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

Midterm Exam

November 10, 2004

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

a. Why a slow key schedule may be desirable in a block cipher?

b. Which of the ECB, CBC, OFB, CFB, CTR modes of encryption can be used with a hash function instead of a block cipher? Why?

c. Consider using a counter value instead of a random value for the IV in CBC encryption, where the counter is incremented at the beginning of each data packet to be encrypted. Comment on the security of this system in comparison to using a random IV.

d. Would CFB-MAC—with the last output block of the CFB computation over a data packet appended to the packet as a checksum—be a secure MAC? Why/why not?

e. Does one-wayness imply collision-resistance? Explain briefly.

f. 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?

g. What is the inherent key escrow feature in ID-based encryption? Explain briefly.

h. 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?

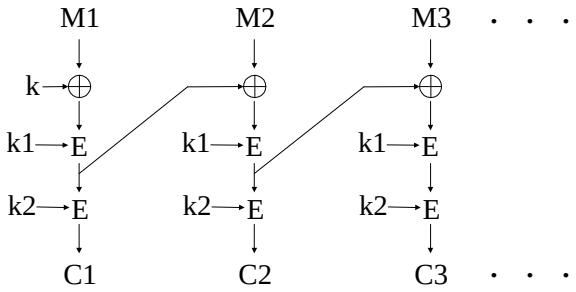
Turn the page

Question 2. (*20 pts.*) "Cyclic redundancy code" (CRC) is a moderately complex error detection algorithm which is linear. That is, for $X, \Delta X \in \{0,1\}^n$, we have $CRC(X \oplus \Delta X) = CRC(X) \oplus F(\Delta X)$ for some easy to compute function F. An earlier version of the 802.11b Wireless Ethernet Protocol used the CRC algorithm for message authentication, by encrypting the CRC checksum of each packet with a stream cipher (RC4) using a symmetric key shared by the mobile device and the base station.

a. Show that this MAC scheme of 802.11b is completely insecure.

b. Comment on the security of the system if a block cipher were used instead of a stream cipher.

Question 3. (*20 pts.*) Consider the following mode of encryption with three keys k, $k1$, $k2$, where k is of the length of the block size and $k1$ and $k2$ are of the length of the key size (denoted by ℓ) of the block cipher E. (E.g., for DES, k would be 64 bits, and $k1$ and $k2$ would be 56 bits each.)



a. Describe the decryption operation for this mode of encryption.

b. Describe a chosen-ciphertext attack where the attacker can discover the full key $(k, k1, k2)$ with $O(2^\ell)$ runs of the encryption/decryption algorithm. You can assume as much memory as you need for the attack. (Hint: Consider two ciphertext messages (C_1, C_2, C_3, C_4) and (C_1', C_2, C_3', C_4), for some randomly chosen $C_1, C_2, C_3, C_4, C_1', C_3'$.)

c. Would a similar *chosen-plaintext* attack work? Argue briefly.

Question 4. (*20 pts.*) Consider a variant of the ElGamal signature scheme where r is computed as β^k instead of g^k, and the verification procedure has β^m instead of g^m for input m.

a. How would you compute s in the new scheme?

b. What should the new verification equation be?

c. Comment on the security of this signature scheme.

Good luck