

Das RSA-Verfahren

14. März 2023

Inhaltsverzeichnis

1	Asymmetrische Verschlüsselung	2
1.1	Das Problem der symmetrischen Verschlüsselung	2
1.2	Was bedeutet asymmetrisch? - Die Idee des RSA-Verfahrens	4
1.3	Zusatz: Erste Versuche	6
1.3.1	Versuch 1: Modulare Addition	6
1.3.2	Versuch 2: Modulare Multiplikation	6
1.3.3	Versuch 3: Modulares Potenzieren	6
2	Ver-und Entschlüsseln von Nachrichten	7
3	Herstellung eines Schlüsselpaars	7
4	Angriffsmöglichkeiten	8
4.1	Primfaktorzerlegung von n	8
4.2	Digitale Signatur	9

1 Asymmetrische Verschlüsselung

1.1 Das Problem der symmetrischen Verschlüsselung

Im ersten Teil des Seminars hast du bereits **symmetrische Verschlüsselungsverfahren** kennengelernt. Dabei müssen sich beiden Parteien, Alice und Bob, auf einen geheimen Schlüssel einigen. Dieser kann zum Ver- und Entschlüsseln von Nachrichten verwendet werden. Im folgenden Merkkasten ist das Senden einer Nachricht von Alice an Bob zusammengefasst. Die beiden wenden dabei eine Caesar-Verschlüsselung an.

Caesar-Verschlüsselung: Alice sendet die Nachricht „HALLO “ an Bob

1. Alice und Bob entscheiden sich gemeinsam für den geheimen Schlüssel k , eine Zahl zwischen 0 und 26.
2. Alice verwendet die Tabelle aus Skript 1 um das Wort in Zahlenwerte zu übersetzen.

HALLO \rightarrow 7, 0, 11, 11, 14

3. Alice verwendet k um die Zahlenwerte zu verschlüsseln. Wenn m die ursprüngliche Zahl ist, dann lässt sich die Geheimzahl c berechnen durch

$$c = (m + k) \mod 26$$

4. Alice sendet die verschlüsselten Zahlen an Bob.
5. Bob entschlüsselt die Zahlen mit

$$m = (c - k)$$

wenn $(c - k) > 0$ gilt. Falls nicht berechnet er

$$m = (c - k) + 26$$

Aufgabe 1

Schau dir Abbildung 1 an. Alice sendet die verschlüsselte Nachricht „MFQQT“ an Bob. Welchen Wert hat das k von Alice? Welches Wort entschlüsselt Bob? Trage deine Ergebnisse in die Abbildung ein.

Aufgabe 2

Alice und Bob haben keine Zeit um sich persönlich zu treffen. Die beiden haben damit kein Problem weil sie ja das Internet zur Verfügung haben. Würdest du den beiden empfehlen ein symmetrisches Verschlüsselungsverfahren anzuwenden. Begründe deine Antwort.

