University Of Washington, CSE 590P – Computer Security - Homework 5

Tadayoshi Kohno, John Manferdelli

Due: 4:30pm February 15, 2007.

See the course website (http://www.cs.washington.edu/education/courses/csep590b/07wi/) for instructions on how to submit your homework via the UW Catalyst Tools. For this assignment, you should submit a PDF file named 'YourLastName-YourFirstInitial-HW5.pdf. Please write your name on the first page. The entire assignment is worth 36 points and there is an opportunity for extra credit.

1. [8] You are a cryptanalyst and are attacking a stream cipher. You learn that the "stream key" is generated by a LFSR with 4 taps ($s_{n+4} = c_0\, s_n + c_1\, s_{n+1} + \ldots + c_3\, s_{n+3} \pmod 2$) and that for 9 consecutive plaintext bits 101010010, the corresponding ciphertext is 010010101. Decrypt the next 6 bits: 110001.

2. [6] Describe in your own words the difference between a public key cipher and a block cipher. If you are designing an encryption security for large documents, what block cipher mode would you use and why? How about the encryption for the communication channel between the "situation room" in the White House and a secure facility at the Department of State (assume there are a lot of similar messages)?

3. [8] Alice publishes an RSA public key with n= 9271 and e=5. Encrypt the message m=34. What is Alice's private key? Prove it by decrypting the encrypted message to get m.

4. [7] Suppose p=67. Use El Gamal to encrypt the message m=22 and show how you would decrypt it too. Use 2 as the base for the system but pick your own random a. When you encrypt, you will of course need to pick a b too.

5. [7] An Identify Friend or Foe ("IFF") system identifies a friendly plane to a landing site. The protocol is as follows: There is a shared secret key, ks, known to all friendly planes and all authorized sites. When a plane approaches, the IFF system sends the plane a challenge consisting of a random number, r. A friendly plane sends back $E_{ks}(r)$ and if the site receives it, it regards the plane as friendly. Otherwise it sends up an interceptor missile. You are an adversary attempting to attack the landing site. Can you mount a man in the middle attack that lets your plane authenticate itself to the site's IFF system? Given your attack, fix the protocol to avoid this attack.