Hintergrund: Große Primzahlen - das Miller Rabin Verfahren

Ein praktisches Problem bei der Anwendung des RSA Verfahrens ist es, die - sehr großen - Primzahlen p und q zu erhalten. RSA mit 2048 Bit Schlüssellänge verwendet momentan etwa 300-stellige Primzahlen, die man bei der Erzeugung des Schlüsselpaars zunächst möglichst zufällig "finden" muss.