INF140 Oblig 1

Overview of CyberSecurity:

Question 1. [5 pts] Use your own words to explain each of the following security attributes in computer systems: confidentiality, integrity, authenticity, accountability, availability.

Confidentiality:
is a way to make data unreachable or shield certain parts of data, text etc. from an unauthorized user. For instance using encryption as a way of “hiding” information.

Integrity:
Integrity is used to keep information from being altered by an unauthorized source. For instance using a hash function and a cryptographic key.

Authenticity:
requires a user to verify their identity to gain access to information etc. for instance using email, passwords…

accountability:
Making an entity accessing or altering data, accountable for the actions. For instance tracing the actions back to the entity’s information.

availability:
Making the information available for the authorized users. No point in having secure measures when it’s not available to the people who need it. Poor availability programs are prone to hardware failures, and also attackers can keep the information from the authorized users.

Question 2. [4 pts] Suppose you need to protect two of the above security attributes, e.g., integrity and authenticity, of a student grade system in a university, which maintains a database of grades of all students and allows a student to check his/her grade. List possible vulnerabilities in the system that may be exploited by attackers, and possible threats that may violate these two security attributes.

Using integrity to protect the information from being altered. It needs to protect the data in the system from being altered by an unauthorized user (like a student hehe), and also that the information can not be viewed by someone other than the authorized ones(student and teacher?). Authenticity is also used so that the teacher or the student have to identify themselves before accessing the data. For instance using UiB login that is connected to your identity.

The integrity of the system needs to be equipped for intentional, as well as unintentional attacks like: user errors, data loss.

These two together need to form a system so that the user is verified and cannot bypass the integrity attribute or at least be strong enough together to stop the attacker.

Question 3. [6 pts] For the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

(i) A law enforcement organization managing extremely sensitive investigative information;
- Confidentiality - High
- Integrity - Moderate
- Availability - Moderate

(ii) A hospital managing patients' health records, which contain privacy-sensitive diseases and allergy information for each patient;
- Confidentiality - Moderate
- Integrity - Moderate
- Availability - low

(iii) An organization managing public information on its Web server
- Confidentiality- Not used
- Integrity - Moderate
- Availability - Moderate

Task 4

Encryption round 1:
EPZTKGKTUGPRGAXNREYLDECMZCPSJGUTGCNZAPMSJZTXZYXJTWRUJLDMOVIO
SBAB

Ciphertext:
WLITNCQDHQCHMVXQBGRGNQPHGPWGEOATEEXJJJLTXQHONLYKGXVAXTRHZVUA
CSLJ

('output from vigenere cipher round ', 1, ' is: ',
'EPZTKGKTUGPRGAXNREYLDECMZCPSJGUTGCNZAPMSJZTXZYXJTWRUJLDMOVIO
SBAB')
('output from vigenere cipher round ', 2, ' is: ',
'BGWEGHXZGPLEXQQVRWIXVCHUGGTJAHOANENJXMNCQOCJTVLSPAQLRXYLHTD
THQKJ')

('decryption round', 1, ' transposition: ',
'BGWEGHXZGPLEXQQVRWIXVCHUGGTJAHOANENJXMNCQOCJTVLSPAQLRXYLHTD
THQKJ')
('vigenere decryption: ', 1,
'ZPYPNTRIGAEGPYLBEURZGJTOPGECCZWVTRLSZXUOKXCUMXDAKGDJAZJSTNMT
SJMB')
('decryption round', 2, ' transposition: ',
'EPZTKGKTUGPRGAXNREYLDECMZCPSJGUTGCNZAPMSJZTXZYXJTWRUJLDMOVIO
SBAB')
('vigenere decryption: ', 2,
'CYBERSECURITYISTECHNOLOGICALLYCOMPLICATEDITISAPROCESSNOTAPRODUC
T')
('decrypt',
'CYBERSECURITYISTECHNOLOGICALLYCOMPLICATEDITISAPROCESSNOTAPRODUC
T')

Question 5. [3 pts] Explain the six design requirements of cryptographically strong hash functions.

a hash function has to: