

RSA-Verfahren

Das RSA-Verfahren, benannt nach deren Entwicklern R. Rivest, A. Shamir und L. Adleman, zählt zu den asymmetrischen Verschlüsselungsverfahren. Asymmetrisch bedeutet dabei, dass zwei verschiedene „Schlüssel“ zum Ver- und Entschlüsseln einer Nachricht benutzt werden. In diesem Zusammenhang sind Schlüssel Methoden bzw. Algorithmen, um eine Nachricht entweder in eine verschlüsselte Form zu überführen oder aus dieser wieder lesbar zu machen. Da es sich beim RSA-Verfahren um ein mathematisches Verfahren handelt, wird jede Art von Nachricht als Zahl kodiert.

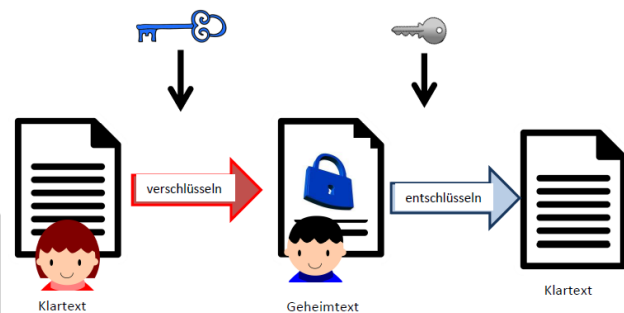


Abbildung 1: Schema des RSA-Verfahrens mit public key (blau) und secret key (grau).



Wie funktioniert das RSA-Verfahren und wie sicher ist es?

Aufgabe 1: Um die Funktionsweise des RSA-Verfahrens zu verstehen, wollen wir den Algorithmus an einem Zahlenbeispiel durchgehen.

- Generieren Sie einen öffentlichen Schlüssel (e, n) und einen privaten Schlüssel d zu den beiden Primzahlen $p = 13$ und $q = 17$. Begründen Sie Ihre Wahl der Komponenten e des öffentlichen Schlüssels.
- Bestimmen Sie nachvollziehbar, wie viele Möglichkeiten es für die Komponente e des öffentlichen Schlüssels gibt.

Aufgabe 2: Im Folgenden sollen nun mittels des öffentlichen und privaten Schlüssels (aus Aufgabe 1) Nachrichten – kodiert als natürliche Zahlen – verschlüsselt und entschlüsselt werden.

Hinweis: Nutzen Sie für die Modulo-Rechnungen die bereitgestellten digitalen Medien.

- Wählen Sie (geheim!) eine natürliche Zahl N , die als geheime Botschaft fungiert. Verschlüsseln Sie diese Nachricht mittels des öffentlichen Schlüssels (e, n) .
- Entschlüsseln Sie die verschlüsselte Nachricht mit dem geheimen Schlüssel d .
- An welchen Stellen gehen beim Verfahren die Informationen des öffentlichen Schlüssels ein?

Aufgabe 3: Im Folgenden soll die Sicherheit des RSA-Verfahrens näher untersucht werden.

- a. Arbeiten Sie dazu in einer Dreiergruppe und nehmen Sie die Rollen von Alice, Bob und Charlie ein¹.

Bob: Wählen Sie (geheim) zwei Primzahlen kleiner als 30, generieren Sie einen öffentlichen Schlüssel (e, n) sowie einen geheimen Schlüssel d .

Alice: Verschlüsseln Sie damit eine geheime Nachricht.

Charlie: Können Sie anhand des öffentlichen Schlüssels und der verschlüsselten Nachricht die geheime Nachricht entschlüsseln? Beschreiben und begründen Sie Ihr Vorgehen.

- b. Für welche Primzahlen p und q sowie Komponenten e war es für Charlie schwieriger die Nachricht zu „knacken“?



¹ Dies sind die Bezeichnungen der Kryptographie für Sender, Empfänger und Dritte, unbefugte Person, die versucht die Nachricht zu entschlüsseln.