Fach: BSN / ITN

Thema: Asymmetrische Verschlüsselung / RSA

Berufskolleg Hilden
des Kreises Mettmann • Europaschule

Datum:

Was ist asymmetrische Verschlüsselung?

Herkömmliche Kryptographie basiert darauf, dass Sender und Empfänger einer Nachricht den gleichen geheimen Schlüssel kennen und benutzen: Der Sender benutzt den geheimen Schlüssel zum Chiffrieren und der Empfänger benutzt ihn zum Entschlüsseln. Die Methode wird *secret-key* oder *symmetrische Verschlüsselung* genannt. Das Hauptproblem hierbei ist, dass sich Sender und Empfänger auf den gleichen geheimen Schlüssel einigen, ohne dass ihn jemand anders zu Gesicht bekommt. Wenn sie sich an verschiedenen geographischen Orten befinden, müssen sie einem Kurier, einer Telefonverbindung oder einem anderen Kommunikationsmedium trauen, um die Offenlegung des geheimen Schlüssels zu verhindern. Jeder, der den Schlüssel während der Übertragung abfangen oder mithören kann, kann danach alle verschlüsselten Nachrichten lesen, ändern, fälschen oder unterschreiben, indem er diesen Schlüssel verwendet. Die Schlüsselerzeugung, -übertragung und -speicherung wird Schlüsselmanagement genannt; alle Kryptosysteme müssen sich damit befassen. Da alle Schlüssel eines symmetrischen Kryptosystems geheim bleiben müssen, haben diese Systeme oft Schwierigkeiten mit einem sicheren Schlüsselmanagement, speziell in offenen Umgebungen mit vielen Nutzern.

Das Konzept der *asymmetrischen Kryptographie* wurde 1976 von Whitfield Diffie und Martin Hellman [DH76] vorgeschlagen, um das Schlüsselmanagementproblem zu lösen. In ihrem Konzept hat jeder Beteiligte zwei Schlüssel, einen *Öffentlichen* und einen *Privaten*. Jeder öffentliche Schlüssel wird veröffentlicht und der private Schlüssel bleibt geheim. Die Notwendigkeit eines gemeinsamen Geheimnisses zwischen Sender und Empfänger ist damit verschwunden: Jede Kommunikation umfaßt nur öffentliche Schlüssel, private Schlüssel werden nie übertragen oder geteilt. Es ist nicht länger notwendig, einem Kommunikationskanal hinsichtlich Abhörsicherheit zu trauen. Die einzige Anforderung ist, dass der Zuordnung zwischen öffentlichem Schlüssel und Nutzer getraut werden kann (bspw. durch ein vertrauenswürdiges Verzeichnis). Jeder, der eine wichtige Information versenden will, chiffriert mit dem öffentlichen Schlüssel, das Chiffrat kann jedoch nur mit dem privaten Schlüssel dechiffriert werden, der sich ausschließlich in der Hand des Empfänger befindet. Darüber hinaus kann asymmetrische Kryptographie nicht nur zur Geheimhaltung (Verschlüsselung) sondern auch zur Authentifikation (digitale Unterschriften) verwendet werden.

Verschlüsselung

Wenn Alice eine geheime Nachricht an Bob senden will, so holt sie Bobs öffentlichen Schlüssel aus einem Verzeichnis und benutzt diesen, die Nachricht zu chiffrieren. Danach versendet sie die verschlüsselte Nachricht. Bob benutzt seinen privaten Schlüssel, um die Nachricht zu dechiffrieren und zu lesen. Kein Zuhörer kann die Nachricht entschlüsseln. Jeder kann eine verschlüsselte Nachricht an Bob senden, aber nur Bob kann sie lesen. Es ist jedoch klar, dass niemand den privaten Schlüssel von Bob aus dem zugehörigen öffentlichen Schlüssel gewinnen können darf.

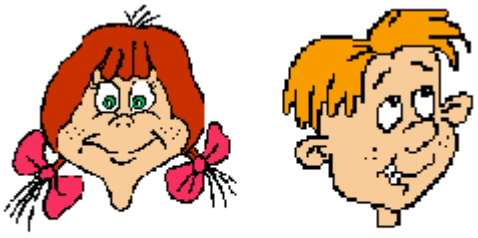

Figure 1. Alice and Bob -
The First Couple of Cryptography

Elektronische Unterschriften

Um eine Nachricht zu unterschreiben, berechnet Alice etwas aus der Nachricht und ihrem privaten Schlüssel. Das Ergebnis wird elektronische Unterschrift genannt und an die Nachricht angehängt. Bob kann die Unterschrift prüfen, indem er einige Berechnungen mit der Nachricht, der Unterschrift und dem öffentlichen Schlüssel von Alice veranstaltet. Wenn das Ergebnis einer einfachen mathematischen Gleichung genügt, so ist die Unterschrift gültig, anderenfalls ist die Unterschrift gefälscht oder die Nachricht wurde verändert.

Ein gutes Buch zur Geschichte der asymmetrischen Kryptographie stammt von Diffie [Dif88].

