Assignment 3 – Due Thursday, February 25

Chapter 6 and Security Models Handout (1st part)

This assignment is shorter than normal, with only 9 days to complete it rather than a full two weeks. Because of this, it will be graded out of 50 points, and count half as much as the regular-length assignments.

1. Consider a system for playing encrypted video, where the video is stored in a large (multi-gigabyte) file using AES in CBC mode. One property you'd like to have in a video player is the ability to jump to an arbitrary spot in the video — skip ahead to the 30 minute mark, for instance. You know that the ciphertext value of any block depends on all of the data before it, but somewhat surprisingly this random access into a CBC-encrypted file is possible. Describe how you can start decrypting at an arbitrary position in the encrypted video stream. Be precise in your answer and justify why this works.

2. For the same reason that it is vital that a one-time pad key to be used only once, CTR mode requires that the initial counter value is not reused. Unfortunately, Lazy Davy doesn't understand this, and when he implements a system using AES in CTR mode, he picks a random initial counter value that he hard-codes into the system, and every encryption uses that same initial counter value. The system that encrypts data is kept in a locked room, but you have managed to gain access with a thumb drive and can encrypt one file of up to 100,000 bytes of your choosing (a chosen plaintext attack — you can't copy the code or steal the AES key). Given this setup, you can perform an encryption so that you can easily decrypt any subsequent encrypted message that is up to 100,000 bytes long. Explain exactly how you would do this: What plaintext would you use for your one chosen plaintext encryption? How would you use the information you learn to decrypt a subsequent message? Do you learn or need to know the AES key? Why or why not?

3. Think about how CTR mode is similar to an XOR-based one-time pad, and answer the following question with justification: Is AES in CTR mode a nonmalleable cipher?

4. A "key recovery attack" takes a matching plaintext/ciphertext pair (P, C) and finds a key K such that $E_K(P) = C$. We can formalize this by saying that there is a probabilistic polynomial time algorithm $\mathsf{findkey}(P, C)$ that computes K. Show that if such a function exists, then the encryption scheme is not IND-CPA secure (to do this, define the adversary functions $A_1^{\mathcal{E}}$ and $A_2^{\mathcal{E}}$ for the chosen-plaintext game, where the adversary functions can call both the encryption oracle and the findkey function). In addition to giving the algorithms, analyze the advantage of your adversary algorithm under the assumption that findkey always succeeds. *(Note: breaking this scheme is easy — what I'm really looking for here is that you can clearly and rigorously describe this in context of formal security models.)*