Kryptologie
Übungsblatt 4

Aufgabe 4.1

Geben Sie die diskreten Logarithmen von $1, ..., 12$ zur Basis 2 modulo 13 an.

Aufgabe 4.2

Beim Shamir'schen No Key Protokoll ist die intuitive Vorstellung die, dass Alice ihre Nachricht m in eine Box einschließt. Diese Box wird an Bob gesandt. Dieser hängt ein weiteres Schloss (für das Bobs Schlüssel passt) hinzu und schickt die Box wieder zurück an Alice. Alice entfernt nun ihr Schloss und schickt die Box, die immer noch von Bob verschlossen ist, an Bob zurück. Dieser öffnet nun die Box mit seinem Schlüssel und erhält die Nachricht.
Ein unberechtigter Zuhörer dieser Korrespondenz sieht eine Box, einmal von Alice verschlossen, einmal sowohl von Alice als auch von Bob, und schließlich von Bob verschlossen. In keinem dieser Fälle kann er sie öffnen.
Beim tatsächlichen Shamir-Protokoll wird zum Ver- und Entschlüsseln eine modulare Exponentiationsfunktion angewandt.
In dieser Aufgabe betrachten wir eine deutliche Vereinfachung: Der Klartext m von Alice wird als ein Bitstring dargestellt. Alice wählt eine Zufallsbitfolge z derselben Länge und schickt $m' = m \oplus z$ an Bob. Bob wählt ebenfalls eine Zufallsbitfolge z' und schickt $m'' = m' \oplus z'$ zurück an Alice. Diese schickt $m''' = m'' \oplus z$ an Bob. Damit wird Alices ursprüngliche Verschlüsselung wieder aufgehoben und Bob erhält tatsächlich $m''' = m \oplus z'$. Nochmaliges XOR mit z' ergibt bei Bob schließlich die Nachricht m.
Ein Abhörer, der m', m'', m''' mitlesen kann, kann die Nachricht m sehr leicht berechnen. Wieso?

Aufgabe 4.3

Sei $n = 17$ und sei $a = 4$ eine Primitivwurzel modulo n. Alice wählt die Zufallszahl $x = 3$ und Bob wählt $y = 6$.
Geben Sie die Diffie-Hellman-Schlüsselvereinbarung mit diesen Parametern an.

Aufgabe 4.4

Bob hat den öffentlichen El Gamal-Schlüssel 9, wobei initial die Primzahl $n = 11$ und die Primitivwurzel $a = 2$ festgelegt wurde.
Alice möchte an Bob die Nachricht 7 schicken. Geben Sie 3 verschiedene Chiffren an, die Alice senden könnte und die dazu führen, dass Bob am Ende korrekt 7 entschlüsseln kann.

Aufgabe 4.5

Sei $n = 103$ eine Primzahl. Überprüfen Sie mit dem Euler-Kriterium, dass 8 ein quadratischer Rest modulo n ist und berechnen Sie die Quadratwurzeln von 8 modulo 103.

Aufgabe 4.6

Beim Rabin-Verschlüsselungsverfahren sei der öffentliche Schlüssel $n = 713$ gegeben. Alice sendet die Nachricht $c = 200$ an Bob. Welche möglichen Klartexte erhält Bob, wenn er zur Berechnung den geheimen Schlüssel $(p, q) = (31, 23)$ benutzt?