Kryptographie

Spielend verschlüsseln lernen mit dem kostenlosen Cryptool

Verschlüsselung, d.h. die Umwandlung eines Klartextes in einen nur vom berechtigten Empfänger zu lesenden Geheimtext, ist für Nicht-Mathematiker häufig ein Buch mit mehr als sieben Siegeln. Doch da Verschlüsselung die Vertraulichkeit und Integrität von Daten sicherstellen kann, ist dies ein Gebiet, in dem sich ein Datenschutzbeauftragter auskennen muss. Mit Cryptool, einer kostenlosen E-Learning-Software für Kryptographie, lässt sich dies in kurzer Zeit verwirklichen.

Mit Cryptool lernen Sie wichtige kryptographische Verfahren sowie ihre Anwendung und Analyse kennen. Durch den spielerischen, aber durchaus ernsthaften Umgang mit der Verschlüsselung gewinnt man, wenn die Verschlüsselung gut ist, Vertrauen in diese Sicherheitsmaßnahme oder fängt an, die Schwächen zu begreifen.

So sollte man z.B. die Vigenère-Verschlüsselung tunlichst nicht mehr benutzen, da sie leicht geknackt werden kann. Sie wurde 1586 entwickelt und bis Anfang des 20. Jahrhunderts eingesetzt.

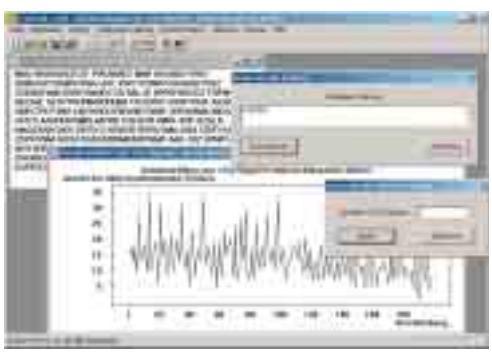
Cryptool lehrt wichtige alte und neue Verschlüsselungstechniken

Das Programm stellt die klassischen symmetrischen Verschlüsselungsalgorithmen Caesar, Vigenère, Hill, Monoalphabetische Substitution, Homophone Substitution, Playfair, Permutation, Addition, XOR und Vernam vor, aber auch die modernen Verfahren IDEA, RC2, RC4, DES, 3DES, AES.

Bei den asymmetrischen Verfahren gibt es das RSA-Verfahren. Digitale Signaturen können Sie mit RSA, DSA und elliptischen Kurven erzeugen. MD2, MD4, MD5, SHA, SHA-1 und RIPEMD-160 sind die verfügbaren HASH-Funktionen.

Ablauf-Demonstrationen zeigen das Vorgehen Schritt für Schritt

Highlights sind die interaktiven Ablauf-Demonstrationen der Hybridverschlüsselung – sie wird bei der E-Mail Verschlüsselung sowohl von PGP als auch von S/Mime verwendet – und der Digitalen Signatur mit dem RSA-Verfahren.



Die automatische Analyse von verschlüsselten Texten bestimmt nicht nur die Passwortlänge, sondern auch das Passwort selbst.

Die Hybridverschlüsselung

Die so genannte Hybridverschlüsslung ist eine Kombination aus einem symmetrischen Verschlüsselungsverfahren zur Verschlüsselung und einem asymmetrischen Verfahren zum Schlüsselmanagement. In der interaktiven Darstellung lässt sich jeder einzelne Schritt nachvollziehen, und Sie können sich alle Zwischenergebnisse anzeigen lassen.

In der Signatur-Demo können Sie in Einzelschritten nachvollziehen, wie aus HASH-Wert und asymmetrischer Verschlüsselung eine digitale Signatur gebildet wird. Auch hier kann jedes Zwischenergebnis betrachtet werden.

Eine weitere, gerade in Schulungen gut einsetzbare Möglichkeit ist das Knacken von Verschlüsselungsoperationen bei zu kurzen Schlüsseln. So können Sie etwa bei den symmetrischen Verfahren durch Teileingabe des (teilweise bekannten) Schlüssels demonstrieren, wie die Laufzeit einer Brute-Force Attacke mit der Zeit größer wird.

In der HASH-Demo sieht man, wie kleinste Änderungen an der Ausgangsdatei den Hashwert massiv ändern. Selbst das Ändern eines Bits in der Ausgangsdatei (z.B. das Ersetzen eines „P" durch ein „Q", da diese sich in der ASCII-Darstellung nur in einem Bit unterscheiden) verändert rund 50% der Bits im Hashwert.

Unterhaltsam lernen und schulen

Cryptool ist ein exzellentes Werkzeug, um sich spielerisch in die Verschlüsselung einzuarbeiten. Als Ergänzung zu einem guten Kryptographie-Lehrbuch erlaubt es das Experimentieren mit dem gerade Gelesenen.

Spaß macht es, die Verschlüsselungsbeispiele aus der beigefügten Kurzgeschichte „Der Dialog der Schwestern" von Carsten Elsner nachzuvollziehen.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.

Download-Info

Die aktuelle deutsche Version von Cryptool können Sie auf der Downloadseite von Datenschutz PRAXIS (www.datenschutzpraxis.de) herunterladen. Sie ist unter Windows lauffähig.