Vortragszusammenfassung Leoben, den 10.04.2025

Karoline Moser

Kryptographie – Die sichere Brücke im digitalen Zeitalter?!

Kryptographie ist eine seit Jahrhunderten perfektionierte Kunst und Wissenschaft zum Schutz von Informationen. Es ist eine Disziplin, die unsichtbar, aber essenziell ist für unser Leben im digitalen Zeitalter. Wenn wir heute online shoppen, Nachrichten verschicken oder Banking-Apps benutzen – überall ist Kryptographie im Spiel.

Sie ist die unsichtbare Brücke, die Vertrauen schafft, wo sich Menschen nie persönlich begegnen – von WhatsApp bis zu Bitcoin. Und diese Brücke muss sicher, stabil und effizient sein. Die moderne Kryptographie, vertreten in diesem Vortrag durch RSA- und Elliptische-Kurven-Kryptosysteme, befindet sich inmitten von signifikanten Herausforderungen und Entwicklungen.

Ver- & Entschlüsselung

Reinhart verschlüsselt eine Nachricht mit einem Algorithmus und einem Schlüssel und sendet den Chiffretext an Lisa, die ihn mit einem Schlüssel entschlüsselt. Bei Private-Key-Kryptographie ist der Schlüssel identisch, bei Public-Key-Kryptographie verschieden. Diffie und Hellman [3] begründeten das Public-Key-Prinzip, auf dem RSA von Rivest, Shamir und Adleman basiert [8]. Der Fokus dieses Vortrags liegt auf der Public-Key-Kryptographie, insbesondere auf den Kryptosystemen RSA und Elliptische Kurven Kryptographie (Elliptic Curve Cryptography, ECC). Neal Koblitz [6] und Victor Miller [7] haben unabhängig voneinander vorgeschlagen, elliptische Kurven in der Kryptographie zu verwenden.

Cäsar Verschlüsselung

Der römische Feldherr Gaius Julius Cäsar wollte bereits geheime Botschaften an seine Truppen senden, ohne dass sie vom Feind gelesen werden konnten. Er verschob jeden Buchstaben um dieselbe Anzahl von Stellen. Dieses Verfahren gehört zur Private-Key-Kryptographie, da Sender und Empfänger denselben geheimen Schlüssel kennen müssen. Heute lässt sich eine solche Verschlüsselung in weniger als einer Sekunde knacken [5].

Beispiel einer Cäsar-Verschlüsselung mit Verschiebung um 3 Stellen: Aus „LEOBEN“ wird „OHREHQ“.

RSA-Kryptographie

RSA ist ein bewährtes Verfahren, das auf einem simplen Prinzip basiert: Es ist sehr einfach, zwei große Zahlen miteinander zu multiplizieren. Es ist aber extrem schwer, das Ergebnis wieder zurückzurechnen, also die ursprünglichen Zahlen zu finden [5].

Ablauf der RSA-Kryptographie:

1. **Schlüsselerzeugung**
    a. Lisa wählt zwei große Primzahlen **p** und **q**.
    b. Lisa berechnet **N = p q**.
    c. Lisa wählt eine Zahl **e**, die teilerfremd zu **(p-1)(q-1)** ist.
    d. Lisa berechnet **d**, sodass **e d = 1 mod (p-1)(q-1).**
    e. Der öffentliche Schlüssel ist somit **(e, N)** und der private Schlüssel von Lisa ist **(d, N)**.
2. **Verschlüsselung**
    a. Reinhart wandelt die Nachricht z.B. „Leoben“ in eine Zahl **M** um.
    b. Die verschlüsselte Nachricht **C** ist **C = M^e mod N**, die Reinhart an Lisa schickt.
3. **Entschlüsselung**
    a. Lisa berechnet **M= C^d mod N**, um **M** zu erhalten.

Elliptische Kurven Kryptographie

Elliptische Kurven Kryptographie (ECC) nutzt die Eigenschaften elliptischer Kurven. Eine solche Kurve über die Reellen Zahlen wird in der allgemeinen Form $y^2 = x^3 + Ax + B$ dargestellt, wobei A und B (reelle) Koeffizienten sind, die $4A^3 + 27B^2 \neq 0$ erfüllen müssen, um Singularitäten zu vermeiden. Diese Kurven sind symmetrisch bezüglich der x-Achse, und jede nicht senkrechte Gerade schneidet sie genau dreimal, wobei die Berührungspunkte bei Tangenten doppelt gezählt werden. Eine elliptische Kurve in der ECC wird über einem endlichen Körper definiert, eine algebraische Struktur, die grundlegende arithmetische Operationen ermöglicht [2, 5].

