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

Final Exam

January 13, 2009

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

a. What is the weakness about using the same key stream multiple times for encryption in a stream cipher? How can it be solved in practice?

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

c. What is the "cube root problem" in RSA encryption? How does the PKCS address it?

d. What is the "existential forgery" problem in digital signatures? Describe a simple solution to preclude this kind of forgery attacks.

e. What is key revocation? Is ID-based or traditional certificate-based key management more suitable with regard to key revocation? Why?

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

g. Does the Kerberos login protocol defend against off-line password guessing with eavesdropping? Explain briefly.

h. What is the limitation of EKE-type protocols that Augmented EKE (A-EKE) tries to solve? What is the approach of A-EKE to solve this problem?

i. What is SPI in IPsec? Describe how it is processed by the sender and the receiver.

j. Does the SSL session establishment protocol (i.e., the main handshake protocol of SSL) have the feature of "perfect forward secrecy"? Why/why not?

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

l. How do Aura et al. approach the problem of securing Mobile IPv6? Describe the basic solution they propose for authenticating the binding update messages.

Question 2. (*20 pts.*)

a. Describe how to realize a puzzle scheme by a one-way hash function against denial of service (DoS) attacks in cryptographic authentication protocols.

b. Make your scheme adaptive such that the server responds to increasing demand with increasingly difficult puzzles.

c. Modify your scheme so that the server remains stateless until the client is authenticated. Also be careful that a client should not be able to use the same answer over and over again.

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?

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