Prüfungsaufgabe

05 October 2015 14:03

✓ 1. a) Primzahlen erzeugen und multiplizieren p, q → n
BigInteger.probablePrime

b) e wählen teilerfremd → $\in \mathbb{Z}^*_{\varphi(n)}$
d berechnen Euklid
↳ Euklid

c) Schlüssel abspeichern in File
easy → sk, pk

✓ 2. a) Öffentlichen key lesen

b) Umwandlung in ASCII Code
mit charAt(..)

c) Verschlüsselung
mit schneller Exp.
→ Integer.toBinaryString(..)

d) File write

3. gelesenes Zeichen^d mod n
✓ – chiffre lesen
✓ – private key lesen
✓ – entschlüsseln
✓ – in text-d.txt schreiben