Name: _____

CSci 530 Midterm Exam
Fall 2020

This exam is open book and open note. You may use electronic devices to consult materials stored on the devices, but you may not use them to access material through the net, or for communication during the 120 minutes in which you are completing the exam. You have **100 minutes** to complete the exam. You must submit the completed exam through the DEN drop box for CSci530 before 110 minutes from the start of the exam. (the extra 10 minutes is to provide time to logistically upload the exam and you may not use additional time to complete the answers).

Type your answers in the exam itself using word, or if you prefer a different editor using the text version of the exam that is provided. The filled out exam document will be what you will return to me as described above. In answering the questions, please TYPE your answers rather than importing large quantities of text using cut and paste in hopes that the cut an pasted text might include an answer**. Pasted text in your responses will be ignored and you will not receive credit for words included in the pasted text.**

Be sure to include your **name in the exam document. Ideally, please rename the document to a file name that includes your name (e.g. csci530-f20-mt-FIRSTNAME-LASTNAME).**

To judge the amount of time you can spend on each question, consider that you have 100 minutes and there are 100 points across the 3 questions.

There are **100 points** in all and **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Complete the following statement:

I, **(replace with your first and last name)** attest to the fact that I completed this exam within the designated time allocated (e.g. in less than 100 minutes), that I did not have knowledge of the exam or answers in advance of its start, that I did not access external material (e.g. web sites) or use the internet during completion of the exam, and that I completed the exam on my own without accepting or providing assistance to anyone else.

Signed: (type you name here). Date: 10/8/2020.

Name: _____

1. **(20 points) Identity and Key Management -** For each of the following methods of authentication and key management, match the method with the **major** characteristics or relevant terms discussed in class. This is **not** a one-to-one mapping. So one or more approach may match a characteristic or term, and a single characteristic or term may also match one or more approaches. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associated a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

    1. Smartcard
    2. Hardware Random Number Generator
    3. Diffie Hellman
    4. Certification Authority (CA)
    5. Face-ID or fingerprint
    6. Kerberos
    7. Passwords
    8. Shibboleth
    9. Microsoft Passport

[Type the corresponding numbers above, separated by commas following the lettered entries below]

a) Single sign on: _____ _____ _____ _____ _____

b) Does not provide authentication: _____ _____ _____ _____ _____

c) Key Storage: _____ _____ _____ _____ _____

d) Authentication based on something about you: _____ _____ _____ _____ _____

e) Authentication based on something you know: _____ _____ _____ _____ _____

f) Authentication based on something you have: _____ _____ _____ _____ _____

g) Federated identity management: _____ _____ _____ _____ _____

h) Can be used to create encryption keys: _____ _____ _____ _____ _____

(note that g is a little bit tricky)

i) Binds or associates key with identity: _____ _____ _____ _____ _____

Name: _____

2. (45 points) Short and medium length answers

a. Key Space – Why is it that cryptosystems with a larger key space (number of valid keys) are typically considered more difficult to break? (5 points)

b. Will a cryptosystem with a larger key size always have a larger key space? Why or why not? (5 points)

c. Describe as many as you can of the encryption, decryption and hashing steps that occur when a message is sent using PGP for both confidentiality and integrity (i.e. it is a signed and encrypted message). Be sure to include the steps used to verify certificates. (10 points)

d. Which parties are authenticated when you log into a computer system using SSH? In what ways is this authentication performed? (10 points)

e. Is the Clark-Wilson model a mandatory or a discretionary access control model? Explain the reason for your answer. (5 points)

f. Why do we consider the Clark-Wilson model an integrity policy and not a confidentiality policy? (5 points)

g. Why are mandatory access control (MAC) policies believed to be more effective at controlling information flow? (5 points)

3. (35 points) Election Campaigns

Name: _____

You have just accepted a job as the Chief Information Security Officer (CISO) for the Truden Presidential campaign (Ms. Truden is a non-partisan candidate that believes in working with both parties). Your role is to protect the computer systems, communications, and information used by the campaign for their political messaging (including advertising and statements made to the media, etc), fundraising (i.e. accepting campaign donations), campaign event scheduling, and get-out-the-vote activities.

a. What are the three basic goals for security that you will attempt to achieve with respect to the computer systems, communications, and information used by the campaign? More specifically, discuss some of the negative consequences that could result if you do not achieve these goals. Your discussion should focus on the specific activities (fundraising, scheduling, get out the vote, and messaging) that were listed above. (10 points)

   (type your answer here)

b. The recent twitter hack demonstrated that criminals were able to log into the accounts of high-profile positions and send messages that appeared to originate from their accounts. In the case of the recent twitter hack, these messages encouraged followers to send bitcoin to the criminals account, but such messages could just have easily been used to spread misleading or embarrassing information about candidates.

   As CISO for the Truden campaign, discuss some of the technical measures that you believe should be taken by the campaign, and also by messaging services like Twitter, to prevent the success of this kind of attack in the future. (Note that there are multiple measures that should be followed and you should talk about all of them that you can think of.) (15 points)

   (type your answer here)

c. Opponents of your campaign might want to obtain internal strategy documents, emails, or even donor lists from your campaign systems or even the personal devices of campaign staff. We saw this in 2016 when internal emails from the democratic national committee were posted to WikiLeaks. Based on our discussion in class (lectures), and even some of the labs, discuss steps that you would impose as CISO to protect this kind of data (e.g. emails, internal documents, voter lists, etc) from disclosure. (10 points)

   (type your answer here)