Anwendung der Zahlenkongruenzen in der RSA Kryptographie

Vortrag Prof. Gert Schmalz

Am 3. Dezember 2008 hielt der hoch angesehene Professor Schmalz, der an der Universität in New England (Australien) doziert, einen Vortrag über Ver- und Entschlüsselung mit dem RSA-Kryptosystem.

Der Vortrag begann mit einer Einführung in das Modulussystem, das mit Hilfe von Restsummen arbeitet. Nach dieser kurzen Vorstellung jenes Systems kamen wir zum eigentlichen Kernthema des Vortragabends, das wie oben erwähnt die RSA-Verschlüsselung behandelte. Diese Verschlüsselung funktioniert mit einem „Private Key“ und einem „Public Key“:

Der Private Key besteht aus zwei nicht nahe nebeneinander liegenden, großen Primzahlen.

Der Public Key ist das Produkt der beiden Primzahlen, der in einem Netzwerk jedem zugänglich ist.

Will nun jemand einer anderen Person eine verschlüsselte Nachricht zukommen lassen, so tut er dies unter Verwendung des Public Keys. Um die Nachricht wieder lesen zu können, muss der Empfänger Kenntnis über den Private Key haben, welcher die Nachricht wiederum entschlüsselt und somit lesbar macht. Beim Versuch des Brechens dieser Verschlüsselung stellt sich die Problematik, dass bei der Primfaktorzerlegung eine der beiden im Private Key enthaltenen Primzahlen bekannt sein muss.
Am Ende des Vortrags erklärte Prof. Schmalz sich noch bereit Fragen zur Kryptographie zu beantworten und stellte ein Programm zur Findung eines Public Keys zur Verfügung.

Stefan Jahn und Aaron C. Stumpf,
Klasse 10b