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

Midterm 1

Instructions: Keep answers concise

NAME_____ SECTION (TA/Hour) _____

Question 1	*Question 2*	*Question 3*	*Question 4*	*Total*

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

Instructions: Keep answers concise (write the answer to question 1 only on this sheet – use back if necessary).

NAME_____ SECTION (TA/Hour) _____

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

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

Instructions: Keep answers concise (write the answer to question 1 only on this sheet – use back if necessary).

NAME_____ SECTION (TA/Hour) _____

Midterm 1 - 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?

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

Instructions: Keep answers concise (write the answer to question 1 only on this sheet – use back if necessary).

NAME_____ SECTION (TA/Hour) _____

Midterm 1 - 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?

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

Instructions: Keep answers concise (write the answer to question 1 only on this sheet – use back if necessary).

NAME_____ SECTION (TA/Hour) _____

Midterm 1 - 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?