Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 8

Exercise 8-1 Recall the definition of the group $\mathbb{Z}_N^*$ and that its order, i.e. the number of elements, is denoted $\phi(N)$.

a) Show $\phi(p^e) = p^e(p-1)$ for any prime p and any $e \leq 1$.

b) Show that $\phi(pq) = \phi(p)\phi(q)$ if p and q are relatively prime.

Hint: Use the Chinese Remainder Theorem.

Exercise 8-2 Let p and q be the primes 17 and 23. Let $N := pq$ and $e := 3$.

a) Compute a number d, such that $d = e^{-1} \mod \phi(N)$.

b) Encrypt the message `abc` using Plain RSA, where $\mathsf{Enc}(m) = m^e \mod N$ and $\mathsf{Dec}(m) = m^d \mod N$. Use an appropriate encoding. Verify that it decrypts correctly.

Exercise 8-3

a) Find all the elements the group $\mathbb{Z}_{13}^*$ of that generate cyclic subgroups of prime order.

b) Show: If g generates $\mathbb{Z}_p^*$, where $p > 2$ is prime, then g^2 generates $\{x \mid \exists y.\, x \equiv y^2 \mod p\}$.

Exercise 8-4 The Diffie Hellman protocol uses a group generating algorithm that outputs a description of a finite cyclic group G together with its order q and a generating element g.

In practice one often uses subgroups of prime order of $\mathbb{Z}_p^*$, for some p. Then, one can take the triple (p, q, g) as the output of the group generating algorithm. This denotes the subgroup of $\mathbb{Z}_p^*$ of order q that is generated by $g \in \mathbb{Z}_p^*$, i.e. $G = \{g^i \mod p \mid i \in \mathbb{N}\}$.

Suppose in the first step of the Diffie-Hellman protocol, the group generating algorithm output $(11, 5, 3)$. Work through the rest of one run of the algorithm with this group.