CNT 5410

Project

1. Goals

The goal of this project is to implement a few selected algorithms/protocols/methods of network security. The programming language can be Java, C, or C++.

2. Part 1 (Due Date: Oct. 9)

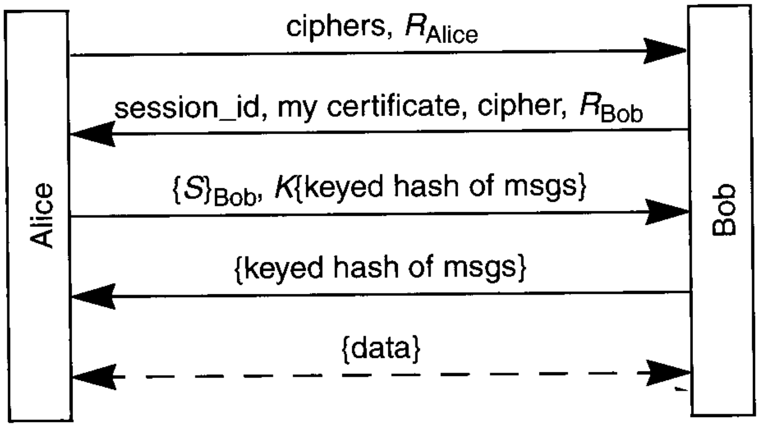
(1) Implement 3DES.
(2) Implement 3DES/CFB for encryption.
(3) Implement 3DES/CBC for integrity protection.
(4) Implement 3DES/PCBC for encryption and integrity protection.
(5) Implement RC4 for encryption.
(6) Implement a toy RSA to encrypt one byte at a time using the following parameters: p = 13, q = 19, e = 5; p = 11, q = 23, e = 3.

Please use the DES library, which can be found from the web; but you should write your own CFB, CBC, PCBC, 3DES, and RC4.

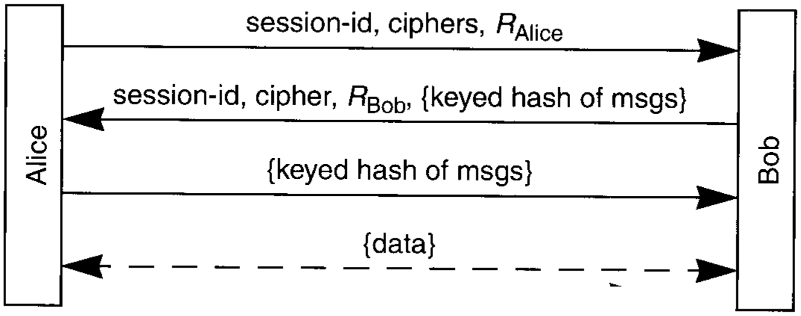
3. Part 2 (Due Date: Nov. 29)

Write a number of SSL-like routines, including at least the following.

(1) Routines for establishing SSL-like connections. They first establish TCP connections and perform the following negotiation. All exchanges shown in the figures below must be implemented. In particular, RSA should be implemented but small public/private keys may be used to encrypt one or two bytes at a time.


ciphers, R_{Alice}
session_id, my certificate, cipher, R_{Bob}
$\{S\}_{\text{Bob}}$, K\{keyed hash of msgs\}
{keyed hash of msgs}
{data}
Alice
Bob

Protocol 19-2. Session initiation if no previous state


session-id, ciphers, R_{Alice}
session-id, cipher, R_{Bob}, {keyed hash of msgs}
{keyed hash of msgs}
{data}
Alice
Bob

Protocol 19-3. Session resumption if both sides remember session-id

(2) Routines for securely exchanging data. They should support the following services: i) A service that uses 3DES/CFB (based on Fig. 4-9) for privacy protection between a client and a server. ii) A service that uses 3DES/CBC (based on Fig. 4-15) for integrity protection between a client and a server. iii) A service that uses 3DES/PCBC (Fig. 13-5) for both privacy and integrity protection. iv) A service that uses RC4 for privacy between a client and a server.

The routines for sending and receiving data may take parameters that specify which services are used. They should also have a parameter indicating whether an eavesdropper should be simulated to modify, remove, or add ciphertext blocks before data are sent out.

Write an application that calls the routines for file transfer. The client and the server must display whatever they see in their respective console windows, including all control and data messages.