Einleitung

In dieser Einleitung wird ein Überblick über die grundlegenden Fragestellungen und Methoden der Kryptographie gegeben.

1.1 Zielsetzung der Kryptographie

Die moderne Kryptographie beschäftigt sich mit der sicheren Informationsübertragung im weiteren Sinne zwischen logischen Einheiten. Solche logischen Einheiten können zum Beispiel Personen oder Computer sein. Eine der grundlegenden und namensgebenden Fragestellungen ist, wie zwei Personen Informationen austauschen können, ohne daß eine mithörende dritte Person diese Informationen erhalten kann. Dabei geht es nicht darum, wie man das Mithören der dritten Person verhindern kann, sondern wie sich die kommunizierenden Personen zu verhalten haben, so daß das Mithören keinen Informationsgewinn bringt.

Die zwei wichtigsten, praktischen Fragestellungen der Kryptographie sind etwa

1. Verschlüsselung, Geheimhaltung. Nur der rechtmäßige Empfänger soll verschlüsselte Daten entschlüsseln bzw. überhaupt nur irgendwelche Informationen aus den verschlüsselten Daten erhalten können.

2. Unterschriften, Signaturen. Alle Personen sollen die Signatur einer Person unter einem Dokument verifizieren, aber niemand soll das Dokument ändern oder die Signatur fälschen können.

Signaturen basieren auf den Teilaspekten Authentizität, Datenintegrität und Nichtzurückweisbarkeit. Darüberhinaus gibt es eine ganze Reihe weiterer Fragestellungen wie zum Beispiel den Austausch von Geheimnissen (Schlüsselaustausch), Revokation (Schlüsselentzug), Anonymität (elektronisches Geld) usw. Der Phantasie und den Anwendungen sind hier wenig Grenzen gesetzt. Die Untersuchung solcher praktischen Fragestellungen führt zu grundlegenden Objekten wie Einweg-Funktionen und Pseudozufallsgeneratoren.

Von den methodischen Ansätzen her kann man die Kryptographie in Kryptographie im spezielleren Sinn und Kryptanalyse unterteilen. Die Kryptographie

im spezielleren Sinn beschäftigt sich mit dem eigentlichen Entwurf von Kryptosystemen, also Methoden zur Lösung obenstehender Aufgaben, während die Kryptanalyse versucht, diese Kryptosysteme zu „knacken“. Diese beiden Ansätze werden auch unter dem Begriff Kryptologie zusammengefaßt, den wir hier synomym mit Kryptographie verwenden.

Geschichtlich gesehen ist die Kryptographie eine alte Disziplin und wurde in Ansätzen und unsystematisch bereits in der Antike, unter anderem von Cäsar, verwendet. Seit dem 20. Jahrhundert findet eine Systematisierung und Formalisierung statt. Eine wichtige Rolle spielte die Kryptographie und insbesondere die Kryptanalyse im 2. Weltkrieg, wo erstmalig Rechenmaschinen zum Einsatz kamen. Die deutsche Chiffriermaschine „Enigma“ wurde von Polen und Briten (unter diesen A. Turing) geknackt. Bis in die 60er Jahre wurde Kryptographie hauptsächlich von Regierungen und Militärs betrieben, die dann einsetzende Verbreitung von Computern führte zu verstärkten Anforderungen aus dem privaten (industriellen) Sektor. Mitte der 70er Jahre erschien die richtungsweisende Arbeit „New directions in cryptography“ von Diffie und Hellman, welche die Kryptographie mit öffentlichem Schlüssel einführte und als Begründung der modernen Kryptographie angesehen werden kann. Eine wichtige Entdeckung in den 80er Jahren sind die Zero-Knowledge-Protokolle, in den 90er Jahren findet mit Computern, Internet, Geldautomaten, Mobilfunk usw. eine massenhafte Verbreitung der Kryptographie statt.

Die Kryptographie befaßt sich heute im wesentlichen mit Algorithmen, Computern und der digitalen Kommunikation und ist ein eigenständiges, interdisziplinäres Gebiet mit Verbindungen zur theoretischen Informatik, Mathematik, Software Engineering, Elektrotechnik, Quantenphysik.

