Computer Science 161 – Computer Security
Instructor: Tygar
6 October 2010

Midterm 1

Question 1

Are the following ciphers vulnerable to a chosen plaintext attack? Show the chosen plaintext attack where it is vulnerable, or argue why it is not vulnerable

- Caesar cipher
- One-time pad
- RSA
- Rabin digital signatures

Answer: Caesar ciphers are vulnerable, since the key (shift value) can be observed from just one character of the encryption. One-time pads are not vulnerable, because the key is chosen randomly, so information about previous keys provides no information about future keys. RSA is believed to be not vulnerable, although no proof of non-vulnerability exists. Rabin signatures are vulnerable, since the ability to take square roots is equivalent to factoring.

Question 2

The cipher block chaining (CBC) mode has the property that it recovers from errors in ciphertext blocks. Show that if an error occurs in the transmission of a block C_j, but all the other blocks are transmitted correctly, then this affects only two blocks for decryption. Which two blocks?

Answer: Cipher block chaining can be written as $P_j = D_K(C_j) \oplus C_{j-1}$ where C_j and P_j are the *j*th ciphertext and plaintext blocks respectively. If C_j is corrupt, then the recovery of P_j and P_{j+1} will be corrupt, but because C_{j+1} is not corrupt, then P_{j+2} and so forth will be recovered correctly.

Question 3

Suppose Alice uses the RSA method to send a message to Bob as follows. She starts with a message consisting of several letters, and assigns $a = 1$, $b = 2$, . . . , $z = 26$. She then encrypts each letter separately and with no padding. For example, if her message is *cat*, she calculates $3^e \bmod n$, $1^e \bmod n$, $20^e \bmod n$, where *e* is Bob's public encryption key and *n* is Bob's modulus. Is this method secure? Why or why not?

Answer: It is not secure. Since *e* and *n* are public, the adversary builds a dictionary $a = 1^e \bmod n$, $b = 2^e \bmod n, \ldots, z = 26^e \bmod n$. The adversary then uses the dictionary to decode any messages.

Question 4

Consider the following variation of Triple DES: we choose keys K_1 and K_2 and compute $E_{K_1}(E_{K_2}(E_{K_2}(m)))$. (Notice that the order of keys is different from the usual version of Triple DES.) If we try to do a meet-in-the-middle attack, will be successful? Why or why not? How many encryption/decryption operations will be required?

Answer: It is vulnerable, since we can compute tables $E_{K_1}^{-1}()$ and $E_{K_2}(E_{K_2}())$. The first table requires 2^{56} decryptions and the second table requires $2 \bullet 2^{56}$ encryptions.