mathbb{P}$ und $p \neq q$. Ferner sei $\mathcal{R} \coloneqq \mathbb{Z}_N$ die Menge aller Klartexte, $\mathcal{S} \coloneqq \mathbb{Z}_N$ die Menge aller Geheimtexte und $\mathcal{A} \coloneqq \{k \in \mathbb{Z}_{\varphi(N)} \mid \mathrm{ggT}(\varphi(N), k) = 1\}$ die Menge aller Schlüssel. Das Rivest-Shamir-Adleman-Kryptosystem $(\mathcal{R}, \mathcal{S}, \mathcal{A})$ definiert eine Chiffrierungsregel $E : \mathcal{R} \to \mathcal{S}, m \mapsto m^e \bmod N$ und Dechiffrierungsregel $D : \mathcal{S} \to \mathcal{R}, c \mapsto c^d \bmod N$ für $e, d \in \mathcal{A}$ mit $ed \bmod \varphi(N) = 1$ [5].

Per Definition ist der private Schlüssel d invers zum öffentlichen Schlüssel e. Ist e vorgegeben, so gilt nach Bemerkung 2.5 folglich

$$d \coloneqq e^{\varphi(\varphi(N))-1} \bmod \varphi(N) = e^{\varphi((p-1)(q-1))-1} \bmod ((p-1)(q-1)) .$$

Folglich ist die Chiffrierungsregel E, die e und N offenbart, unzureichend um die Dechiffrierungsregel D praktisch zu berechnen. Gemäß der Neudefinition ist E eine Falltürfunktion, sofern D invers zu E ist.

3.1 Korrektheit

Nicht zuletzt ist zu zeigen, dass das Rivest-Shamir-Adleman-Kryptosystem wie behauptet funktioniert.

Satz 3.2: Sei $N \coloneqq pq$ eine Semiprimzahl mit $p, q \in \mathbb{P}$ und $p \neq q$. Gilt $d \coloneqq a \bmod p = a \bmod q$ für ein $a \in \mathbb{Z}$, dann folgt $d = a \bmod N$.

Die Korrektheit ist nachfolgend beschrieben und bewiesen unter obenstehender Voraussetzung.

Bemerkung 3.3: Sei $N \coloneqq pq$ eine Semiprimzahl mit $p, q \in \mathbb{P}$ und $p \neq q$. Ferner seien $e, d \in \{z \in \mathbb{Z}_{\varphi(N)} \mid \mathrm{ggT}(N, z) = 1\}$ mit $ed \bmod \varphi(N) = 1$. Zu zeigen ist, dass $m^{ed} \bmod N = m \bmod N$ für alle $m \in \mathbb{Z}_N$ gilt.

Beweis: Zu Beginn ist $m^{ed} \bmod p = m \bmod p$ zu verifizieren. Vorweg ist festzuhalten, dass $ed \bmod \varphi(N) = 1 \Leftrightarrow ed = 1 + t\varphi(N)$ für ein $t \in \mathbb{N}$ gilt. Daraus folgt

$$m^{ed} \bmod p = m \left(m^{t\varphi(N)}\right) \bmod p.$$

Ist $m \bmod p = 0$, so gilt offensichtlich $m^{ed} \bmod p = 0$. Andernfalls ist $m \bmod p \neq 0$, sodass nach Satz 2.4 folglich

$$\begin{aligned} m \left(m^{t\varphi(N)}\right) \bmod p &= m \left(m^{t\varphi(p)\varphi(q)}\right) \bmod p \\ &= m \left(1^{t\varphi(q)}\right) \bmod p \\ &= m \bmod p \end{aligned}$$

gilt, denn m ist genau dann teilerfremd zu p. Durch Symmetrie folgt ebenso $m^{ed} \bmod q = m \bmod q$, wodurch sofort $m^{ed} \bmod N = m \bmod N$ mit Satz 3.2 folgt. □

3.2 Visualisierung

Folgend ist das Wort $\mathbf{u} \coloneqq \mathtt{S}$ beispielhaft chiffriert. Nach Tabelle 1 ist $\mathbf{u}$ äquivalent zu $\mathbf{v} \coloneqq \psi(\mathtt{S}) = \mathtt{18}$. Sei fortan $N \coloneqq 3 \cdot 11 = 33$ eine Semiprimzahl, und sei $e \coloneqq 3$ der öffentliche Schlüssel. Für $\varphi(33) = \varphi(3)\varphi(11) = 2 \cdot 10 = 20$ ist folglich $d \coloneqq 3^{\varphi(33)-1} \bmod \varphi(33) = 3^{19} \bmod 20 = 7$ der private Schlüssel. Demnach ist die Chiffrierungsregel $E : \mathbb{Z}_{33} \to \mathbb{Z}_{33}, m \mapsto m^3 \bmod 33$, während die Dechiffrierungsregel $D : \mathbb{Z}_{33} \to \mathbb{Z}_{33}, c \mapsto c^7 \bmod 33$ entspricht. Chiffriert ergibt $\mathbf{v}$ dann $\mathbf{w} \coloneqq E(18) = 18^3 \bmod 33 = 24$. Selbstverständlich ist $\mathbf{w}$ wiederum dechiffriert $\mathbf{v}$, also $D(24) = 24^7 \bmod 33 = 18$.

