

Die Verschlüsselung ist möglich, dazu braucht man nur auf den nächsten "4. Zustand" zu kommen.

Aufgabe 4 (RSA)

Gegeben sei eine RSA Verschlüsselung mit $n=3337$ und $e = 79$.

a) Verschlüsseln Sie hiermit die Nachricht $m=688$.

Berechnung: $m^e \bmod n = 688^{79} \% 3337 = 1570$ (Geheimtext)

b) Welcher der Entschlüsselungsschlüssel 17, 512 oder 1019 ergibt bei der Entschlüsselung des gerade berechneten Geheimtexts wieder die Nachricht 688?

Berechnung: $c^d \bmod n = 1570^{1019} \% 3337 = 688$

Aufgabe 5 (Verschlüsselungsmodi)

Erstellen Sie eine Tabelle in der sie die wichtigsten Eigenschaften (u.a. die Vorteile und Nachteile, die Einsatzgebiete, etc.) der Modi ECB und CBC gegenüberstellen.

ECB Vorteile:

- schneller Algorithmus
- es können Klartextblöcke außerhalb einer Reihenfolge (also im wahlfreien Zugriff) decodiert, eingefügt und gelöscht werden

ECB Nachteile:

- unsicheres Verfahren (sehr simpel, Klartextmuster werden nicht verwischt)

CBC Vorteile:

- sehr sicheres Verfahren

CBC Nachteile:

- langsamer Algorithmus
- kein wahlfreier Zugriff, bei Einfügen und Löschen muss komplett neu chiffriert werden