

Glossar

Der Name Polyas leitet sich von George Pólya her, der 1919 bewies, dass das Divisionsverfahren zur Sitzverteilung von Saint-Laguë das Verfahren mit dem kleinsten quadratischen Fehler, und somit das gerechteste ist.

George Pólya

George Pólya wurde in Budapest am 13.12.1887 geboren, und schloß 1905 das staatliche Gymnasium als einer der besten vier Schüler ab, was ihm ein Stipendium an der Universität von Budapest einbrachte. Er begann, wie auch sein Vater, ein Jura-Studium, das ihn jedoch langweilte. Er interessierte sich mehr für Latein und Ungarisch. Später studierte er Physik, Mathematik und Philosophie. Seine Entwicklung wurde geprägt durch Lipót Fejér, der auch Riesz, Szegő und Erdős unterrichtete.

Pólya begann recht schnell seine Studien auf die Mathematik zu konzentrieren, die er 1912 mit dem Dokortitel abschloß.

Im Herbst 1912 ging er nach Göttingen, wo er Hilbert, Klein und Weyl traf. Zwei Jahre später wechselte er zur Eidgenössische Technische Hochschule (ETH) in Zürich.

Im Jahre 1940 ging er in die USA, wo er nach zahlreichen Veröffentlichungen am 7. September 1985 starb.

Authentifikation

Bei der Authentifikation wird die Zuordnung eines unbekanntem Benutzers zu einer Berechtigung geprüft. Die Identität muß hierzu nicht bekannt sein. Als Beispiel läßt sich hier ein Haustürschloß nehmen. Dieses authentifiziert den Zugang zum Haus anhand des passenden Schlüssels, unabhängig davon, wer den Schlüssel besitzt.

Blinde Signatur

Die blinde Signatur dient dem Signieren einer Nachricht ohne deren Inhalt preiszugeben. Als Vergleich kann man das Einprägen eines Siegels auf einen verschlossenen Briefumschlag ansehen. Das Siegel ist dann auch auf dem eingeschlossenen Brief erkennbar.

Diskrete Logarithmen

Unter dem diskreten Logarithmus versteht man die Lösung der Gleichung $a^x = y \pmod{n}$ bei gegebenen a , y und n . Dieses Problem ist ohne Kenntnis der Primfaktorzerlegung von n derzeit nicht in realistischer Zeit lösbar.

Identifikation

Bei der Identifikation wird ein Unbekannter durch eindeutige Merkmale als eine bekannte Person erkannt. Diese Merkmale können z.B. durch biometrische Merkmale, Passwörter, signierte Antworten oder persönlichen Kontakt erfasst werden.

Message Digest

Für die meisten Signaturverfahren wird nicht die gesamte Nachricht signiert, sondern nur eine Prüfsumme, die aus der Original-Nachricht berechnet wird. Die bekanntesten Verfahren für die Bildung einer solchen Prüfsumme sind MD5 und SHA1.

Diese Verfahren haben den Vorteil, dass aus der Prüfsumme nicht mehr auf den ursprünglichen Text geschlossen werden kann, und dass selbst kleinste Veränderungen des Originals zu großen Änderungen der Prüfsumme führen.

Public Key Kryptographie

Bei der Public-Key-Verschlüsselung werden unterschiedliche Schlüssel für die Verschlüsselung (Public-Key) und für die Entschlüsselung (Private-Key) verwandt. Dabei sind die Schritte der Entschlüsselung und Verschlüsselung austauschbar. Im Vergleich zu den symmetrischen Verfahren bietet sich hier der Vorteil, dass die Schlüsselverteilung bei vielen Kommunikationspartnern wesentlich einfacher ist. Zum anderen sind durch sie erst Verfahren zum Signieren von Nachrichten möglich geworden.

Signatur

Unter einer Signatur versteht man die überprüfbare Kopplung einer Identität mit einem Dokument, im normalen Leben meist durch eine Unterschrift.

In der Kryptographie wird dies durch das Anhängen einer, mit dem privaten Schlüssel codierte, Prüfsumme der Nachricht gelöst. Da nur der Eigentümer des privaten Schlüssels dies tun kann, ist die Identität sichergestellt. Durch Entschlüsseln der codierten Prüfsumme mit dem öffentlichen Schlüssel des Unterzeichners, kann nun jeder, durch Vergleich der Prüfsumme des eigentlichen Textes mit der des Unterzeichners, vergleichen.

Eine Signatur stellt somit auch sicher, dass die Nachricht nicht zwischen Unterzeichnung und späterer Prüfung durch Dritte geändert wurde.