Verschlüsselungssoftware gesucht

Beitrag von „Herr Rau“ vom 5. Juli 2014 21:54

> Zitat von Hawkeye
>
> Oder muss dafür mein geheimer Schlüssel passen?

Richtig. Ich habe das mal in einem Blogeintrag (http://www.herr-rau.de/wordpress/2013…bei-e-mails.htm) zu erklären versucht, das war aber prä-Snowden und ist immer noch viel zu technisch.

Deinen öffentlichen Schlüssel kann jeder wissen, deshalb kannst du ihn auch per Mail verschicken und auf deine Webseite stellen. Bei den bekannteren "("symmetrischen") Verschlüsselungsverfahren ist es so, dass man einen Schlüssel zum Verschlüsseln braucht und im Prinzip den gleichen, nur quasi andersherum, zum Entschlüsseln. Wer den Verschlüsselungscode kennt (alle Zeichen um eins nach rechts schieben), der kann auch leicht den Entschlüsselungscode (alle Zeichen wieder um eins nach links schieben) herausbringen.
Bei asymmetrischen Verschlüsselungsverfahren hilft dir der Verschlüsselungsschlüssel aber gar nichts, wenn es ums Entschlüsseln geht. Deswegen kann auch jeder eine Mail an mich verschlüsseln (mit dem öffentlichen, frei zugänglichen Schlüsselteil), aber nur ich kann sie entschlüsseln (mit meinem privaten Entschlüsselungsteil).

(Für Fortschreitenden: Ich kann die Nachricht aber auch mit meinem privaten Schlüssel signieren, und nur wenn mein dir ja bekannter öffentlicher Schlüsselteil dazu passt, dann weißt du, dass die Mail garantiert von mir stammt.)