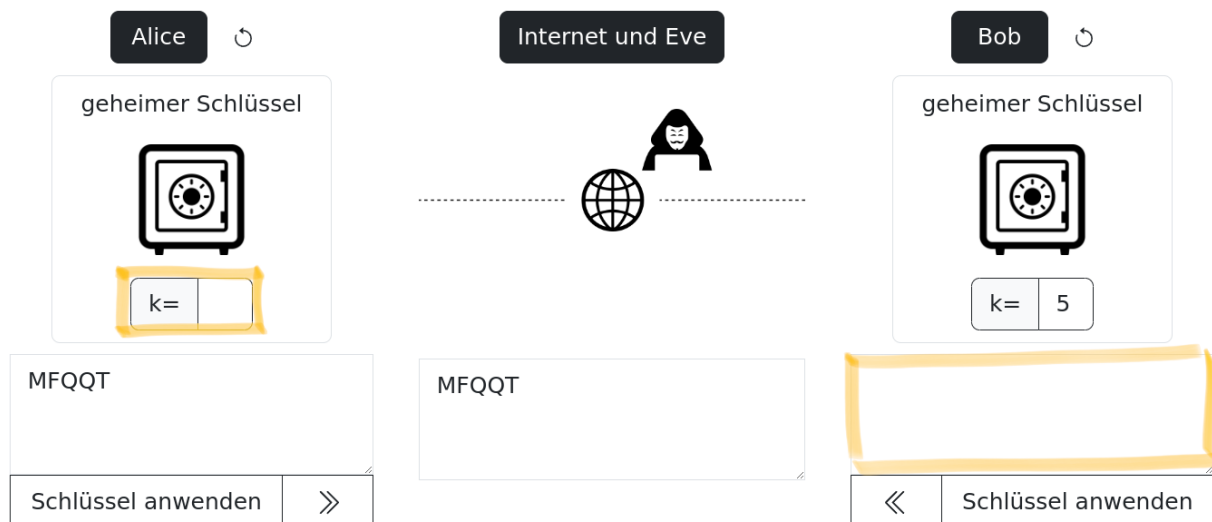
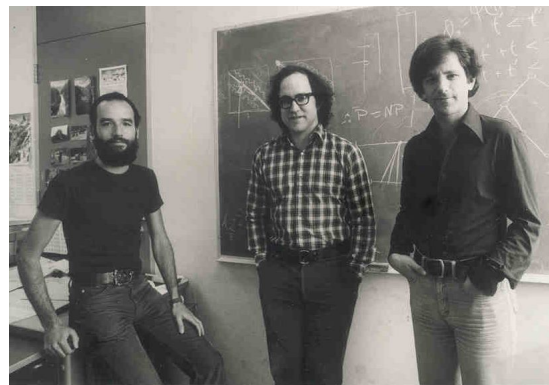


Abbildung 1: Alice sendet eine verschlüsselte Nachricht an Bob mit dem Caesar-Verfahren. Hackerin Eve gelangt nur an die verschlüsselte Nachricht. Sie muss den geheimen Schlüssel k kennen um die Nachricht zu entschlüsseln.

Bei symmetrischen Verschlüsselungen ist der gefährlichste Moment der Austausch des geheimen Schlüssels zwischen Alice und Bob. Kann dieser Austausch von Eve abgehört oder anderweitig beobachtet werden ist das ganze Verfahren sinnlos.

Alice und Bob wollen aber auch sicher miteinander kommunizieren, wenn sie sich nie im Leben persönlich sehen werden. Um dieses Problem zu lösen verwendet man **asymmetrische Verschlüsselungen**. Wir wollen uns in diesem Skript eines davon genauer anschauen - das RSA-Verfahren.

Der Name RSA kommt von den Nachnamen Rivest, Shamir und Adleman, den Erfindern. Die drei Herren sind rechts im Bild dargestellt. Es wurde im Jahre 1977 erfunden und ist seitdem aus dem alltäglichen Leben nicht mehr wegzudenken. Es wird so gut wie überall eingesetzt, wo sicherer Nachrichtenaustausch über das Internet erforderlich ist. Es kommt unter Anderem zum Einsatz bei



- Apps zum Chatten (Telegram, Threema, usw.),
- jedem Öffnen einer sicheren Website (<https://...>) im Internet,
- Bankgeschäften oder
- der Fernwartung von Computern.

Im letzten Kapitel des Skripts wird genauer auf die Einsatzgebiete eingegangen.

1.2 Was bedeutet asymmetrisch? - Die Idee des RSA-Verfahrens

In diesem Kapitel wollen wir verstehen, warum das RSA-Verfahren als asymmetrisch bezeichnet wird. Dazu reicht es zunächst aus, wenn wir uns nur den Ablauf des Nachrichtenaustauschs anschauen. Öffne dazu die Website

<https://mx3030.github.io/rsa/>



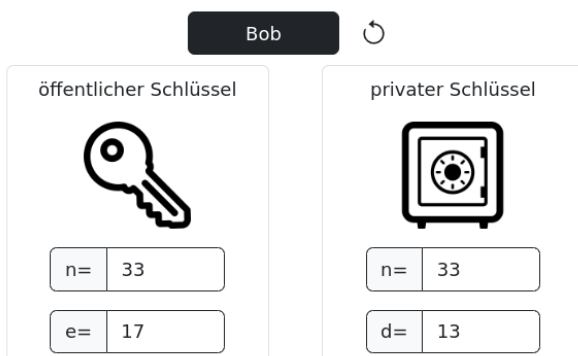
oder verwende den QR-Code.


