Implementierung moderner Public-Key-Algorithmen
Prof. Dr. Michael Braun, WS2015/16

Praktikum

Implementierung der Skalarmultiplikation auf elliptischen Kurven über dem endlichen Körper $\mathbb{F}_{2^m}$

- Das C-Programm `pka_name1_name2_name3.c` soll ergänzt werden.
- Die Ansi-C-Implementierung soll sich mit gcc mittels

  ```
  cc pka_name1_name2_name3.c -O3 -Wall -pedantic
  ```

  fehlerfrei und ohne Warnung übersetzen lassen.
- name1, name2, name3 sollen durch die Nachnamen der Team-Mitglieder (maximal drei Personen pro Team) ersetzt werden.
- Es soll eine Routine Skalarmultiplikation `mult_scalar(...)` implementiert werden.
- Die vorgegebene Schnittstelle soll eingehalten werden, da diese vom bereitgestellten Testprogramm `test_ecc_b163` verwendet wird.
- Das korrekt ablaufende Programm soll bis 11. Januar 2016, 12:00 Uhr, an `michael.braun@h-da.de` gesendet werden. Nur dann ist die Zulassung für die Klausur möglich.
- In der letzten Vorlesung wird eine Laufzeitmessung der Programme durchgeführt und ein Ranking zwischen den Teams erstellt.
- Die besten drei Teams erhalten relevante Bonuspunkte für die Klausur (eine Benotungsstufe besser – also 0,3 oder 0,4).