

Homework 4

Due date: Nov 13

1. (30 pts) You wish to send an email to your project team member Bob. In the email body, you present some of your ideas to design the framework of the project. You also send an attachment of the GnuPG software package, because Bob complained to you that he has trouble accessing the software for his homework. Please identify the security need in this scenario, state how you achieve these security needs (*e.g.*, use which cryptographic algorithm(s): DES, RSA, DSS, etc.), and explain the reason behind your choices and measures.
2. (40 pts) Alice wants to send a message m to her stockbroker Bob. The message contains a list of trading instructions. Each instruction is represented as an entry with three fields of the same lengths: “[num shares] [sell/ buy] [stock symbol]”. She has a pair of RSA public (K_{U_A}) and private (K_{R_A}) keys and a public-key certificate C_A from Verisign. Alice also has a public key of Bob (K_{U_B}) which she retrieved from a public key server.

Here is what Alice does to send the message m .

- (a) Alice first generates a fingerprint of Bob’s public key K_{U_B} , then calls Bob to verify the fingerprint (Refer to GnuPG for the concept of fingerprint);
- (b) Alice randomly picks a new DES key K_S , and computes $C_K = E_{RSA}(K_{R_A}, E_{RSA}(K_{U_B}, K_S))$ using RSA algorithm;
- (c) Alice computes $C_m = E_{DES-ECB}(K_S, m)$ in ECB mode using DES algorithm;
- (d) Alice sends $C = C_K || C_m$ to Bob along with her certificate C_A .

Here is what Bob does, upon receiving C :

- (a) Bob verifies Alice’s certificate C_A , and retrieves her public key K_{U_A} ;
- (b) Bob verifies the authentication and integrity of C_K and decrypts it via $K_S = D_{RSA}(K_{U_A}, D_{RSA}(K_{R_B}, C_K))$;
- (c) Bob decrypts the message $m = D_{DES-ECB}(K_S, C_m)$ via DES in ECB mode.

Please identify the security weakness in the above communication protocol, and suggest how you can improve it.