Modern Cryptography Dec 10, 2019

Homework 10

Lecturer: Daniel Slamanig, TA: Karen Klein, Guillermo Perez Due: 23.59 CET, Dec 18, 2019

To get credit for this homework it must be submitted no later than Wednesday, December 11th via TUWEL. If you have not registered for the tutorial (192.063 Tutorial on Introduction to Modern Cryptography 2019W) on TUWEL, please do so. If you are unable to register for the course on TUWEL for some reason, submit your homework via email to via email to `michael.walter@ist.ac.at`, please use "MC19 Homework 10" as subject.

1. Key-Exchange
   - **[10.1 in book, 2nd edition]** Let Π be a key-exchange protocol, and $(\mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme. Consider the following interactive protocol Π' for encrypting a message: first, the sender and receiver run Π to generate a shared key k. Next, the sender computes $c \leftarrow \mathsf{Enc}_k(m)$ and sends c to the other party, who decrypts and recovers m using k.
     - Formulate a definition of indistinguishable encryptions in the presence of an eavesdropper (cf. Definition in part 1 of the lecture) appropriate for this interactive setting.
     - Prove that if Π is secure in the presence of an eavesdropper and $(\mathsf{Enc}, \mathsf{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper, then Π' satisfies your definition.
2. Discrete Logarithms (Baby-Step/Giant-Step Algorithm)
   - Prove that the Baby-Step/Giant-Step algorithm computes the discrete logarithm x given $g^x = h \bmod p$.
   - How are the fact that g is a generator of $\mathbb{Z}_p^*$ and the uniqueness of the output of the algorithm related? When is the output not unique?
   - Compute the discrete logarithm for $g^x = h \bmod p$ with $g = 3$, $h = 13$ and $p = 29$ using the Baby-Step/Giant-Step algorithm.
3. Group generators
   - Provide a proof for the following statement: If there exists a generator modulo n, then there are $\varphi(\varphi(n))$ many of them.