1.2 Fachliche Unterteilung

Bezüglich des „Touch-and-feel“ der verwendeten Methoden kann man die Kryptographie grob wie folgt unterteilen.

Theoretische Grundlagen aus der Informatik Hierzu gehören neben anderem Informationstheorie und Untersuchungen über Einwegfunktionen, Pseudozufallsgeneratoren, probabilistische interaktive Beweise wie zum Beispiel Zero-Knowledge Beweise. Dabei geht es häufig um das Auffinden der richtigen Definitionen („Was ist Sicherheit?“) sowie um Grundlagen- und Machbarkeitsresultate für kryptographische Aufgaben.

Symmetrische Kryptoverfahren (Secret Key) Dies sind spezielle Verfahren zur Verschlüsselung (Block- und Stromchiffren) und Authentifizierung (Mes-

sage Authentication Codes MACs, ferner Hashfunktionen), bei denen man im allgemeinen davon ausgeht, daß die kommunizierenden Personen sich einen geheimen Schlüssel teilen. Ein Schlüssel ist einfach eine digitale Information. Die Untersuchung der Sicherheit dieser Verfahren basiert mehr oder weniger auf statistischen Methoden und ist im wesentlichen heuristisch. Symmetrische Kryptoverfahren sind im allgemeinen effizienter als die asymmetrischen Kryptoverfahren.

Asymmetrische Kryptoverfahren (Public Key) Hier sind jeder Person ein öffentlicher (allen Personen bekannter) und ein geheimer Schlüssel zugeordnet. Darauf aufbauend betreibt man dann Verfahren zur Verschlüsselung, zum Unterschreiben und zum Schlüsselaustausch geheimer Schlüssel für symmetrische Kryptoverfahren. Die Untersuchung der Sicherheit dieser Verfahren basiert im wesentlichen auf der Reduktion zu algorithmischen Problemen aus der Mathematik mit hoher Komplexität. Entsprechend geht bei asymmetrischen Kryptoverfahren die meiste Mathematik und besonders die algebraische Zahlentheorie ein. Die asymmetrische Kryptographie wurde 1976 wie oben bereits erwähnt von Diffie und Hellman erfunden.

Technische Fragestellungen Hier untersucht man, inwieweit die verwendeten Geräte auch physikalisch sicher sind. Zum Beispiel kann man aus Stromverbrauch, elektromagnetischer Abstrahlung oder Öffnen der Geräte unauthorisierten Zugang zu Informationen erhalten. Eine andere Disziplin ist die Untersuchung biometrischer Verfahren (z.B. Identifikation durch Fingerabdruck oder Iris).

1.3 Terminologie und Konzepte der Verschlüsselung

Kryptographie im allgemeinen macht nur Sinn, wenn innerhalb eines abgeschlossenen Systems mindestens drei logische Einheiten (Personen, Computer, Programme) kommunizieren wollen. Man stellt sich üblicherweise Personen vor und nennt diese Alice, Bob, usw. Gegebenfalls deuten die Namen auch auf eine spezielle Funktion hin, wie zum Beispiel Eve für „Eavesdropper“. Sender und Empfänger bezeichnen die legitimen Teilnehmer einer Kommunikation, wohingegen ein Angreifer auf die Kommunikation illegitimen Einfluß zu nehmen sucht. Die Kommunikation zwischen Sender und Empfänger erfolgt über einen Kanal, auf den der Angreifer üblicherweise Lese- und Schreibzugriff hat.

