Elliptische Kurven & Kryptologie Serie 10

Drei Kryptosysteme: RSA, Massey-Omura, Diffie-Helman Abgabe: 16. Mai

---

1. ***RSA Kryptosystem***: Der öffentliche Schlüssel sei $(851, 17)$, also $n = 851$ und $e = 17$.

(a) Berechne d aus $n = 23 \cdot 37$.

(b) Berechne $19^{17} \mod n$.

2. ***Massey-Omura Kryptosystem***: Die zugrundeliegende multiplikative Gruppe sei $\mathbb{Z}_{131}^*$.

Alice sendet Bob die Zahl 81, Bob sendet dann Alice die Zahl 11, und schliesslich sendet Alice die Zahl 15 an Bob, worauf Bob die Nachricht P von Alice entschlüsselt.

Durch eine Indiskretion weiss man $e_B = 67$; berechne P.

3. ***Diffie-Helman Schlüsselaustausch***: Die zugrundeliegende multiplikative Gruppe sei wieder $\mathbb{Z}_{131}^*$ und $g = 43$ sei das vereinbarte Gruppenelement.

Alice sendet Bob die Zahl 7, und $e_B = 17$.

(a) Welche Zahl sendet Bob an Alice?

(b) Welches ist der daraus resultierende Schlüssel?