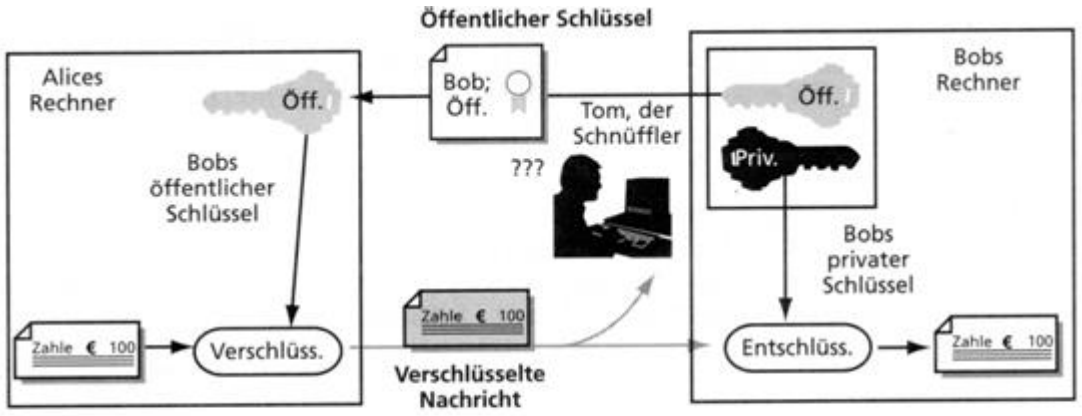

Abbildung 9.2: Einsatz des RSA-Algorithmus zur Public-Key-Verschlüsselung. Jeder, der Bobs öffentlichen Schlüssel kennt, kann ihm eine Nachricht senden, die nur Bob lesen kann. Bob hält seinen privaten Schlüssel geheim und erzeugt daraus seinen öffentlichen Schlüssel. Alice verschlüsselt ihre Nachricht an Bob mit dessen öffentlichem Schlüssel. Der öffentliche Schlüssel allein genügt nicht zur Entschlüsselung der Nachricht. Dies gelingt nur mit Bobs privatem Schlüssel.

Was ist RSA?

RSA ist ein asymmetrisches Kryptosystem, dass sich zum Verschlüsseln und zur Authentifikation eignet. Es wurde 1977 von Ron Rivest, Adi Shamir und Leonard Adleman [RSA78] erfunden. Es funktioniert folgendermaßen:

- Man nehme 2 große Primzahlen p und q.
- Bilde deren Produkt $n=p*q$, welches Modul genannt wird.
- Man wähle eine Zahl e die kleiner als n und teilerfremd (relativ prim) zu $p-1$ und $q-1$ ist.
- Finde eine Zahl d, so daß $(e*d)-1$ durch $(p-1)*(q-1)$ teilbar ist. Die Werte e und d werden öffentlicher und privater Exponent genannt.
- Der öffentliche Schlüssel ist das Paar (n,e), der private Schlüssel ist das Paar (n,d).
- Die Faktoren p und q werden sicher vernichtet oder mit dem privaten Schlüssel zusammen aufbewahrt.

Es wird angenommen, dass es schwierig ist, den privaten Exponenten d aus dem öffentlichen Schlüssel (n,e) zu berechnen. Sollte jemand n in p und q faktorisieren, so kann er natürlich d berechnen. Deshalb ist die Sicherheit von RSA mindestens an die Annahme geknüpft, Faktorisierung sei schwierig. Ein leichter Faktorisierungsalgorithmus oder ein anderer funktionierender Angriff würde RSA "brechen"

RSA Verschlüsselung

Alice möchte eine Nachricht m an Bob schicken. Alice erstellt den Chiffretext c durch modulare Potenzierung: $c = m^e \bmod n$, wobei (n,e) Bobs öffentlicher Schlüssel ist. Sie sendet c an Bob. Um dies zu dechiffrieren potenziert Bob ebenfalls: $c^d \bmod n = (m^{e*d} \bmod n = m^{(p-1)*(q-1)-1} \bmod n =) m$. (Die letzte Identität ist ein zahlentheoretischer Satz, nämlich die Eulersche Verallgemeinerung des kleinen Satzes von Fermat.) Da nur Bob d kennt, kann nur Bob c entschlüsseln.

RSA Authentifizierung

Alice möchte eine Nachricht m an Bob unterschreiben, so dass Bob sicher sein kann, dass diese Nachricht authentisch und von Alice ist. Alice erstellt eine elektronische Unterschrift durch Potenzieren: $s = m^d \bmod n$, wobei (n,d) der private Schlüssel von Alice ist. Sie sendet m und s an Bob. Dieser prüft die Unterschrift durch eine Potenzierung: $s^e \bmod n$ muss mit m übereinstimmen, wenn (n,e) Alice öffentlicher Schlüssel ist. So ist Verschlüsselung und Authentifizierung ohne Teilung eines Geheimnisses möglich: Jede Person hat nur die öffentlichen Schlüssel der anderen und seinen eigen privaten Schlüssel. Jeder kann Nachrichten verschlüsselt senden oder Unterschriften prüfen, aber nur derjenige, der den richtigen privaten Schlüssel hat, kann Nachrichten entschlüsseln oder unterschreiben.