Durch die Eigenschaften elliptischer Kurven lässt sich die Punktaddition definieren. Eine Gerade durch zwei Punkte P und Q auf der Kurve schneidet die Kurve in einem dritten Punkt (-R), dessen Spiegelung R das Additionsergebnis ist.

In der ECC wird ein Generatorpunkt G mit einem Skalar d multipliziert, um Punkte wie 2G, 3G usw. zu erzeugen. Selbst wenn G und dG bekannt sind, ist es extrem schwer d zu bestimmen. Der Multiplikationsfaktor d ist der private Schlüssel. Der Punkt, also dG, kann öffentlich bekannt sein, aber d, der Multiplikationsfaktor, muss geheim bleiben. Dieses sogenannte Elliptic Curve Discrete Logarithm Problem (ECDLP) bildet die Grundlage der Sicherheit in der ECC [4].

Ablauf der ECC:

1. **Schlüsselerzeugung**
    a. Lisa wählt eine elliptische Kurve und einen Punkt **G** auf dieser Kurve.
    b. Lisa wählt eine zufällige Zahl **d** als privaten Schlüssel.
    c. Der öffentliche Schlüssel von Lisa ist **Q = dG**, ein Punkt auf der elliptischen Kurve.
2. **Verschlüsselung**
    a. Reinhart wandelt die Nachricht z.B. „Leoben“ in einen Punkt **M** auf der elliptischen Kurve um.

   b. Reinhart wählt eine zufällige Zahl **k**.
   c. Reinhart berechnet $\mathbf{R_1 = kG}$ und $\mathbf{R_2 = M + kQ}$.
   d. Die verschlüsselte Nachricht ist $\mathbf{(R_1, R_2)}$, die Reinhart an Lisa schickt.
3. **Entschlüsselung**
   a. Lisa berechnet $\mathbf{dR_1 = dkG = kdG = kQ}$.
   b. Die entschlüsselte Nachricht ist $\mathbf{M = R_2 - dR_1 = R_2 - kQ = M + kQ - kQ}$.

Sicherheitsanalyse

Die Sicherheit kryptographischer Systeme kann durch das Lösen der zugrundeliegenden mathematischen Probleme oder durch Designfehler gefährdet werden. Lokale Kopien von Nachrichten oder sensiblen Daten, die während der Ver- oder Entschlüsselung erstellt werden, stellen eine besondere Gefahr dar und müssen sicher gelöscht werden.

Für Verfahren wie RSA und Elliptische Kurven Kryptographie sind *Side-Channel Attacks* riskant. Hierbei werden Informationen aus Nebenkanälen, wie Stromverbrauch oder elektromagnetische Emissionen, analysiert, um Rückschlüsse auf Schlüssel zu ziehen.

Ein kryptographisches System ist nur so sicher wie sein schwächstes Glied. Der menschliche Faktor, etwa der unvorsichtige Umgang mit privaten Schlüsseln, kann oft das größte Risiko darstellen, wodurch selbst robuste und sichere Systeme kompromittiert werden können [2].

Vergleichsanalyse

RSA stützt seine Sicherheit auf die Komplexität der Faktorisierung großer Zahlen und benötigt daher große Primzahlen, um robust zu sein. ECC ermöglicht kürzere Schlüssellängen, was in puncto Geschwindigkeit und Effizienz von Vorteil ist [4].

Bei der Anwendung der Elliptischen Kurven Kryptographie ist die Auswahl einer sicheren Kurve und eines geeigneten Generatorpunkts entscheidend. Es wird geraten, standardisierte und bewährte Kurven zu verwenden. Dank der höheren Effizienz dieses Systems können kürzere Schlüssel verwendet werden, was zu Einsparungen bei Rechenleistung, Bandbreite und Speicher führt [1].

Literaturverzeichnis

[1] Elaine Barker. SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 - General. Tech. rep. Gaithersburg, MD, USA, May 2020. URL: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[2] Duncan Buell. Fundamentals of Cryptography. Springer Nature Switzerland AG, 2021. ISBN: 978-3030734916

[3] Whitfield Diffie and Martin E. Hellman. ”New directions in cryptography”. In: IEEE Transactions on Information Theory 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[4] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, 2004. ISBN: 978-1441929297

[5] Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC Press, 2021. ISBN: 978-1-4665-7027-6

[6] Neal Koblitz. “Elliptic Curve Cryptosystems”. In: Mathematics of Computation 48.177 (1987), pp. 203–209. ISSN: 00255718.

[7] Victor S. Miller. “Use of Elliptic Curves in Cryptography”. In: Advances in Cryptology — CRYPTO ’85 Proceedings. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1.

[8] Ron L. Rivest, Adi Shamir, and Len Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: Commun. ACM 21.2 (Feb. 1978), 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342.