# TK2100

T-00 INTRODUKSJON

1. Hva er informasjonssikkerhet?
   * Information security centers around three main areas:
     + Confidentiality
     + Integrity
     + Availability

Confidentiality means that information transmitted from the sender to the designated receiver is received by this person and not intercepted by any unauthorized third party.

Integrity means that information transmitted from the sender to the receiver is the truthful, correct, and intended message. Such message has not been tampered with, altered, colluded, or inserted with false information.

Availability means that the information from the sender to the receiver is readily available for the intended receiver by correct addressing safely and efficiently.

1. I forhold til informasjonsikkerhet hva står «C.I.A» for?

Confidentiality, Integrity, Availability

1. Forklar begrepene nedenfor (gi gjerne eksempler på begrepene også):
   * + Kryptering
       - Cryptography derives from the Greek alphabet meaning secreted or hidden. There are many ways to make messages secret. And early method Jules Cesar´s shift cipher where letters were transposed. More modern methods use algorithms, hash tables, and other cyphertext methods.
     + Adgangskontroll
       - The use of passwords is securing access for the designed person only. Passwords should contain at least eight characters to make hacking less probable. The formula x = lg2(y)\*n where y signifies the number of characters to choose from (i.e.: the alphabets of 26 characters) and the number of characters in the password (e.g.: 8 characters) describes the bit strength of the password. A bit strength of 80 should be the minimum to attain access security.
     + Autentisering
       - Authentication of the receiver is essential to ensure that the correct person receives information/massage. Methods of authentication can be secured by a two-way process where the receiver must verify his Identity before a massage can be obtained.
     + Authorizing
       - Authorizing is a managerial task to ensure that person of authority gets access according to the level of his authority.
2. Hva betyr Integritet? Hvordan kan man bevare integriteten til noe?

* Integrity means that information transmitted from the sender to the receiver is the truthful, correct, and intended message. Such message has not been tampered with, altered, colluded, or inserted with false information. To maintain integrity, it is important to secure that the lines of communication are safe at all times by having programs that detect infiltration and eavesdropping.

1. Hva betyr Tilgjengelighet?
   * + Accessibility means the availability of information for the designated person.
2. Hva står begrepet «A.A.A» for? forklar kort hva hver enkelt «A» står for.
   * Assurance, Authenticity, Anonymity
     + Assurance means confidentially in the massages received.
     + Authenticity means that’s the message originates from the true sender.
     + Anonymity means that no unauthorized persons are advised of you receiving the message.
3. Er Cæsar Chiper en «sikker» måte å kryptere informasjon på?
   * + No
4. Hva slags kryptografiske funksjoner er: «SHA-1» og «SHA-256» eksempler på?
   * Dette er ikke kryptografiske funksjoner
   * Dette er Hash funksjoner
   * Dette kan man ikke svare på uten å vite hvilken algoritme klokkesyklusen på en datamaskin kjører.
   * SHA-1 and SHA-256 are examples of Hash functions.
5. Hva står «MAC» for?
   * Message Authentication Codes
6. Hva vil et «DOS» angrep bety?
   * Denial-of-service: To interrupt or limit a computer service or destroy the accessibility of such service
7. Nevn de 10 prinsippene for sikker design av datasystemer og en kort beskrivelse av hver av de.

C.I.A

A.A.A

HASING

MAC

SHA

Cryptography

2