

Universität Konstanz

Sommersemester 2021

Fachbereich Mathematik und Statistik

Prof. Dr. Salma Kuhlmann

Dr. Lothar Sebastian Krapp, Michele Serra

## **RSA-Verfahren**

Autor: Sophia-Elena Mauch

Datum: 23.06.2021

Supervisor: Michele Serra

### Abstract:

In diesem Vortrag zum *RSA-Verfahren* soll es um die Funktionsweise sowie die mathematischen Grundlagen dieses effizienten Verschlüsselungsverfahrens gehen. Zum besseren Verständnis des prinzipiellen Ablaufs liegt am Anfang dieser Abfassung der Fokus auf der Darstellung einer überblicksartigen und schematisch aufgearbeiteten Erklärung des Verfahrens. Hiernach werden die diesem Verfahren zugrundeliegenden mathematischen Gesetzmäßigkeiten herausgearbeitet - hierzu muss tiefer auf die Themengebiete (*große Primzahlen und Primzahlfindung, Lösen modularer Potenzgleichungen* sowie den *Satz von Euler*) eingegangen werden. Den Abschluss bildet ein kurzer Ausblick zur Einbindung der RSA-Verschlüsselung im schulischen Sekundarstufen-Bereich.