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

Final Exam

January 10, 2008

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. What is the risk of using the same k value multiple times in ElGamal encryption? Discuss briefly.

c. In an RSA system, is it safe to have a common modulus n used by all users (where the factorization of n is known by a trusted authority)? Why/why not?

d. Establishing a secure channel between two previously unacquainted parties over an insecure network requires support from a trusted third party, either a KDC or a CA. What are the relative advantages of each approach?

e. What is the basic idea of ID-based encryption? Name an advantage and a disadvantage of ID-based encryption against traditional, certificate-based solutions.

f. Describe briefly how an offline dictionary attack works. How does salt help defending against these attacks?

g. What is TGT in Kerberos? Describe how it is used briefly. What is a performance advantage of having the TGT encrypted with the KDC's master secret rather than the user's master secret?

h. What is the main strength of the EKE protcol in comparison to Lamport's hash scheme?

i. What is the replay protection mechanism in AH and ESP? Explain its operation briefly.

j. What is a virtual private network (VPN)? How can IPsec help establishing a VPN? Which mode of IPsec operation would be used for this kind of application?

k. Two approaches regarding generation of qualified (legally-binding) signature keys is, (i) the user to generate the key pair and get his public key certified by the CA, or, (ii) to have the key pair generated by the CA on a trusted computer. Name a relative advantage of each approach

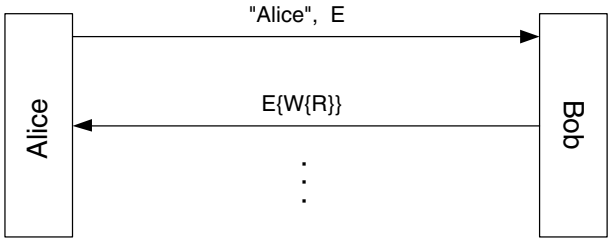
l. What is Aura et al.'s basic approach to securing Mobile IPv6? How do they achieve their purpose? Describe the basic solution they present.

Turn the page

Question 2. (*20 pts.*) On the risks of password encryption in the RSA-EKE protocol:

a. What are the risks of sending $W\{E\}$ in the first message, and of sending $W\{E\{R\}\}$ in the second message? Explain each one briefly.

b. As an alternative, consider sending the first two messages as follows:



Would this protocol solve the problems mentioned in part (a)?

c. In the challenge-response phase, which side would you have ask his challenge first? Why? Complete the protocol accordingly.

d. Show that the protocol you gave in part (c) is not secure either.

Question 3. (*20 pts.*) On Bellovin's ESP attacks:

a. Summarize how each of the following attacks works:

- Reading encrypted data cut-and-paste attack
- Connection hijacking cut-and-paste attack
- IV attack on TCP destination port number

b. Is the TCP (or UDP) checksum a problem for these attacks? Why? If so, how can it be dealt with? Explain for each attack.

c. Is the TCP sequence number a problem for these attacks? Discuss for each attack.

Good luck