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

Final Exam

January 4, 2010

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

a. What is the major limitation of a traditional substitution cipher? How do modern block ciphers address it?

b. Consider the RSA algorithm where the modulus n is a large prime rather than a composite number. Would the encryption be secure? Why/why not?

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

d. What is function sharing? What is its advantage over simple secret sharing?

e. What is the salt in a password-based authentication system? How does it help in defending against offline dictionary attacks?

f. Describe how the Kerberos login protocol works. Is it secure against offline password guessing with passive eavesdropping?

g. What is the advantage of a puzzle scheme for DoS protection over a cookie scheme?

h. What is the main advantage of EKE-type strong password protocols?

i. What is an SA in IPsec? Describe how the sender and the receiver finds the SA to be used to process an IP packet.

j. Describe how 3D-Secure is related to and differs from its predecessor SET.

k. What is the advantage of using 3D-Secure in on-line purchases?

l. What are the relative advantages and disadvantages of S/MIME and PGP? What are the environments that would favor each?

Turn the page

Question 2. (*20 pts.*) Explain the following points regarding Tuomas Aura's talk on Mobile IPv6 security:

a. What is the problem with the binding updates when no authentication is present?

b. What is the approach of Aura et al. to this problem?

c. What is the basic solution they propose?

d. What is the problem with this solution when satellite links are common?

e. What would be a simple solution to prevent such passive attacks? (without any major changes to the basic setting such as adding a PKI)

Question 3. (*20 pts.*) A protocol to establish a fresh session key using long-term, certified Diffie-Hellman public keys is the protocol of Yacobi and Shmuely. The protocol, in a slightly modified form, is as follows:

- The system has a common prime modulus p and a generator g. Each party i has a long-term private key $\alpha_i \in Z_{p-1}$ and a public key $P_i = g^{\alpha_i} \bmod p$.
- To establish a session key between i and j, party i generates a random $R_i \in Z_{p-1}$, computes $X_i = \alpha_i + R_i \bmod p - 1$, and sends X_i to j. Similarly, j computes a random $R_j \in Z_{p-1}$, $X_j = \alpha_j + R_j \bmod p - 1$, and sends X_j to i.
- i computes the session key as
$$K_{i,j} = (g^{X_j} P_j^{-1})^{R_i} \bmod p$$
and j computes
$$K_{j,i} = (g^{X_i} P_i^{-1})^{R_j} \bmod p.$$

a. Show that the protocol is correct (i.e., $K_{i,j} = K_{j,i}$).

b. Show that a passive attacker Trudy who has broken a session key $K_{A,B}$ between Alice and Bob can compute any future session keys between these two parties.

c. Describe a simple addition to the session key computation which will preclude this and any similar attacks on this protocol.

Good luck