Overview of Cybersecurity (20 pts)

Question 1:

*Explain the meanings of the following security attributes in computer systems: conﬁdentiality, integrity, authenticity, accountability, availability.*

*For each attribute, describe an example in which the attribute of an asset in an information system can be potentially violated and the security techniques/controls that can be used to protect the attribute of the asset.*

**Confidentiality:** Confidentiality deals with the private and confidential information such as unauthorized entities cannot access the system.

* Violation:  
  Its common to use password protection to keep your unwanted individuals away, however there is a lot of different approaches an attacker can take to gain access anyways. E.g. the use of software to guess the password, and unfortunately its common to use weak passwords and use it to multiple accounts, which makes it way easier for the unauthorized individual.
* Protection:  
  To protect against these attacks you can choose a much stronger password, or even better, the use of two factor authentication. Some examples on this is biometrical confirmations or the use of your phone for confirmation.

**Integrity:** Integrity assures that information isn’t tampered by the program it’s using or along the destination of the information.

* Violation:  
  Even if most of the information traveling through the internet is encrypted, there exists exploits that can give an unauthorized person the ability to modify information between sender and receiver.
* Protection  
  To protect yourself from integrity attacks the sender and receiver must be assure that their software doesn’t contain any form for malware and be connected to a secure network.

**Authenticity:** Authenticity is about being able to confirm and verify the user is who they say they are, and that they are being trustworthy.

* Violation:

**Accountability:** Accountability

* Violation:  
  Yes
* Protection:  
  Yes

**Availability:** Availability

* Violation:  
  Yes
* Protection:  
  Yes

The information we have is readily accessible to those people that should have it.

Question 2:

*Consider a company whose operations are housed in two buildings on the same property:*

* *one building is headquarters*
* *the other building contains network and computer services.*

*The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters’ LAN and the Network Services’ LAN. Internet users connect to the Web server through a ﬁrewall. Dial-up users get access to a particular server on the Network Services’ LAN.*

*Read Section 1.5 in Chapter 1 and develop an attack tree in which*

* *the root node represents disclosure of proprietary secrets;*
* *there are at least 10 nodes;*
* *attacks include physical, social engineering, and technical attacks;*
* *both AND and OR nodes may be contained.*

Network attack

Software attack

Human attack

Cryptographic Tools (60 pts)

Question 3:

Encrypt the following sentence

Cybersecurity is an evolving process and is determined by the weakest link

by

* the Vigenère cipher with key k = human; and
* the column transposition cipher 34681752

The Vigenère Cipher

Question 4: