Homework 3

Required Reading Assignment

W. Stallings, "Cryptography and Network-Security,"

- 8th edition: Chapter 15 Cryptographic Key Management and Distribution
- 7th edition: Chapter 14 Key Management and Distribution.

Written Assignment

due by Tuesday, September 29, 11:59pm

(submission using Blackboard)

Problem 1

Demonstrate graphically an active attack against the following protocol:

1. A sends to B

   (A, $E(PU_B, M)$, B)

2. B sends to A

   (B, $E(PU_A, M)$, A)

The attack should break the following security services attempted to be implemented by this protocol:

C - Confidentiality
AR - Authentication of the Receiver.

Notation:

X represents a unique name of user X, where X=A or B
M means a message
$E(PU_Y, Z)$ means Z encrypted using a public key of Y

Hint:

Assume that

- the receiver knows the identity of the sender only based on the contents of the data stream received in the first step of the protocol
- an attacker can be a valid user of a network.

Problem 2

Draw a four-level hierarchy of the certification authorities, including

USA – state – city/county – institution,

that includes George Mason University (GMU), University of Virginia (UVA), and University of South Florida (USF).

Assuming that

- **Public Key Infrastructure with Strict Hierarchy is being used**
- **during registration, each user receives only the public key of his local CA and the public key of the USA,**

answer the following questions:

1. Which certificates need to be added to a signed message sent
   a. by Jordan from GMU to Betty from UVA,
   b. by Lucia from USF to Sandeep from GMU?

2. Which certificates need to be downloaded from the public repository and verified by the sender before sending an encrypted message to the respective receiver in case of the following transmissions:
   a. by Jordan from GMU to Betty from UVA,
   b. by Lucia from USF to Sandeep from GMU?

Requirements and Hints:

- **Please use the notation introduced in slides for Lecture 4 to denote certificates.**
- **The correct answers for question 2) are substantially different from the correct answers for question 1).**
- **You need to solve four individual problems corresponding to the cases 1a, 1b, 2a, and 2b.**

3. How many public-key encryptions, public-key decryptions, signature generations, and signature verifications, including those involving both the message and the certificate chain, need to be performed by the sender and the receiver in each of the four aforementioned cases: 1a, 1b, 2a, 2b? Please provide a number separately for each kind of operation.

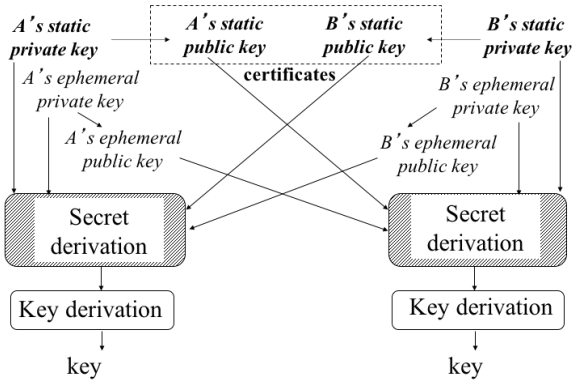
Assumptions:

- **Certificate Revocation Lists (CRLs) are issued separately by each Certification Authority, and cover only certificates issued by the respective CA.**
- **Certificates and CRLs are stored in a single public repository.**

4. What are the possible ways of minimizing the number of certificates that need to be verified by
    a. receivers in cases 1a and 1b, and
    b. senders in cases 2a and 2b?

Problem 3

Explain the difference between the static and ephemeral public key pairs used in the authenticated key agreement scheme shown in the figure below.



What is a difference between these two key pairs? What is a role of each pair?