

HW # 3

Solution

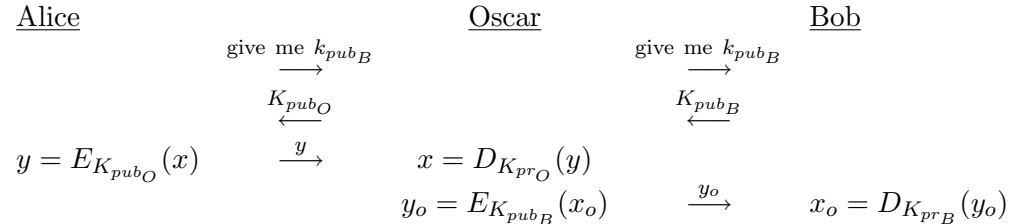
1. (15 points) Consider the following protocol which Alice uses to send a secret message to Bob:

1. Alice asks Bob for his public key K_{pub_B} .
2. Bob sends his public key K_{pub_B} to Alice.
3. Alice now encrypts the message x as follows: $y = E_{K_{pub_B}}(x)$.
4. Alice sends y to Bob.

Assume that Oscar can intercept messages, modify messages and create messages. However, he can not break the cryptosystems. Given the protocol above, perform the following tasks:

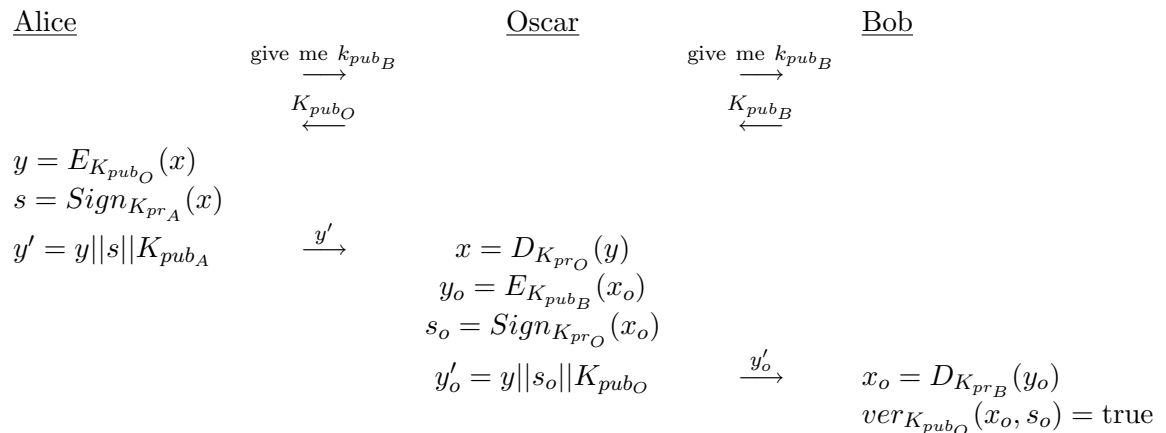
- (a) Which attack could Oscar use to be able to read and modify Alices message? Describe the Attack using the notation above.

The attack is called Man-in-the-Middle Attack.



- (b) If Alice would send $y' = y || \text{Sign}_{K_{pr_A}}(x) || K_{pub_A}$ in step 4 to Bob, could Oscar still read and modify Alices message? If so describe how he could do this using the notation above.

Yes



- (c) Now Alice and Bob are really angry at Oscar and they want a new scheme that relies on public key cryptography and secret key cryptography, but where they can find out if Oscar reads and changes messages. The new scheme should not involve any 3rd party like a CA or KDC. Can such a scheme exist? Explain briefly.

Such a scheme can not exist. It is impossible to establish secret communication between two parties if the attacker (Oscar) can intercept, modify, and fabricate any message between the two parties.

Alice and Bob would have to have a pre-established secret or out-of-band communication to verify that they are talking to each other and not to Oscar.

2. (10 points) Find at least one on-line certification authority that issues certificates to individual users at no cost. Learn about the procedure used to issue certificates.
- Prepare data necessary for your application, and apply for a certificate.
 - Analyze the obtained certificate, and find the size and position of its most significant fields.
 - If the policy of the given certification authority allows that, revoke your certificate, download the CRL containing the serial number of your certificate, and analyze the contents of this CRL.
 - Write a short report documenting your findings.

No solution published as the result is based on your experience.

3. (5 points) Compute the two public keys and the common key for the Diffie-Hellman key agreement protocol with $p = 479$, $\alpha = 2$, and $a_A = 5$, $a_B = 7$.

Perform the computation of the common key for Alice and Bob. This is also a perfect check of your results.

Alice

$$k_{prA} = a_A = 5$$

$$k_{pubA} = b_A = \alpha^{a_A} \text{ mod } p$$

$$k_{pubA} = b_A = 2^5 \equiv 32 \text{ mod } 479$$

$$k_{AB} = b_B^{a_A} = \alpha^{a_A a_B} \text{ mod } p$$

$$k_{AB} = 128^5 \equiv 198 \text{ mod } 479$$

Bob

$$k_{prB} = a_B = 7$$

$$k_{pubB} = b_B = \alpha^{a_B} \text{ mod } p$$

$$k_{pubB} = b_B = 2^7 \equiv 128 \text{ mod } 479$$

$$k_{AB} = b_A^{a_B} = \alpha^{a_A a_B} \text{ mod } p$$

$$k_{AB} = 32^7 \equiv 198 \text{ mod } 479$$