KryptoRide - Kryptographie zum Mitmachen

Holpriger Kopfrechenritt durch ein paar Grundlagen moderner Kryptographie hin zu den zwei berühmten Beispielen *RSA-Verschlüsselung* und *Diffie-Hellman-Schlüsselaustausch*.

In letzter Zeit nimmt das Interesse an Themen rund um die Kryptographie (Verschüsselung von Nachrichten) zu. Auch deines? Wend du Lust hast, einmal an ganz einfachen Beispielen erklärt zu bekommen, auf welchen - in der Tat sehr einfachen! - mathematischen Grundlagen moderne Verschlüsselungstechniken aufbauen, dann komm vorbei mit Zettel und Bleistift und mach mit.

Wir behandeln zuerst Restklassen (*Modulo*rechnen), Eulersche Phi-Funktion, zyklische Gruppen und weiteres zahlentheoretisches Minimalrüstzeug an *sehr* einfachen Beispielen. Auf diesen Beispielen aufbauend wird gezeigt, wie die RSA-Verschlüsselung und der Diffie-Hellman-Schlüsselaustausch funktionieren.

Nötiges Vorwissen: Überhaupt keines, bis auf schriftliches Multiplizieren etc.
Es wird viel und schnell geschrieben werden. Weicheier bringen bitte einen Taschenrechner mit ;-)