ITIS 6200/8200 Principles of Information Security and Privacy

Midterm

**Candidates:**

* Bob has a public-private key pair (pub\_Bob, pri\_Bob). Alice needs to send some information to Bob. She wants to make sure that when Bob opens the message, he can verify that this is from Alice but not anyone else. So she sends out the message as: [ Alice, Epub\_Bob(message) ] to Bob. Basically, she first sends out her name in clear text, then encrypts the message with Bob’s public key. Please discuss, can an attacker M impersonate Alice and send out a packet in Alice’s name? How can he do it? Here we assume that M also has the public key of Bob. For the same question, if Alice sends out [ Epub\_Bob(Alice, message) ], can M still impersonate Alice? (Here Alice puts her name in the encryption.)
* 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) 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.**

1. Name at least two advantages and two disadvantages of symmetric encryption algorithms, and provide examples to explain them.
2. Name at least two advantages and two disadvantages of asymmetric encryption algorithms, and provide examples to explain them.

**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