Mathematische Grundlage der Kryptografie

Martin Schuchardt, Matrikelnummer 1216705

4. Juni 2014

1 Einleitung

Die Kryptographie beschäftigt sich mit dem Sichern von Informationen vor unbefugtem lesenden und schreibenden Zugriff. Dies umfasst außerdem noch den Schutz der Integrität von Informationen und der eindeutigen Identifikation des Urhebers. Zusammen mit der Kryptoanalyse, welche sich mit dem Entschlüsseln und somit der Sicherheit der Algorithmen beschäftigt, bildet sie das Themengebiet der Kryptologie.

Im folgenden werden Teile der mathematischen Grundlage der Kryptografie aufgezählt, anhand von Beispielen deren Zusammenhang mit mathematischen Methoden erklärt und mit diesem Basiswissen ein Einblick in moderne Verschlüsselungstechniken am Beispiel RSA gewagt.

2 Algebra der Kryptografie

Zum Verschlüsseln von Informationen wird aus einer Menge an Zeichen aus einem endlichen Alphabet eine Nachricht erstellt und diese mit einem Schlüssel und einem Algorithmus codiert. Das Ergebnis, die verschlüsselte Nachricht, auch Kryptogramm genannt, besteht wiederum aus einer Anzahl an Zeichen aus dem vordefinierten Eingabealphabet. Die Verschlüsselung ist eine mathematische Abbildung f, welche eine Nachricht aus der Definitionsmenge $\mathbf{M}$, bestehend aus einer festgelegten Anzahl an Zeichen aus dem Eingabealphabet $m_0,\ m_1,\ m_2,\ \ldots$ mit dem Schlüssel $\mathbf{K}$ in eine Zeichenfolge $e_0,\ e_1,\ e_2,\ \ldots$ der Bildmenge $\mathbf{E}$ transformiert.

$$f\colon \mathbf{M} \times \mathbf{K} \to \mathbf{E}\colon \quad (m_i, k) \mapsto f(m_i, k) = e_i \qquad \text{für } i \in \mathbb{N}_0 \tag{1}$$

Um die Dekodierung zu gewährleisten muss sichergestellt werden, dass

- aus jeder Kombination von Schlüssel und Nachricht genau ein Kryptotext abgeleitet werden kann
- kein Kryptotext aus zwei verschiedenen Paaren von Schlüssel und Klartext Nachricht erzeugt wird

- aus einem Kryptotext mithilfe des Algorithmus und dem entsprechenden Schlüssel genau ein Klartext berechnet wird.

Kryptographische Algorithmen werden oftmals kombiniert um bessere Ergebnisse zu erzielen. Eine Funktion welche die Definition (1) erfüllt ist bijektiv. Um die Hintereinanderausführung zu gewähren muss zusätzlich die Bildmenge der ersten Funktion mit der Definitionsmenge der zweiten übereinstimmen, bei beliebigen Kombinationen müssen Bildmenge und Definitionsmenge der verwendeten Funktionen identisch sein. Diese Eigenschaften werden als homomorph bezeichnet. Details zur Definition findet man in „Communication Theory of Secrecy Systems“ (vgl. C. Shannon 1949 [4]).

3 Einfache Chiffrierungsverfahren

Die ausgewählten Beispiele dieses Kapitels sollen die Anwendung der mathematischen Operationen demonstrieren. Der interessierten Leserin empfehle ich das Kapitel 4 aus [4].

3.1 Substitution

Diese Chiffre tauscht einzelne Zeichen des Eingabealphabets durch ein fixes Substitutionszeichen aus: $E = e_0e_1e_2e_3\cdots = f(m_0)f(m_1)f(m_2)f(m_3)\ldots$ Das Ergebnis E ist eine Permutation des Eingabealphabets und die Chiffrierung ist umkehrbar durch $f^{-1}(m_i) = e_i$.

3.2 Transposition - Permutation

Die Botschaft wird in Gruppen einer fixen Länge unterteilt und jede Gruppe mit einer fixen Permutation neu geordnet:

Beispiel 3.1 *Für eine Länge $d = 5$ könnte die Permutation 1 2 0 4 3 lauten:*

m_0	m_1	m_2	m_3	m_4		m_5	m_6	m_7	m_8	m_9	wird zu
m_1	m_2	m_0	m_4	m_3		m_6	m_7	m_5	m_9	m_8	

3.3 Vigenère und Variationen - Grundrechenarten, Modulo

Die Zeichen der Botschaft werden um einen fixen Wert verschoben, beispielsweise wird der Zahlenwert von Buchstaben aus dem ASCII-Zeichensatz mit der Chiffrierungsfunktion $e_i = m_i + k_i \pmod{26}$ verändert:

Beispiel 3.2 *Als Schlüssel dient „GAH“*

Botschaft:	*N*	*O*	*W*	*I*	*S*	*T*	*H*	*E*
Schlüssel:	*G*	*A*	*H*	*G*	*A*	*H*	*G*	*A*
Kryptogramm:	*T*	*O*	*D*	*O*	*S*	*A*	*N*	*E*

Eine Variante der Vigenère Verschlüsselung ist die bekannte Caesar-Verschlüsselung, bei der ein Schlüssel der Länge Eins verwendet wird.

