

**CMPSCI 177 - Computer Security**  
**Fall 2009**  
**Fourth Homework - Malware, DES, and Public Key**

Due: 28 OCT 09 2:00pm

**Part I: Malware**

1. Someone suggests a worm defense system that is based on the idea of throttling. With throttling, each machine in a network can connect to at most  $n$  other, different hosts (IP addresses) in  $t$  seconds (typical values are  $n = 10$  and  $t = 120$  seconds). Connections to any other than the first  $n$  machines are blocked (dropped) during the period  $t$ .

Name a legitimate application that is likely to be negatively affected by this system and briefly discuss your answer.

2. You are developing a worm that uses a random number generator to generate IP addresses of potential victims that the worm scans. What do you use to seed this random number generator once your worm has infected a new host?

**Part II: DES**

1. Consider the following 64 bit key:

1001110110100001010111011010100111001000111010101101011011001011

What is the value of the key used for the fourth round of the DES encryption algorithm?

2. Consider the following 48 bit string:

110101010011010010111001010001001011010101011101

If this string is input to the  $s$  boxes in the DES encryption algorithm, what string is output from the  $s$  boxes?

**Part III: Public Key**

1. Use the superincreasing sequence  $S=[1,3,7,16,39,67,145,279]$ , modulus  $n=559$ , and multiplier  $w=19$  to generate a public key sequence  $H$  for Merkle-Hellman.

2. Assume that you received the ciphertext  $C=105$  from someone using the public key generated in exercise 1. You are to decipher  $C$  and determine the message  $M$  that was used to generate  $C$ .

3. Alice has chosen primes  $p=2357$  and  $q=2551$  and exponent  $e=3674911$  to use with the RSA algorithm. What does Alice publish as her public key?

4. Suppose Alice receives the following message from Bob, who used the public key from exercise 3 to encrypt it: 3650502. Determine the plaintext that Alice obtains from this ciphertext.