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

Final Exam

January 5, 2013

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 PKCS address it?

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

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

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

g. 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?

h. 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?

i. What is a replay attack? Describe the replay protection mechanism in AH and ESP. Explain how it works briefly.

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. 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. Describe briefly Bellovin's connection hijacking attack on IPsec encryption without authentication. Why is the TCP sequence number a source of complication in this attack? How can it be tackled?

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