Quiz 5 student name: Evan Smith

1: 20 what is secret-key Encryption, is it secure enough and why, or why not?

Secret key encryption is where a key is used to produce a mask of some sort that is used to encrypt the plaintext. It is not sufficiently secure in many cases because it only requires obtaining the single secret key to decode the cyphertext. In contrast, an identity-based encoding also requires knowing a user’s personal key as well. In some cases, a secret-key encryption is sufficient, especially if that key is systematically changed in short order.

2: 25 what is mono and poly alphabetic substitute cipher? What is the famous example for poly? Why is it is hard to decode?

The most famous polyalphabetic substitute cypher (in my opinion) is the Enigma code. It is hard to decode because the secret-key is an ordering of an additional level of encoding – the encoding wheels. These wheels then reassign some letters to others in specific ways, so frequency analysis is not able to determine the cypher.

3: 15 what is DES? How does it work(briefly)? What is AES? Why is AES better?

DES is an encryption standard that splits the plaintext in half, and then uses a 56-bit key to encode the plaintext using permutation, xor, and others. AES is another encryption standard which uses a 128 bit key, and uses shuffling of rows and columns of the data matrix, among other things. AES is better for many reasons, most notably that it uses a larger key, is faster, and operates on the entire plaintext block, rather than only half.

4:10 what’s the problem with the simple encryption block by block? Which lab task this week is to show you the reason?

Encryption block-by-block applies the encoding to each block with no regard to the file as a whole, or with any look at the previous data. Task 2 from the lab this week shows that with ECB (which is block-by-block) an image is more or less discernable after encoding, since each block is separate even in encoding.

5: 30 What are those Encryption modes discussed in the book and lectures? Brief explain the encryption method for each mode ECB, CBC, CFB and OFB and and if you change one bit in second block of encrypted file, when you decode it, how many and which blocks stay the same and how many and which blocks get corrupted.

ECB – text divided into blocks, each block being padded if needed. Each block is encrypted with the same single key, meaning there is a one-to-one character alignment, and repeated plaintext blocks will produce identical cyphertext blocks. A corrupted block in an encryption only affects that block on decryption.

CBC– text divided into blocks, each block being padded if needed. The first block is encoded like ECB, expect that an imput vector IV is used to xor the block before encryption step. That encrypted block is then used to xor the next block, and so on. A corrupted block in an encryption affects all following blocks, since the error is propagated.

CFB – text is not split into blocks, and the IV is encrypted prior to xor with plaintext. The next vector is taken from the cyphertext, encrypted, and then xored with the next section. A corrupted block in an encryption affects all following blocks, since the error is propagated.

OFB – similar to CFB, except that the key used for each stage is simply encrypted each step, rather than derived from the cyphertext. A corrupted block in an encryption only affects that block on decryption.