4 Asymmetrische Verschlüsselungsverfahren

Eine der größten Schwierigkeiten bei symmetrischen Verschlüsselungsverfahren stellt der Austausch des Schlüssels dar. Sobald alle Teilnehmer in Besitz des Schlüssels sind können Nachrichten sicher übertragen werden, aber im speziellen der Schlüssel darf nicht in falsche Hände geraten und muss gesichert übertragen werden - ein Teufelskreis.

Asymmetrische Verfahren verwenden zwei Schlüssel, den public und den private key. Eine mit dem public key verschlüsselte Nachricht kann nur mit dem private key wieder entschlüsselt werden. Der Algorithmus lässt sich auch mit vertauschten Schlüsseln verwenden: ein mit dem private key verschlüsselter Text kann mit dem public key entschlüsselt werden - diese Variante wird für elektronische Signaturen eingesetzt.

Eines der ersten praktisch anwendbaren asymmetrischen Kryptosysteme war RSA [3] auf Basis der Arbeit von Diffie und Hellman [1].

Der Algorithmus verwendet zwei Primzahlen beliebiger Länge, aus deren Produkt das Zahlenpaar für die beiden Schlüssel bestimmt wird. Die Sicherheit der Codierung ist gegeben da für die Kryptoanalyse die Faktorisierung des Primzahlenproduktes durchgeführt werden müsste. Die Komplexität dieses Problems wird in der Klasse NP vermutet und es ist bisher kein Verfahren bekannt welches Zahlen in polynomieller Zeit faktorisieren kann. Sofern entsprechend lange Zahlen verwendet werden erfordert das Brechen des Primzahlenproduktes auch mit modernster Hardware einen sehr hohem Zeitaufwand. RSA768, eine Primzahl mit 232 Stellen, wurde 2009 in 3 Jahren mit einer Rechenleistung von 2000 2.2 GHz-Opteron-CPU Jahren geknackt[1]. Solange kein effizienterer Algorithmus gefunden wird gilt RSA deshalb als sicher, empfohlen wird eine Schlüssellänge ab 3072 Bit[2].
Zur Verschlüsselung wird die Nachricht M in Form von Integer Blöcken repräsentiert. Die codierte Botschaft C wird aus der e-ten Potenz von M modulo n gebildet, zum Entschlüsseln wird der mit d potenzierte Kryptotext modulo n berechnet.

$$\mathbf{C} \equiv \mathbf{E}(\mathbf{M}) \equiv \mathbf{M}^e \pmod{n} \text{ zum verschlüsseln}$$
$$\mathbf{D}(\mathbf{C}) \equiv \mathbf{C}^d \pmod{n} \text{ zum entschlüsseln}$$

Der öffentliche Schlüssel besteht aus (e, n), der private aus (d, n). n ist das Produkt zweier zufällig gewählter, großer Primzahlen p und q:

$$n = p \cdot q$$

Die Komponente d des privaten Schlüssels wird zufällig gewählt, muss aber teilerfremd zu $(p-1) \cdot (q-1)$ sein:

$$\mathrm{ggT}(d, (p-1) \cdot (q-1)) = 1$$

[1] www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge.htm
[2] www.nsa.gov/business/programs/elliptic_curve.shtml

e ist das multiplikative inverse[3] zu d und erfüllt das Kongruenzsystem

$$e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$$

Zum besseren Verständnis kann die Leserin ein einfaches Beispiel selbst rechnen, mit den Primzahlen $p = 47$ und $q = 59$ sowie der Wahl von $d = 157$ sollte $e = 17$ als öffentliche Schlüsselkomponente ermittelt werden. Die Lösung liefert Kapitel 8 aus [3] oder auch Wikipedia [4]. Die mathematischen Grundlagen der Zahlentehorie sollten aus der diskreten Mathematik bekannt sein [2].

5 Schlussfolgerung

Solange das Problem der Faktorisierung nicht effizient gelöst wird, dürfte die Verschlüsselung mit RSA ausreichend sicher sein. In der Vergangenheit wurden die Methoden und die Rechenleistung der Computer schrittweise verbessert, sollte sich eine Gefährdung abzeichnen wird vermutlich noch ausreichend Zeit zur Verfügung stehen um alternative Methoden wie beispielsweise diskreten Logarithmen auf elliptischen Kurven[5] einzusetzen.

Dass geheime Nachrichten in der Zukunft möglicherweise mit vertretbarem Aufwand massenhaft entschlüsselbar sind widerspricht dem Begriff „sicher“ jedoch. Organisationen wie die NSA bewahren verschlüsselte, verdächtige Nachrichten in der Hoffnung diese irgendwann einmal effizient Dekodieren zu können in ihren Archiven vorsichtshalber bereits auf[6].

Literatur

[1] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[2] A. Dür, G. Moser, and H. Zankl. Diskrete Mathematik für Informatiker. skriptum zur vorlesung, 2. auflage, 2013.

[3] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[4] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, Oktober 1949.

[3] Die Berechnung erfolgt mithilfe des erweiterten Euklidischen Algorithmus.
[4] http://en.wikipedia.org/wiki/RSA_cryptosystem
[5] Grundlage zur Schlüsselgenerierung bei der Elliptic Curve Cryptography (ECC)
[6] http://heise.de/-2171858