Verschlüsselung Im Kontext der Verschlüsselung betrachten wir Klartexte M (plaintexts, Nachrichten, messages), welche vom Sender durch einen Verschlüsse-

lungsvorgang $\mathcal{E}$ in Chiffretexte C (ciphertexts) umgewandelt werden sollen. Der Chiffretext C wird nach Empfang durch den Empfänger durch ein Entschlüsselungsverfahren $\mathcal{D}$ wieder in den Klartext M umgewandelt. Die Klartexte und Chiffretexte stammen aus einem vordefinierten Klartext- bzw. Chiffretextraum, und diese sind jeweils Mengen von Worten über einem Alphabet (ein Alphabet ist eine endliche nicht leere Menge Σ und die Menge der Worte über Σ ist $\Sigma^* = \cup_{i=0}^{\infty}\Sigma^i$). Im Normalfall betrachten wir das Alphabet $\{0,1\}$, also Bits, so daß die Worte endliche Bitstrings sind. Zur Ver- und Entschlüsselung werden im allgemeinen Schlüssel e, d benötigt, welche aus den entsprechenden vordefinierten Schlüsselräumen stammen.

Bei $\mathcal{E}$ und $\mathcal{D}$ handelt es sich heutzutage üblicherweise um Programme, die zur Ausführung durch einen Computer vorgesehen sind. Das Verschlüsselungsverfahren $\mathcal{E}$ erwartet den Schlüssel e und die Nachricht M als Eingabe, und liefert C als Ausgabe. Hierbei ist erlaubt (und eigentlich sogar erforderlich), daß $\mathcal{E}$ sich des Zufalls bedient und bei festem e und M nicht immer das gleiche C berechnet. Das Entschlüsselungsverfahren erwartet seinerseits d und C als Eingabe, und liefert M als Ausgabe. Die Ausführung von $\mathcal{E}$ und $\mathcal{D}$ soll möglichst effizient sein.

Für $d = e$ befinden wir uns in der Situation eines symmetrischen Kryptosystems. Hier wird $d = e$ zwischen den Kommunikationspartnern geheimgehalten. Als Verallgemeinerung der symmetrischen Situation kann man auch die Situation betrachten, in der sich d sich leicht aus e berechnen läßt.

Ein Public-Key Kryptosystem liegt vor, wenn e öffentlich ist und d vom Empfänger geheimgehalten wird. Man nennt e den öffentlichen und d den geheimen (privaten) Schlüssel des Empfängers. Hier soll es im wesentlichen unmöglich sein, d aus e zu berechnen. Verschlüsselungen können von jedem Teilnehmer berechnet werden, Entschlüsselungen sind jedoch nur mit Hilfe des geheimen Schlüssels d möglich. Abgesehen von der möglichen Nichteindeutigkeit der Chiffretexte liefert ein Public-Key Kryptosystem eine Einweg-Funktion mit Falltür (und Falltürinformation d).

Beispiel Als Beispiel betrachten wir die affin-linearen Blockchiffren. Sei $R = \mathbb{Z}/m\mathbb{Z}$ der Ring der ganzen Zahlen modulo m mit $m \geq 2$ und $n \geq 1$. Der zu definierende Verschlüsselungsalgorithmus $\mathcal{E}$ soll einen Klartext M der Länge n über dem Alphabet R, also $M \in R^n$, in einen Chiffretext aus R^n bijektiv abbilden. Sei hierzu $A \in R^{n\times n}$ invertierbar über R und $b \in R^n$. Wir fassen A und b als Schlüssel auf. Es gelte $C = \mathcal{E}(A, b, M) = AM + b$, so daß $M = \mathcal{D}(A, b, C) = A^{-1}(C - b)$.

Das Alphabet A,...,Z kann als R mit $m = 26$ codiert werden. Mit $n = 1$, $A = (1)$ und $b = 3$ erhalten wir den Chiffre von Cäsar. Wegen der geringen

Anzahl von möglichen Schlüsseln b ist dieses Verfahren leicht zu brechen. Mit beliebigem n, $A = I_n$ und $b \in R^n$ erhalten wir den Chiffre von Vignère. Dieser hat die Eigenschaft, daß einzelne Buchstaben nicht immer auf dieselben Buchstaben abgebildet werden. Eine Kryptanalyse basierend auf der Häufigkeit des Auftretens von Buchstaben wird hier aber nur geringfügig erschwert. Den Hill-Chiffre erhält man mit $b = 0$ und A beliebig. Der Permutationschiffre entspricht dem Spezialfall, wo A eine Permutationsmatrix ist.

