

HW #5: Protocols: Authentication and Key Exchange
CS 392/681: Computer Security
Fall 2006

[50pts] DUE 10/21/2006 (midnight)

Problem 1 [5+20pts]

Alice has a discrete-logarithm secret key x and the corresponding public key such that $y = g^x \pmod p$ (p, q, g are discrete-log parameters). Assume that Alice's public key is delivered to Bob in an authenticated manner (e.g., through a CA that both Alice and Bob trust). Alice proves to Bob that she knows the secret key x corresponding to the public key y using the following protocol:

1. Alice chooses a random k in Z_q , computes $r = g^k \pmod p$, and sends k in Bob
 2. Bob picks an l -bit long random nonce c and sends it to Alice
 3. Alice computes $s = k + cx \pmod q$ and sends s to Bob
 4. Bob accepts/rejects if $g^s = ry^c \pmod p$ or not.
- Does the above protocol satisfy the “correctness” property?
 - Is the above protocol secure in the presence of an active attacker? If so, why and under what conditions? If not, why? Note that it is computationally infeasible for an attacker to break the discrete-logarithm problem (i.e. to compute x , given y, p, q, g)

Problem 2 [25pts]

A and B share keys K_a and K_b , respectively, with a trusted authority T. A authenticates to B using the following protocol:

A \rightarrow B: Here's A
B \rightarrow A: Nb (a nonce)
A \rightarrow B: Enc(K_a , Nb)
B \rightarrow T: Enc(K_b , (A, Enc(K_a , Nb)))
T \rightarrow B: Enc(K_b , Nb)

[Enc(K, m) denotes a symmetric-key encryption (such as AES) of message m with the key K .]

Show an attack on the above protocol.