Antwortblatt zum AB1 | Das Caesar-Verfahren

Aufgabe 1 | Caesar Verschlüsselung

Teil d | Reflexion

Wie sicher ist dieses Verschlüsselungsverfahren?

Welche Probleme könnten auftreten?

Was würdest du verbessern?

Welche Nachrichten würdest du so verschicken?

Antwortblatt zum Zusatzblatt | Hacker – Caesar

Aufgabe 1 | Brainstorming

Wie würdest du beim Caesar-Verfahren vorgehen, um eine Nachricht zu entschlüsseln?

Aufgabe 2 | Caesar hacken

Teil b | So machen es die Profis

Wie gehst du vor, wenn du nicht beim ersten Mal einen sinnvollen Klartext erhältst?

Antwortblatt zum AB 2 | Public Key erzeugen

Aufgabe 1 | Primzahlen

Teil a | Primzahlen
Definition einer Primzahl:

Aufgabe 2 | Berechnung von e

Teil c | Eulersche Phi-Funktion
Was fällt dir auf, wenn du die Funktionsargumente n und die Funktionswerte a anschaust?

Antwortblatt zum Zusatzblatt | Euklidischer Algorithmus

Aufgabe 1 | Allgemein

Teil c | Vergleich
Bestimme den ggT(234,123) und ggT(897,624)

1. mit der Primfaktorzerlegung
2. mit dem Euklidischen Algorithmus

Welche Erkenntnis ziehst du?

Antwortblatt zum AB 3 | Nachrichten verschlüsseln

Aufgabe 1 | Modulo

Teil c | Modulo rechnen
Was fällt dir auf, wenn du die ersten Aufgaben 1.-3. anschaust?

Was fällt dir auf, wenn du die letzten Aufgaben 4.-5. anschaust?

Aufgabe 2 | Nachricht verschlüsseln

Teil b | Geheimtext c
Notiere dir die Gleichung $c \equiv m^e \bmod N$ mit deinen gewählten Zahlen und überlege wie du vorgehen musst

Antwortblatt zum AB 4 | Nachrichten entschlüsseln

Aufgabe 1 | Nachricht entschlüsseln

Teil a | Private Key
(Zusatzblatt: Notiere dir e, N und φ(N)**)**

Notiere dir (d,N):

Teil b | Nachricht entschlüsseln
Notiere dir die Gleichung $m \equiv c^d \bmod N$ mit deinen gewählten Zahlen und überlege wie du vorgehen musst.

Aufgabe 2 | Reflexion
Welche Unterschiede erkennst du im Vergleich zum Caesar Verschlüsselungsverfahren? Welche Gemeinsamkeiten?

Antwortblatt zum AB 5 | Nachrichten verschicken

Aufgabe 2 | Reflexion

Wie sicher ist das RSA-Verfahren?

Hat das RSA-Verfahren Zukunft?

Wer hat generell Interesse daran Daten zu entschlüsseln?

Antwortblatt zum Zusatzblatt | Hacker - RSA

Aufgabe 1 | Brute-Force-Attacke

Teil d |Reflexion

Weitere mögliche Angriffe sind:

- Seitenkanalattacke
- Man-in-the-middle-Angriff
- Chosen-Plaintext-Angriff