(Applied) Cryptography

Tutorial for week 7

Bernardo Portela (bernardo.portela@fc.up.pt) Rogério Reis (rogerio.reis@fc.up.pt)

November 17, 2023

1. Compute the following discrete logarithms:
   (a) $\log_2(13)$ in $\mathbb{Z}_{23}$, i.e., find x s.t. $2^x \equiv 13 \pmod{23}$.
   (b) $\log_{10}(22)$ in $\mathbb{Z}_{47}$.
   (c) $\log_{627}(608)$ in $\mathbb{Z}_{941}$.
2. Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a Diffie-Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks your assistance, so you tell him to use the secret exponent $b = 871$. What is the value B should Bob send to Alice, and what is the secret shared value? Can you guess the secret exponent used by Alice? Check the exponent used by Alice that you found to see if it matches the secret shared value computed by Bob.
3. In the Diffie-Hellman protocol, and given the public parameters p, prime, and $g \in \mathbb{Z}_p$, each participant selects a secret number x and sends the other participant $g^x \mod p$. What would happen if the participants sent each other $x^g \mod p$ instead? Give one method Alice and Bob could use to agree on a key. Can Eve (a passive attacker) break the system without finding the secret numbers? Can Eve find the secret numbers?