ITIS 6200/8200 Principles of Information Security and Privacy

Midterm

**Candidates:**

**Question 1**. Design MAC for storing files

05-solutions.pdf

**Question 2**. Block ciphers. Draw a diagram of reusing IV for every block in designing block cipher chaining mode. What is the formula for the ciphertext?

Is this design IND-CPA secure? Why?

**Question 3**. Length extension attack on some MAC() design

**Question 3. Hash**

Alice’s computer stores the files in the following way: for every file F, the computer will calculate the hash value of the file hash(F), (e.g., using SHA-2) and store it after the file. Every time when Alice login, the machine will automatically hash all the files and compare the results to the stored hash values. In this way, if by accident the hard drive is mis-functioning and flips a few bits in a file, Alice can immediately detect it since the hash value will be different. Now an attacker hacks into Alice’s machine and he tries to change several files. The attacker also knows the hash function that the computer uses. Please describe what the attacker needs to do so that the next time Alice login, the machine will not detect the changes. **Also, please discuss how we should improve the mechanism to detect such changes.**

**Question 4. PRNGs and Diffie-Hellman Key Exchange**

Eve is an eavesdropper between Alice and Bob.

1. Alice and Bob each seed a PRNG with different random inputs.
2. Alice and Bob each use their PRNG to generate some pseudorandom output.
3. Eve learns both Alice’s and Bob’s pseudorandom outputs from step 2.
4. Alice, without reseeding, uses her PRNG from the previous steps to generate a, and Bob, without reseeding, uses his PRNG from the previous steps to generate b.
5. Alice and Bob perform a Diffie-Hellman key exchange using their generated secrets (a and b). Recall that, in Diffie-Hellman, neither a nor b are directly sent over the channel.

Assume that Eve always learns the internal state of a PRNG between steps 3 and 4. Eve wants to learn the Diffie-Hellman shared secret gab mod p.

Q 4.1: If Alice and Bob both use a PRNG that are not rollback-resistant. Can Eve learn about the shared secret gab mod p? If yes, how?

Q 4.2: If Alice uses a PRNG that is not rollback-resistant. Bob uses a PRNG that outputs the same number each time. Can Eve learn about the shared secret gab mod p? If yes, how?

Q 4.3: Diffie-Hellman Key Exchange is vulnerable to Man-in-the Middle attack. Consider Mallory, who can intercept and modify the messages between Alice and Eve. If