Affin-lineare Blockchiffren können leicht gebrochen werden, wenn mindestens $n + 1$ Klartext- und Chiffretextpaare (M_i, C_i) vorliegen. Dann gilt nämlich $C_i - C_0 = A(M_i - M_0)$, und ist U die Matrix mit den Spalten $C_i - C_0$ und V die Matrix mit den Spalten $M_i - M_0$, so folgt $U = AV$. Ist V invertierbar, so ergibt sich $A = UV^{-1}$ und $b = C_0 - AM_0$.

Wird b im Vignère Chiffre zufällig und gleichverteilt aus R^n gewählt und nur einmal verwendet, erhält man im wesentlichen Vernam's one-time pad. Mit b ist auch der Chiffretext völlig zufällig und in keiner Weise mit dem Klartext verbunden. Es ist daher nicht möglich, Informationen aus dem Chiffretext über den Klartext zu erhalten. Dieser Chiffre ist aber nicht besonders praktikabel.

Angriffe und Sicherheitsmodelle Eine grundlegende Anforderung an Kryptosysteme ist, daß sie ihre Sicherheit nicht aus der Geheimhaltung der verwendeten Algorithmen und Implementierungen ableiten sollten, sondern aus den geheimen Schlüsseln. Dies wird als Prinzip von Kerkhoff bezeichnet. Hierfür gibt es eine Reihe von Gründen.

- Die geheimen Schlüssel lassen sich leichter und häufiger austauschen. Größere Flexibilität im allgemeinen.
- Die Geheimhaltung funktioniert im allgemeinen nicht über einen längeren Zeitraum (siehe COMP128 von GSM im Mobilfunk, RC4 von RSA). Bei Bekanntwerden muß unter Umständen auf neue Algorithmen und Implementierungen umgestellt werden.
- Sind die verwendeten Algorithmen und Implementierungen öffentlich, können sie von unabhängiger Seite untersucht werden. Dies eliminiert Designfehler und baut Vertrauen bei Benutzern bzw. Kunden auf (siehe beispielweise das Cryptophone).

Gegen eine Veröffentlichung der Algorithmen und Implementierungen können bei Firmen Geschäftsgeheimnisse und bei staatlichen Behörden der Wunsch sprechen, einen weitverbreiteten Gebrauch (z.B. durch Terroristen) des für eigene Zwecke entwickelten und benutzten, vielleicht sehr sicheren Kryptosystems zu verhindern.

In bezug auf die Sicherheit eines Kryptosystems betrachtet man verschiedene Angriffsstrategien und zugehörige Sicherheitsmodelle. Ein Angreifer kann (bei konstanten Schlüsseln) beispielsweise versuchen, Chiffretexte zu entschlüsseln oder den geheimen Schlüssel in Erfahrung zu bringen. Von einem praktischen Standpunkt aus kann ein Angreifer auch Strom- und Zeitmessungen verwenden. Man unterscheidet folgende Situationen in bezug auf die Fähigkeiten des Angreifers.

1. *Chipertext-only Angriff.* Der Angreifer erhält nur Chiffretexte.
2. *Known-plaintext Angriff.* Der Angreifer erhält Klartexte und die zugehörigen Chiffretexte.
3. *Chosen-plaintext Angriff.* Der Angreifer kann sich die Klartexte aussuchen und erhält die zugehörigen Chiffretexte.
4. *Chosen-ciphertext Angriff.* Der Angreifer kann sich Chiffretexte aussuchen und erhält die zugehörigen Klartexte.

Die beiden letzten Angriffe gibt es auch in adaptiver und kombinierter Form, wobei der Angreifer die gewählten Klartexte bzw. Chiffretexte in Abhängigkeit zuvor erhaltener Chiffretexte bzw. Klartexte und den Ergebnissen von Zwischenrechnungen wählen darf.

