

# 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.

From:

<https://www.info-bw.de/> -

Permanent link:

[https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:rsaverfahren:miller\\_rabin:start?rev=1674121742](https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:rsaverfahren:miller_rabin:start?rev=1674121742)

Last update: **19.01.2023 09:49**

