CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Final Exam

January 10, 2005

Question 1. (*60 pts.*) Answer briefly each of the following questions:

a. What are the differences between a MAC and a digital signature? What are the respective advantages of each?

b. Does collision-resistance imply one-wayness? Explain briefly.

c. A dishonest dealer might distribute "bad" shares for a Blakley threshold scheme, i.e., shares for which different t-subsets determine different keys. Given all n shares, we could test the consistency of the shares by computing the key for every one of the $\binom{n}{t}$ t-subsets of participants, and verifying that the same key is computed in each case. Describe a more efficient method for testing the consistency of the shares.

d. What is the purpose of the salt in password-based authentication systems? Describe how it is used when a user logs into the system from a terminal.

e. What is the main advantage of the Expanded Needham-Schroeder Protocol over the basic one? How is this feature achieved?

f. What is the "single sign-on" property? How does Kerberos provide it?

g. Where would you prefer using an anarchical PKI over an hierarchical one? Where would you prefer an hierarchical one?

h. What is NAT? Why is it problematic for IPsec AH?

i. Why is the TCP sequence number a possible source of complication for the IV attacks on the TCP port number? Under what kind of ISN (initial sequence number) generation schemes is this problem easy to deal with?

j. Given that CBC-MAC is provably secure as a MAC, why does it fail in PEM? Explain briefly.

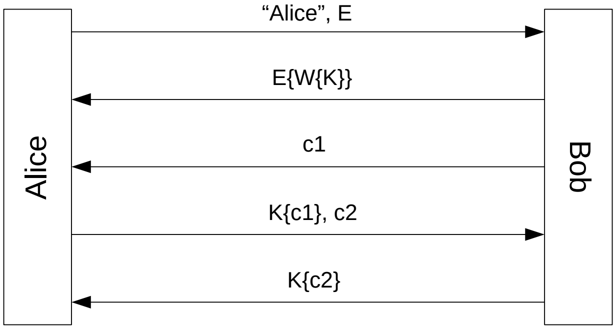
k. What are the major risks of doing e-commerce over SSL/TLS? How does SET deal with these problems?

l. Why doesn't it suffice to be undetectable for a watermarking scheme to be secure? Explain the concept with an attack that doesn't require detection.

Turn the page

Question 2. (*20 pts.*)

Consider the following EKE-type protocol, where E is a per-session public key generated by Alice's terminal, W is the shared secret derived from Alice's password, and K is the session key to be used.



a. Why is this protocol not secure?

b. Describe a simple modification to secure this protocol.

Question 3. (*20 pts.*)

a. Briefly describe how a puzzle scheme is used against denial of service (DoS) attacks in cryptographic authentication protocols.

b. How can you make such a puzzle scheme adaptive so that the server responds to increasing demand with increasingly difficult puzzles.

c. Describe how you can make the server remain stateless until the client is authenticated. The system must take caution that the same client cannot use the same answer over a long period of time.

d. Why is a one-way hash function preferred in these puzzle schemes rather than mathematical problems, such as factoring an integer of a certain size?

Good luck