1) Hva er informasjonssikkerhet

Informasjonssikkerhet er praksisen om sikring av informasjon og tjenester gjennom prosesser og rutiner.

2) I forhold til informasjonssikkerhet hva står “C.I.A” for?

C = Confidentiality
I = Integrity
A = Availability

3) Forklar begrepene nedenfor (gi gjerne eksempler på begrepene også)

Kryptering: er omgjøring av informasjon via en hemmelig “krypteringsnøkkel” slik at informasjonen kan bare ses av en annen krypteringsnøkkel. F.eks bruk av en symmetrisk nøkkel hvor begge parter har samme nøkkel.

Adgangskontroll: er regler og retningslinjer (policy) som begrenser adgangen til informasjon til de personene/systemene som trenger å vite. F.eks regulerer tilgangen til nettverket via MAC-adresse.

Autentisering: avgjør identiteten eller rollen til noen. F.eks en bilnøkkel eller innloggingspassord.

4) Hva betyr integritet? Hvordan kan man bevare integriteten til noe?

Integritet betyr å informasjonen ikke har blitt endret på en uautorisert måte.
Man kan bevare integriteten til noe ved å bruke backups (periodisk arkivering), sjekksummer (berenger på grunnlag av all informasjon som man kan sjekke at sjekksummen samsvarer med informasjonen).

5) Hva betyr tilgjengelighet?

Tilgjengelighet er at informasjonen er tilgjengelig for og kan bli endret av de som er autorisert til det.

6) Hva står begrepet “A.A.A” for? Forklar kort hva hver enkelt “A” står for.

Begrepet A.A.A står for Assurance, authenticity og anonymity.

Assurance handler om hvordan tillit etableres og administreres. Det blir basert på retningslinjer, tillatelser og beskyttelsesmekanismer.

Authenticity handler om evnen til å slå fast om utsagn, retningslinjer og tillatelser gitt av en person/system er ekte og ikke er forfalsket.

Anonymity handler om transaksjoner eller lagrede data ikke skal kunne føres tilbake til en person/system.

7) Er Cæsar Chiper en “sikker” måte å kryptere informasjon på?

Cæsar Chiper er en enkel måte å sikre informasjon på men er lett å knekke. Det går ut på at hver bokstav erstattes med den tre bortenfor. Ettersom det er en enkel kryptering av informasjonen og kan løses enkelt ved litt kryptoanalyse.

8) 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.

9) Hva står MAC for?

- Message Autorization Certificate
- Message Authentication Codes
- Message Anonymity Controll
- **Ingen av alternativene**

10) Hva vil et «DOS» angrep bety?

Et “DOS” (denial-of-service) angrep er en måte å avbryte en datatjeneste eller ødelegge tilgang til tjenesten.

11) Nevn de 10 prinsippene for sikker design av datasystemer og en kort beskrivelse av hver av de.

De 10 sikkerhets prinsippene er:

- **Economy of mechanism**: Enkel design og implementering av sikkerhetstiltak
- **Fail-safe defaults**: Standard konfigurering skal være konservativt
- **Complete mediation**: All adgang til en ressurs må sjekkes for om det er i tråd med et beskyttelses-skjema
- **Open design**: Arkitektur og design bør være offentlig tilgjengelig
- **Separation of privilege**: Ulike betingelser kreves for å få tilgang til ressurser eller at et program skal utføre en bestemt handling. Systemet bør også være modularisert på en måte at komprimering av en komponent ikke sprer jeg.
- **Least privilege**: Hvert program bør operere med kun det minimum av rettigheter det trenger for å fungere skikkelig
- **Least common mechanism**: I systemer med flere brukere bør det være minst mulig mekanismer som tillater deling av en ressurs mellom flere brukere
- **Psychological acceptability**: Brukergrensesnitt og tilbakemeldinger bør være godt designet og lett å forstå. Alle sikkerhetsinnstillinger bør være i linje med hva en “vanlig bruker” forventer.
- **Work factor**: Når man designer et sikkerhetsskjema skal man sammenligne kostnaden ved å bryte en sikkerhetsmekanisme med de ressursene en forventet angriper vil disponere
- **Compromise recording**: Noen ganger er det bedre å loggføre konsekvensene av et inngrep istedenfor å sette inn mer sofistikerte tiltak for å forhindre det