Universität Greifswald
Institute für Mathematik and Informatik
Lecturer: Marc Hellmuth Tutor: Nikolai Nøjgaard

11. Exercise "Datenstrukturen und Effiziente Algorithmen", WS 18/19

Exercise 1: (4 Credits)
Show that if p is prime and e is a positive integer, then $\varphi(p^e) = p^{e-1}(p-1)$, where φ denotes Euler's phi function.

Exercise 2: (4 Credits)
Show that for any integer $n > 1$ and for any $a \in Z_n^*$, the function $f_a\colon Z_n^* \to Z_n^*$ defined by $f_a(x) = ax \mod n$ is a permutation of Z_n^*, that is, a bijective map.

Exercise 3: (5 Credits)
Prove that the equation $ax \equiv ay \pmod n$ implies $x \equiv y \pmod n$ whenever $\gcd(a, n) = 1$. Show that the condition $\gcd(a, n) = 1$ is necessary by supplying a counterexample with $\gcd(a, n) > 1$.

Exercise 4: RSA public-key cryptosystem (7 Credits)
Let $S_A = (d, n)$ and $P_A = (e, n)$ be the secret and public key of Alice, respectively. Here $n = pq$, where p and q are distinct primes. We assume that $P_A = (e, n)$ is known for all participants.
Prove that if Alice's public exponent e is 3 and an adversary obtains Alice's secret exponent d, where $0 < d < \varphi(n)$, then the adversary can factor Alice's $n = pq$ in time polynomial in the number of bits in n.

Exercise 5: RSA public-key cryptosystem (10 Credits)
Letters $A, B, C, \ldots, Y, Z$ are identified with their letter number in the alphabet. Thus, $A = 01, B = 02, \ldots, Z = 26$. By way of example, the three numbers "18 19 01" would encode the word "R S A".
Let $p = 7, q = 11$ and e be the smallest odd positive integer that is relatively prime to $\varphi(n)$, where φ denotes Euler's phi function.
Based on p, q, e and the encoding of letters as above, use the RSA public-key cryptosystem

(a) to encode the word "H U T" and

(b) to decode the word "68 71 68".

Deadline: Wednesday - January 23, 2019 - 12.15pm