**CMSC 426 Computer Security Midterm**

Name:

Assigned: 3/31/2022

Due: 4/1/2022 at 11:59pm

Total points: 100

**1. Block Ciphers (10 pts)**

a) Suppose that you are encrypting a message using 3DES, and all three keys are identical. In a few sentences, describe why this would be insecure.

b) Which block cipher mode of operation results in a ciphertext with poor diffusion? Justify your answer.

**2. Diffie-Hellman Key Exchange (10 pts)**

Suppose Alice and Bob perform the Diffie-Hellman key exchange. Alice and Bob agree on the

and . Alice chooses the private integer and Bob chooses the private integer . **Show your work** for of the following steps:

a) In the space below, show how Alice computes the value that she sends to Bob.

b) In the space below, show how Bob computes the value that he sends to Alice.

c) In the space below, show how Alice computes the key.

d) In the space below, show how Bob computes the key .

**3. RSA Cryptanalysis (15 pts)**

Suppose that Bob generates an RSA keypair with and where is a 4096-bit number. Alice encrypts the message with no padding using Bob’s public key and sends it to Bob via an insecure channel. Eve intercepts the ciphertext and knows and from Bob’s public key. With just this information (i.e. Eve does not need to factor or somehow find ), how could she decrypt ? Provide a detailed explanation below, showing a mathematical solution.

**4. CIA Triad, Hashing, and PKI (15 points)**

Suppose that Alice and Bob each have X.509 certificates associating their public keys with their identities, and they have access to asymmetric encryption and cryptographically secure hashing. Describe in detail how Alice can send a message to Bob in a way that ensures integrity, authentication, and non-repudiation of the message, but does not ensure confidentiality. Make sure to use mathematical notation where appropriate. There are multiple possible solutions to this question that will be accepted.

**5. Linux Security (10 pts)**

a) What property does a file have when its SUID bit is set on Linux? Why might a file with the SUID bit set be a good target for an exploit?

b) What three numbers must be provided to the chmod command in order to set the following permissions on a file?

* The owner can read, write to, and execute the file
* The group can read and execute the file
* All other users can read the file

**6. Password Cracking (10 pts)**

Describe a type of password cracking attack which a salted password hash would NOT be effective at defending against. Justify your answer.

**7. Windows Security (10 pts)**

a) In a few sentences, describe how the NTLM relay attack works. What must happen in order for this attack to work?

b) In a few sentences, describe the purpose of the Ticket-Granting Server (TGS) in the Kerberos protocol.

**8. Assembly and Shellcode (10 pts)**

a) Which assembly instruction is equivalent to “POP EIP”?

b) Why can the instruction “MOV EAX, 0” not typically be part of the shellcode in an exploit?

**9. Exploits and Defenses (10 pts)**

a) What is a stack canary? In a few sentences, how it defends against stack buffer overflow exploits.

b) In a few sentences, describe how a Return-to-Libc (Ret2Libc) exploit works. What type of defense does a Ret2Libc exploit circumvent?