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

Midterm Exam

November 2, 2006

Question 1. (*40 pts.*) Answer briefly each of the following questions:

a. What is the Kerckhoffs' principle? Why is that principle important?

b. In which of the ECB, CBC, OFB, CFB, and CTR modes of operation, is decryption parallelizable?

c. Why is collision resistence a requirement for cryptographic hash functions? Explain with an attack scenario.

d. Consider "randomized hashing" where a signer to sign a message m first generates a sufficiently long (say 128-bit) random r, computes $H(r\|m)$, and signs it along with r. Would collision resistence be a requirement for H in this case? Why?

e. Can the Merkle-Hellman knapsack cryptosystem be used as a signature algorithm in a straightforward manner—using the private key operation for signing and the public key operation for verification? Why/why not? (Assume the input is always hashed before signing; hence existential forgery attacks are not applicable.)

f. Suppose all members in a group use 5 as their RSA encryption exponent. What is the risk of sending the same message to multiple members in such a system? How does PKCS solve this problem?

g. Consider the signature scheme obtained from the graph isomorphism zero-knowledge protocol as discussed in class. Why do the graphs generated per-signature must be included in the hash that produces the challenge sequence? Explain briefly.

h. What is the limitation of simple secret sharing systems that function sharing schemes aim to solve? Discuss briefly.

Turn the page

Question 2. (*20 pts.*) Being a finite-state machine an LFSR eventually cycles. An LFSR is said to have maximal period if, when started at any non-zero state, it visits all non-zero states before it enters a state for a second time—i.e., has a cycle length of $2^n - 1$ for any non-zero starting value. Also recall that the cells in the LFSR that are included in the feedback function are called *taps*. Prove that an LFSR can have maximal period only if

a. the leading cell x_1 is a tap,

b. the number of taps is even.

(Hint: Show that when one of these conditions is not satisfied, there is a state vector that gets into a cycle immediately.)

Question 3. (*20 pts.*) Alice and Bob are very good friends and don't mind sharing the same RSA modulus n. Of course, to have their own different private keys, they use different public exponents, e_1, e_2. Moreover e_1 and e_2 are relatively prime. A common friend Charlie sends a message x to both, encrypting it with their respective RSA keys, $y_1 = x^{e_1} \bmod n$, $y_2 = x^{e_2} \bmod n$. Show how Eve, who knows the public keys of Alice and Bob and observes the ciphertexts y_1 and y_2, can find out the message x.

Question 4. (*20 pts.*) Consider an ElGamal encryption system with public keys (p, g, β) and private key α, where p is a large prime, g is a generator of Z_p^*, and $\beta = g^\alpha \bmod p$.

a. Describe an (n, n) function sharing scheme to share the decryption function, which is unconditionally secure.

b. Discuss how this idea can be generalized to a (t, n) threshold scheme for an arbitrary $t \leq n$ using Shamir secret sharing and Lagrange interpolation. Also explain why a straightforward implementation of Shamir is not possible here.

c. Complete your threshold decryption scheme in part (b) by a special selection of the ElGamal parameters. (Hint: Take p to be a safe prime; and use $g' = g^i$ instead of g for some particular i.)

Good luck