Bei den symmetrischen Verfahren mussten beide Parteien alle Informationen (den geheimen Schlüssel) kennen. RSA ist nun ein asymmetrisches Verfahren, weil Alice über Informationen verfügt, die Bob nicht kennt und umgekehrt. Bei diesen geheimen Informationen handelt es sich um **private** Schlüssel, die zum Entschlüsseln der erhaltenen Nachrichten verwendet werden.

Wir wollen uns jetzt anschauen, wie Alice eine Nachricht an Bob sendet.

Alice sendet eine Nachricht an Bob

Drücke auf den Button von **Bob** um die Perspektive von Bob einzunehmen.

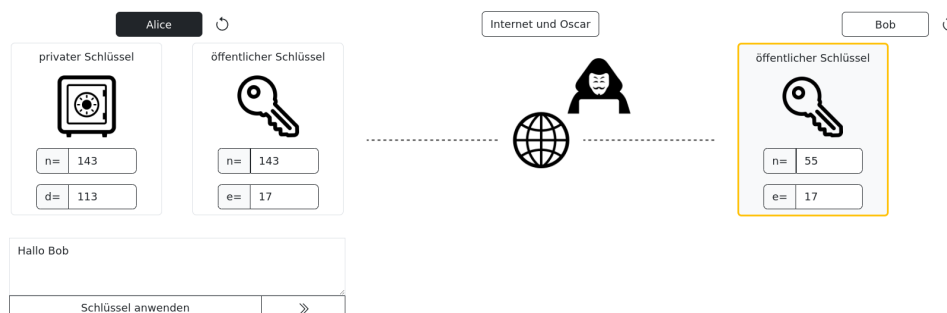



Durch Drücken von  baut sich Bob ein Schlüsselpaar (Kapitel 3) bestehend aus einem **öffentlichen** und einem **privaten** Schlüssel.

Der **öffentliche** Schlüssel besteht aus zwei Zahlen (n, e) und ist frei zugänglich für alle Personen.

Der **private** Schlüssel besteht aus zwei Zahlen (n, d) und ist ein Geheimnis von Bob.

Drücke auf den Button von **Alice** um die Perspektive von Alice einzunehmen.




Alice verfasst die Nachricht „Hallo Bob“. Sie holt sich den **öffentlichen** Schlüssel von Bob und verschlüsselt ihre Nachricht durch Drücken von **Schlüssel anwenden** (Kapitel 2). Durch Drücken von  sendet sie die verschlüsselte Nachricht zu Bob.

Wechsle in die Perspektive von **Bob**.

Bob
↻


öffentlicher Schlüssel



n=
55

e=
17

privater Schlüssel



n=
55

d=
33

allezeg

⏪
Schlüssel anwenden

Nur Bob kann die Nachricht entschlüsseln, da er im Besitz des **privaten** Schlüssels ist (Kapitel 2). Wähle den privaten Schlüssel aus und drücke auf **Schlüssel anwenden**.

Aufgabe

Sende eine Antwort von Bob an Alice. Beschreibe den Ablauf.

Aufgabe

Alice baut sich ein Schlüsselpaar. Bob baut sich kein Schlüsselpaar. Welche der beiden Aussagen ist richtig?

- ☐ Alice kann eine verschlüsselte Nachricht an Bob senden.

☐ Bob kann eine verschlüsselte Nachricht an Alice senden.

Aufgabe

Welche Schlüssel kennt Alice?

- ☐ privat Alice

☐ privat Bob

☐ öffentlich Alice

☐ öffentlich Bob

Welche Schlüssel kennt Bob?

- ☐ privat Alice

☐ privat Bob

☐ öffentlich Alice

☐ öffentlich Bob

Welche Schlüssel kennt Oscar?

- ☐ privat Alice

☐ privat Bob

☐ öffentlich Alice

☐ öffentlich Bob

Mit welchem Schlüssel verschlüsselt Bob eine Nachricht an Alice?

- ☐ privat Alice

☐ privat Bob

☐ öffentlich Alice

☐ öffentlich Bob

Mit welchem Schlüssel entschlüsselt Alice eine Nachricht von Bob?

- ☐ privat Alice

☐ privat Bob

☐ öffentlich Alice

☐ öffentlich Bob

1.3 Zusatz: Erste Versuche

In Kapitel 2 und 3 wird gezeigt, wie die Idee von öffentlichen und privaten Schlüsseln beim RSA-Verfahren umgesetzt wird. In diesem Zusatzkapitel sollen einige Beobachtungen beschrieben werden, die erklären warum das RSA-Verfahren auf diese Art und Weise funktionieren muss.

1.3.1 Versuch 1: Modulare Addition

1.3.2 Versuch 2: Modulare Multiplikation

1.3.3 Versuch 3: Modulares Potenzieren

2 Ver-und Entschlüsseln von Nachrichten

Wir wollen nun verstehen, was beim Ver-und Entschlüsseln der Nachrichten passiert. Was läuft also im Hintergrund ab, wenn auf Schlüssel anwenden gedrückt wird.

Zunächst machen wir uns klar, dass man jede Nachricht in eine Folge von Zahlenwerte übersetzten kann. Genauers dazu findest du im Zusatzkasten am Ende des Kapitels.

Wie werden nun also Zahlen mit dem RSA-Verfahren verschlüsselt?


Aufgabe

Berechne die folgenden Kongruenzen mit der Methode der schnellen Exponentiation.

Aufgabe

Verwende einen Schlüssel mit $n = 11$ und schicke die Zahl 12. Was beobachtest du? Was muss beim Senden von Nachrichten also bachtet werden?

3 Herstellung eines Schlüsselpaars

Damit das Ver-und Entschlüsseln auf diese Art und Weise funktioniert, muss dass eigene Schlüsselpaar nach einer festgelegten Methode gebaut werden. Bei Drücken auf  passiert genau das.

Aufgabe

Konstruiere dein eigenes Schlüsselpaar. Verwende keine Primzahlen > 30 .

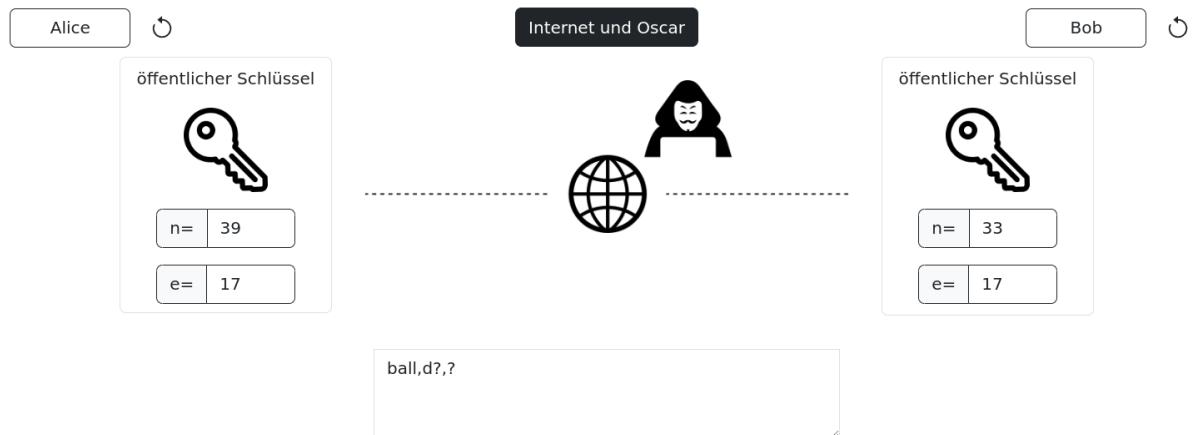
Hefte deinen öffentlichen Schlüssel mit Namen an die Tafel.

Nehme dir einen freien öffentlichen Schlüssel von der Tafel und schicke eine verschlüsselte Zahlenfolge (max. 5 Zahlen).

Gebe dem Inhaber des öffentlichen Schlüssels deine Nachricht.

