

Test 2 Review

Name _____

Student ID number _____

Notation: Encrypt M with Bob's public key: $\{M\}_{\text{Bob}}$

Sign M with Bob's private key: $[M]_{\text{Bob}}$

Encrypt P with symmetric key K is denoted $E(P,K)$

Decrypt C with symmetric key K is denoted $D(C,K)$

$h(x)$ is a secure cryptographic hash function

Directions: Read each problem carefully and provide complete, but concise answers. When analyzing protocols, we assume that the cryptography is secure.

1) (10 points)

a) Why do we hash passwords that are stored in a password file?

b) Why is it better to hash passwords than to encrypt the password file with a symmetric cipher?

2) (10 points) Timestamps and nonces are both used in security protocols to prevent replay attacks.

a) Give one significant advantage of a timestamp over a nonce.

b) Give one significant advantage of a nonce over a timestamp.

3) (10 points)

a) Methods used to prevent covert channels are inherently weak. Is it better to use such weak methods or to do nothing at all? Why?

b) Suppose that the only cryptosystem you have access to is known to be weak. Is it better to use this weak system to encrypt your data or to do nothing at all? Why?

c) Methods used for inference control are inherently weak. Is it better to use such weak methods or to do nothing at all? Why?

4) (10 points) With respect to biometrics,

a) What is the authentication problem?

b) What is the identification problem?

c) Which is inherently easier, authentication or identification? Why?

5) (10 points) Recall Lampson's access control matrix.

a) Give one significant advantage of capabilities over ACLs.

b) Give one significant advantage of ACLs over capabilities.

6) (10 points) Suppose that passwords are stored as follows, where there are 128 possible choices for each character: If a password exceeds 16 characters, it is truncated to 16 characters. If a password is less than 16 characters, it is padded with "A" until it is exactly 16 characters. The resulting 16-character password is split into two parts, X_0 and X_1 , where X_0 consists of the first 8 characters and X_1 consists of the last 8 characters. Then we compute and store $Y_0=h(X_0)$ and $Y_1=h(X_1)$, which are used for password verification.

a) What is the expected work for an exhaustive search to recover one specific password?

b) How could you attack a specific password in a way that would, in general, provide a significant shortcut over an exhaustive search and also provide an improvement over a standard dictionary attack?

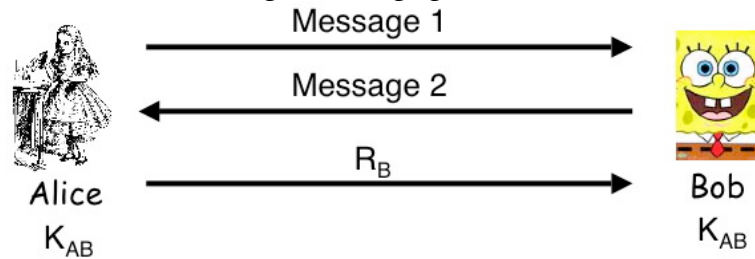
7) (10 points) At which layer of the protocol stack does each of the following types of firewalls operate?

a) packet filter

b) stateful packet filter

c) application proxy

8) (10 points) Consider the following 3-message protocol.



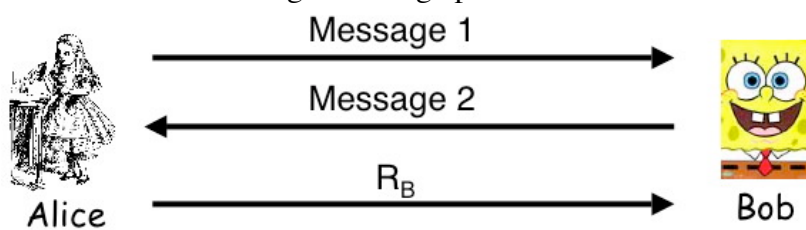
For each part below, answer the following: Is the protocol practical, given that Bob is a server dealing with many users? Who is securely authenticated? Is the session key K secure?

a) Message 1: "Alice", $E(K, R_A, K_{AB})$ Message 2: $R_A, E(R_B, K_{AB})$

b) Message 1: "Alice", R_A Message 2: $E(K, R_A, R_B, K_{AB})$

c) Message 1: $E(\text{"Alice"}, K, R_A, K_{AB})$ Message 2: $R_A, E(R_B, K_{AB})$

9) (10 points) Consider the following 3-message protocol.



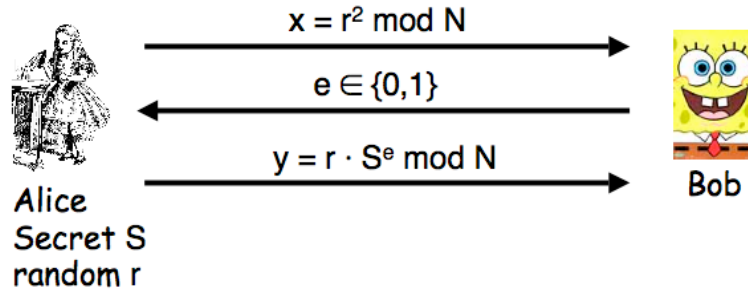
For each of the following, answer the same questions given in the previous problem.

a) Message 1: $\{\text{"Alice"}, K, R_A\}_{Bob}$ Message 2: R_A, R_B

b) Message 1: "Alice", $\{K, R_A\}_{Bob}$ Message 2: $R_A, \{R_B\}_{Alice}$

c) Message 1: $\{\text{"Alice"}, K, R_A, R_B\}_{Bob}$ Message 2: $R_A, \{R_B\}_{Alice}$

10) (10 points) The Fiat-Shamir zero knowledge protocol is illustrated below. Suppose that $N = 63$ and $v = 43$.



a) In the first iteration of the protocol, Alice sends $x = 37$ in message one, Bob sends $e = 0$ in message two and Alice sends $y = 10$ in message three. Precisely what does Bob compute to verify this iteration of the protocol?

b) In the second iteration of the protocol, Alice sends $x = 37$, Bob sends $e = 1$, and Alice sends $y = 4$. Find S and verify that $v = S^2 \pmod N$. Hint: $10^{-1} \pmod{63} = 19$.