

RSA

A) Kognitive (Ziele) Kompetenzen

I)

- Der Schüler kennen verschiedene Verschlüsselungsarten und können diese in symmetrische und asymmetrische Verschlüsselung unterteilen
- Der Schüler kennen den Ablauf des Verschlüsselungsverfahrens RSA

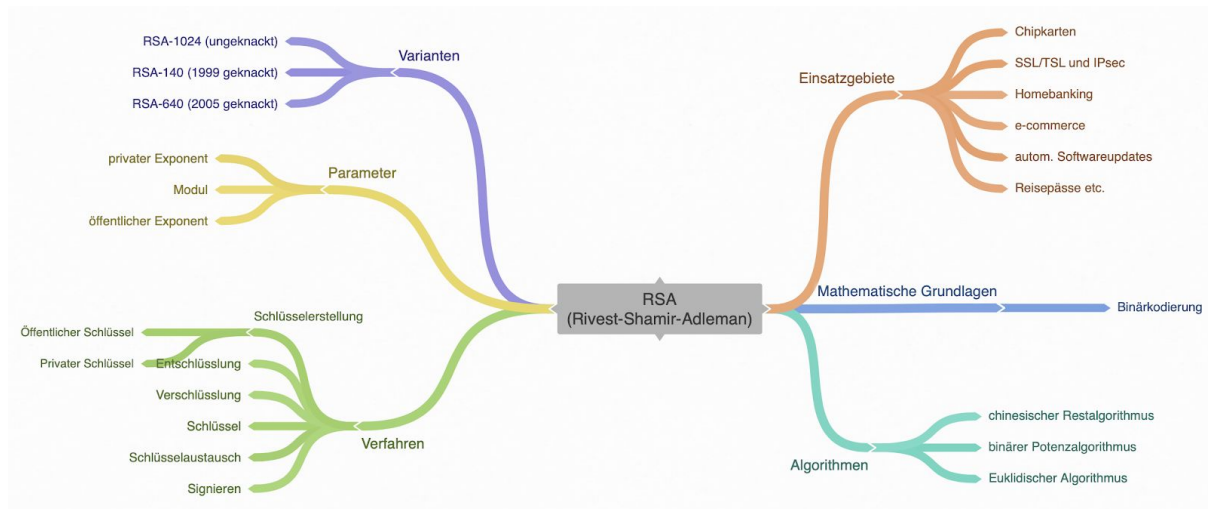
II)

- Der Schüler beherrschen mathematische Grundfähigkeiten zur RSA
- Der Schüler können einen Text mit RSA verschlüsseln und entschlüsseln

III)

- Der Schüler ist in der Lage, passende Situationen, in denen RSA verwendet werden sollte, herauszufinden und in diesen RSA anzuwenden

B) Begriffsnetz



C) Aufgaben

1. Ordne den Verschlüsselungsverfahren ihre jeweiligen Besonderheiten und ihr Anwendungsgebiet zu.
2. Wie viele Schlüssel werden zu einem symmetrischen bzw asymmetrischen Verschlüsselungs und Entschlüsselungsvorgang benötigt?
3. Wer besitzt bei einem asymmetrischen Informationsaustausch von Heinz und Peter welchen Schlüssel? Ziehe dazu die Schlüssel zu den jeweiligen Teilnehmern.
4. Löse die folgende Aufgabe unter Verwendung des Lerntools* und zwei selbst gewählten Primzahlen. (* <https://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/>)
5. Zähle 4 Situationen auf in der RSA zur Verschlüsselung angewendet wird.