Entschlüssele die Nachricht, die du erhalten hast.

4 Angriffsmöglichkeiten

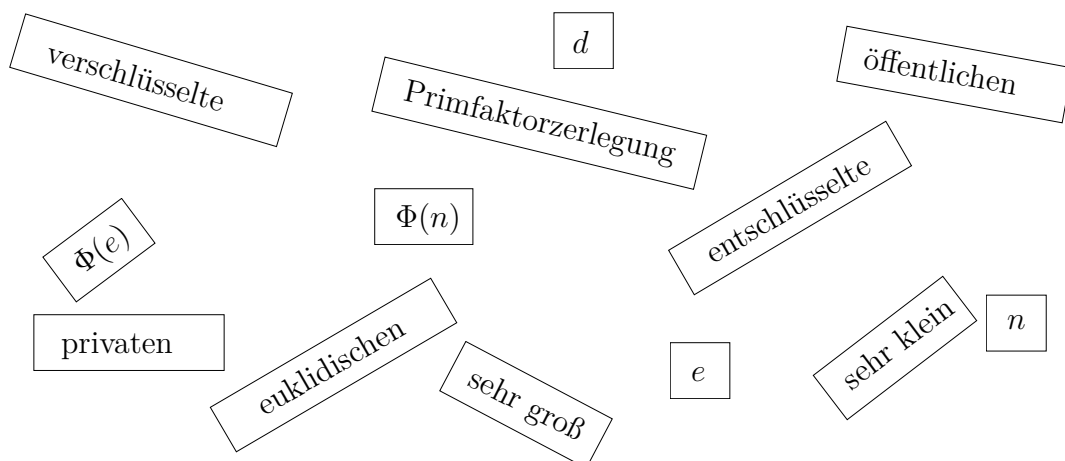


In diesem Abschnitt wollen wir die Perspektive von Oscar einnehmen. Drücke auf den Button **Oscar** um seine Situation grafisch darzustellen.

4.1 Primfaktorzerlegung von n

Fülle den Lückentext mit den Begriffen. Nicht alle Begriffe können verwendet werden.

Oscar kann nur an die _____ Nachricht gelangen und kennt den _____ Schlüssel. Um die Nachricht zu entschlüsseln benötigt er aber den _____ Schlüssel, genauer die Zahl _____. Diese ist das Inverse zu _____ modulo _____. Das lässt sich leicht mit dem erweiterten _____ Algorithmus berechnen, wenn $\Phi(n)$ bekannt ist. Wenn n _____ ist, dauert es unfassbar lange $\Phi(n)$ zu bestimmen. Nur wenn man die _____ von n kennt, gilt sofort $\Phi(n) = (p - 1) \cdot (q - 1)$.



Zusammenfassung: Angriff durch Primfaktorzerlegung

$$\begin{aligned}n &= p \cdot q \\ \Phi(n) &= (p - 1) \cdot (q - 1) \\ d^{-1} &\equiv e \pmod{\Phi(n)} \\ x &\equiv y^d \pmod{n}\end{aligned}$$

Aufgabe

Hacke den privaten Schlüssel zu einem öffentlichen Schlüssel. Verwende das Primzahlsieb.

Um sich gegen diesen Angriff zu verteidigen wählt man ein sehr großes n . Ein RSA-Schlüssel in der Praxis besteht in der Regel aus 2048 Bit. Es ist dann sehr einfach n selber zu konstruieren, aber unmöglich die Zerlegung von n als Außenstehender zu finden. Außer man benötigt die Zerlegung erst in 100 Jahren.

4.2 Digitale Signatur

Ein weiterer Angriff könnte durch „Social Engineering“ (soziale Manipulation) erfolgen. Dabei würde Oscar so tun, als wäre er Bob. Wenn Alice eine Anfrage an Bob schickt um den öffentlichen Schlüssel zu holen, könnte Oscar die Anfrage abfangen und stattdessen seinen öffentlichen Schlüssel an Alice senden. Wenn Alice die verschlüsselte Nachricht an Bob schickt, kann Oscar diese Nachricht entschlüsseln.

Um dieses Problem auszuschließen verwendet man in der Praxis digitale Signaturen. Test