

# HW # 3

Due Date: Wednesday, September 26th, 2007, 7:20 PM  
at the beginning of class

## Reading Assignment:

- W. Stallings, *Cryptography and Network Security*, Chapter 2.1, 2.2, 7.3, 9.1, 10.1, 10.2, 11, 14.2, 15.1.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapters 1.3–1.11.

## Problems:

Please use very legible handwriting or type the answers. In either case you can draw diagrams and write formulae by hand but they have to be legible and the diagrams have to be labeled clearly. Answers that neither the TA nor the instructor can read receive 0 points. You are allowed to work in groups on these problems but you have to **write your own solution** in your own words. Copying the solution from someone else (in class or otherwise e.g. Internet) is a serious honor code violation and will be treated as such.

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.
- (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.
- (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.

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.
  - (a) Prepare data necessary for your application, and apply for a certificate.
  - (b) Analyze the obtained certificate, and find the size and position of its most significant fields.
  - (c) 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.
  - (d) Write a short report documenting your findings.
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.