Das für Public-Key Systeme stärkste Sicherheitsmodell ist Nichtunterscheidbarkeit unter einem adaptiven Chosen-ciphertext Angriff (IND-CCA2). Hier versucht ein Angreifer die Chiffretexte zweier von ihm vorgegebener Nachrichten den Nachrichten zuzuordnen. Gelingt ihm das mit Wahrscheinlichkeit signifikant besser als $1/2$, so gilt der Angriff als erfolgreich.

1.4 Terminologie und Konzepte der Signaturen

Im Kontext der Signatur gelten zur Verschlüsselung analoge Bezeichnungen. In gewisser Weise sind Signieren und Verifizieren dual zu Ver- und Entschlüsseln. Der Sender heißt hier auch Signierer (signer), und der Empfänger Verifizierer (verifier). Durch ein Signaturverfahren $\mathcal{S}$ wird die Signatur bezüglich einer Nachricht erstellt, und mit einem Verifikationsverfahren $\mathcal{V}$ überprüft. Es gibt entsprechend Nachrichten-, Signatur- und Schlüsselräume.

Bei $\mathcal{S}$ und $\mathcal{V}$ handelt es sich heutzutage wieder üblicherweise um Programme, die zur Ausführung durch einen Computer vorgesehen sind. Das Signaturverfahren $\mathcal{S}$ erwartet den Schlüssel d und die Nachricht M als Eingabe, und liefert σ als Ausgabe. Hierbei ist wieder erlaubt (aber nicht unbedingt erforderlich), daß $\mathcal{S}$ sich

des Zufalls bedient und bei festem d und M nicht immer das gleiche σ berechnet. Das Verifikationsverfahren erwartet seinerseits e, σ und M als Eingabe, und liefert wahr oder falsch als Ausgabe. Die Ausführung von $\mathcal{S}$ und $\mathcal{V}$ soll möglichst effizient sein.

Für $d = e$ befinden wir uns in der Situation eines symmetrischen Systems. Hier wird $d = e$ zwischen den Kommunikationspartnern geheimgehalten. Als Verallgemeinerung der symmetrischen Situation kann man auch die Situation betrachten, in der sich d sich leicht aus e berechnen läßt. Das Verfahren $\mathcal{S}$ ist dann üblicherweise ein Message Authentication Code (MAC) und $\mathcal{V}$ überprüft nur $\mathcal{S}(d, M) = \sigma$. Die Integrität einer Nachricht M wird durch Versenden des Tupels $(m, \mathcal{S}(d, M))$ gewährleistet. Dritte können dies nicht überprüfen, weshalb sich diese Situation nicht für Signaturen eignet.

Ein Public-Key System liegt vor, wenn e wieder öffentlich ist und d vom Signierer geheimgehalten wird. Man nennt e den öffentlichen und d den geheimen (privaten) Schlüssel des Signierers. Hier soll es im wesentlichen wieder unmöglich sein, d aus e zu berechnen. Verifikationen können von jedem Teilnehmer durchgeführt werden, Signieren ist jedoch nur mit Hilfe des geheimen Schlüssels d möglich.

Angriffe und Sicherheitsmodelle Die Sicherheit sollte nach dem Prinzip von Kerkhoff wieder auf den geheimen Schlüsseln beruhen, und nicht der Geheimhaltung von $\mathcal{S}$.

In bezug auf die Sicherheit eines Signaturverfahrens betrachtet man verschiedene Angriffsstrategien und zugehörige Sicherheitsmodelle. Ein Angreifer kann (bei konstanten Schlüsseln) beispielsweise folgendes erreichen:

1. *Existenzielle Fälschung.* Der Angreifer berechnet eine Signatur für eine Nachricht.

2. *Selektive Fälschung.* Der Angreifer berechnet eine Signatur für eine Nachricht seiner Wahl.

3. *Universelle Fälschung.* Der Angreifer kann Signaturen für jede beliebige Nachricht berechnen.

4. *Total break.* Der Angreifer berechnet den geheimen Schlüssel des Signierers.

Man unterscheidet folgende Situationen in bezug auf die Fähigkeiten des Angreifers.

1. *Key-only Angriff.* Der Angreifer kennt nur den öffentlichen Schlüssel des Signierers.

2. *Known-Signature Angriff.* Der Angreifer erhält Nachrichten und die zugehörigen Signaturen.

3. *Chosen-Message Angriff.* Der Angreifer kann sich die Nachrichten aussuchen und erhält die zugehörigen Signaturen.

Den letzten Angriff gibt es auch in adaptiver Form, wobei der Angreifer die gewählten Nachrichten in Abhängigkeit zuvor erhaltener Signaturen und den Ergebnissen von Zwischenrechnungen wählen darf.

Das für Signaturverfahren stärkste Sicherheitsmodell ist Sicherheit bezüglich existenzieller Fälschung unter adaptiven Chosen-Message Angriffen.

In Signaturverfahren finden kryptographische Hashfunktionen eine wichtige Anwendung. Im allgemeinen wird nicht die Nachricht selbst, sondern nur der Hashwert der Nachricht signiert. Dies bringt zwei Vorteile mit sich: Zum einen kann erst durch die Verwendung geeigneter Hashfunktionen die Sicherheit von in der Praxis relevanten Signaturverfahren bewiesen werden (allerdings nur im Zufallsorakelmodell), zum anderen sind Hashwerte viel kürzer als die Nachrichten und das Signaturverfahren somit im Endeffekt effizienter. Eine erforderliche Eigenschaft der Hashfunktionen ist offenbar die Kollisionsfreiheit.

1.5 Vergleich von Public-Key und Secret-Key Verfahren

Public-Key und Secret-Key Verfahren haben teilweise sich ergänzende Vorteile, welche in gängigen Kryptosystemen genutzt werden.

Public-Key Verfahren bieten im wesentlichen eine größere Funktionalität, wie zum Beispiel Schlüsselaustausch und -management, digitale Unterschriften und höherstehende Protokolle. Auf der anderen Seite sind Secret-Key Verfahren und insbesondere die Secret-Key Verschlüsselung deutlich effizienter im Hinblick auf Schlüssellänge und Datendurchsatz als die entsprechenden Public-Key Versionen.

Für praktische Verschlüsselungsverfahren verwendet man daher die Public-Key Verfahren für den Austausch von Sitzungsschlüsseln (Sessionkeys), und diese dann für die Secret-Key Verschlüsselung der eigentlichen Nachrichten.

1.6 Protokolle

Unter einem Protokoll versteht man eine definierte Abfolge von Kommunikationsschritten zwischen mindestens zwei Teilnehmern, welches eine kryptographische

Aufgabe löst. Ein typisches Beispiel ist das folgende Challenge-Response Protokoll zur Identifikation. Wir nehmen an, Alice besitzt den öffentlichen Schlüssel e und geheimen Schlüssel d eines Signaturverfahrens. Bob soll überzeugt werden, daß Alice d kennt, ohne das d an Bob geschickt wird.

1. Bob wählt eine zufällige Nachricht M aus und schickt sie an Alice.
2. Alice schickt Bob ihre Signatur der Nachricht M unter Verwendung von d.
3. Bob glaubt, daß Alice d kennt, wenn die Signatur bezüglich e gültig ist.

Eine Angreiferin Eve möchte Bob ebenfalls davon überzeugen, daß sie d kennt, auch wenn dies nicht der Fall ist. Wird M aus einer ausreichend großen Menge von Nachrichten gewählt, müßte Eve mit hoher Wahrscheinlichkeit eine Signaturfälschung berechnen.

Im allgemeinen können Angreifer eines Protokolls passiv oder aktiv sein und in die Kommunikation des Protokoll beliebig eingreifen (substitute, replay, insert). Zum Beweis der Sicherheit eines Protokolls versucht man im allgemeinen zu zeigen, daß ein erfolgreicher Angreifer auch die zugrundeliegenden kryptographischen Funktionen angreifen kann.