Die mathematische Seite des RSA-Verfahrens

Bramkamp gen. Beckmann, Nadja, Christoph-Probst-Gymnasium, Gilching

Hinführung zu dem Thema ist die aktuelle Relevanz der sicheren Verschlüsselung von Daten und die Geschichte der Kryptologie. Zum besseren Verständnis werden die wichtigsten mathematische Grundlagen des RSA-Verfahrens vorgestellt, in diesem Fall die Modulo-Rechnung, der erweiterte Euklidische Algorithmus, die Eulersche Phi-Funktion und der damit verbundene Satz von Euler.
Im folgenden Teil wird die allgemeine Funktionsweise der asymmetrischen Verschlüsselung erläutert. Im Anschluss wird aufgezeigt, wie die Schlüssel generiert werden und wie die Ver- und Entschlüsselung abläuft. Um zu beweisen, dass die Decodierung stets die ursprüngliche Nachricht liefert, wird die Korrektheit des Dechiffrieralgorithmus gezeigt. Abschließend wird das Erläuterte an einem Beispiel demonstriert.
Daraufhin wird anhand von Chipkarten gezeigt, wie die praktische Umsetzung des RSA-Verfahrens erfolgt und wie die Modifizierung durch den chinesischen Restsatz arbeitet. Hier wird der Eigenanteil, eine mit ,,Python“ implementierte Messreihe, vorgestellt, die dokumentiert, wie schnell das RSA-Verfahren mit bzw. ohne chinesischen Restsatz ist.
Abschließend wird auf die Quantenkryptographie als mögliche Zukunft der Kryptologie eingegangen.