Abschließend ist die modulare Multiplikation anhand einer Analoguhr anschaulich dargestellt.

Abbildung 2: Zifferblatt einer Analoguhr

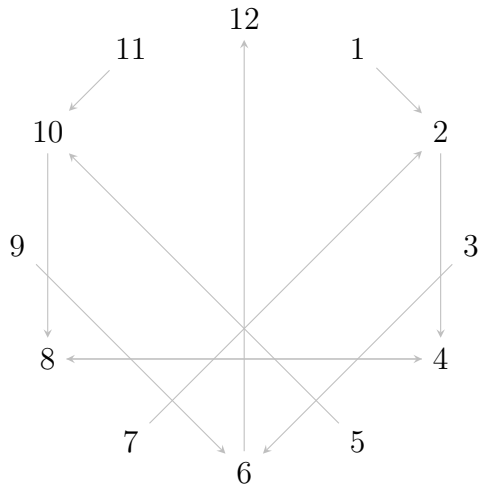
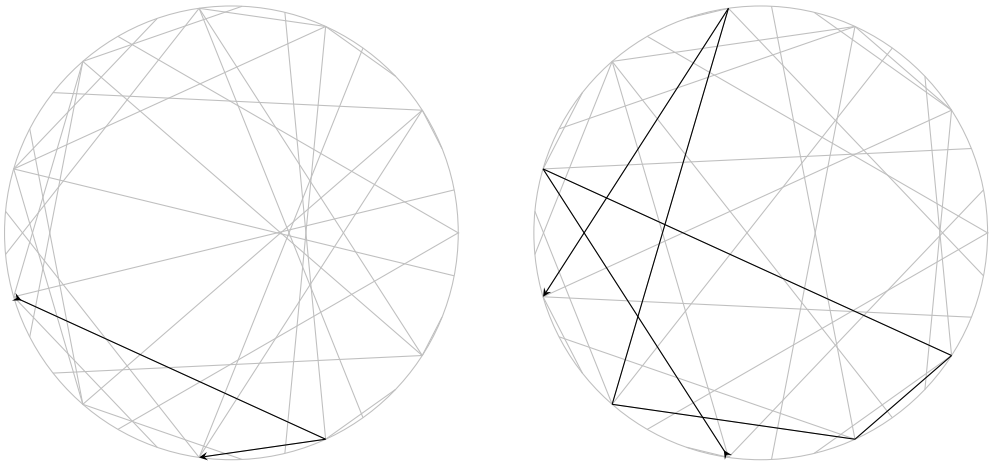


Abbildung 2 stellt jede Multiplikation mit 2 durch einen Pfeil dar, wobei der Zahlenbereich auf 12 beschränkt ist. So entspricht $2^3 \cdot 5$ Uhr natürlich nicht 40 Uhr, sondern 4 Uhr. Des Weiteren besteht hier die Möglichkeit, den Zahlenbereich beliebig zu erweitern.

Abbildung 3: Zifferblätter erweitert auf 33 Ziffern



$E(18) = 18^3 \bmod 33 = 24$ $\qquad$ $D(24) = 24^7 \bmod 33 = 18$

Bezugnehmend auf das vorherige Beispiel ist links die Chiffrierung und rechts die Dechiffrierung dargestellt. Links repräsentiert jede graue Linie eine Multiplikation mit 18. Rechts ist dagegen eine Multiplikation mit 24 dargestellt. Der schwarze Pfad repräsentiert gerade den Sonderfall der modularen Exponentiation, also die Chiffrierung beziehungsweise Dechiffrierung.

Referenzen

[1] Diffie Whitefield and Martin Hellman. New Directions in Cryptography, November 1976. ee.stanford.edu/~hellman/publications/24.pdf (Zugriff am 15. Februar 2022).

[2] Ronald Rivest, Adi Shamir, and Len Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, 1977. people.csail.mit.edu/rivest/Rsapaper.pdf (Zugriff am 16. Januar 2022).

[3] Joakim Nilsson. Integer factorization algorithms, 2020. umu.diva-portal.org/smash/record.jsf?pid=diva2:1460632 (Zugriff am 3. März 2022).

[4] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Emmanuel Thomé Nadia Heninger, and Paul Zimmermann. Factorization of RSA-250, February 2020. sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html (Zugriff am 16. März 2022).

[5] Kathleen Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016. www.rfc-editor.org/info/rfc8017 (Zugriff am 15. Februar 2022).