IN2120 – Informasjonssikkerhet: Workshop uke 3: Nøkkelhåndtering og PKI

**Oppgave 1**

1. Hvorfor er god håndtering av kryptografiske nøkler essensielt for styrken på kryptografi?

* Fordi feil bruk av nøklene kan påvirke sikkerheten til det nøklene er ment å beskytte. Eks. data, passord, osv. Viktig for å forebygge skade som kan oppstå dersom nøklene blir kompromittert.

1. Tre viktige kategorier er: i) symmetriske hemmelige nøkler, II) asymmetriske offentlige nøkler, og III) asymmetriske privatnøkler. Forklar hvilken type sikkerhet tjenester/beskyttelse (dvs. konfidensialitet, integritet og autentisitet) som kreves for hver nøkkelkategori.
2. Symmetriske hemmelige nøkler: konfidensialitet, integritet og autentisitet.
3. Asymmetriske offentlige nøkler: integritet, autentisitet.
4. Asymmetriske private nøkler: konfidensialitet, integritet og autentisitet.
5. Beskriv sikkerhetsmekanismer/metoder som kan brukes til å implementere den nødvendige sikkerhetstjenesten/beskyttelse for nøkler.

* Fysiske beskyttelse av maskinene som genererer nøklene.
* Aldri oppbevar nøklene åpent tilgjengelig, med mindre det er offentlige nøkler.
* Nøkler må bli tilfeldig valgt.
* Hierarki: nøkler beskyttet av en master key, som igjen beskyttes av låser, passord biometrics etc.
* En enkelt nøkkel skal bare brukes til **ett** formål, f.eks. kryptering, autentifikasjon, key wrapping(?), generere tilfeldige nummer, eller digital signatur.
* Korte krypto-perioder (fra begynnelsen av beskyttelsesperioden til slutten av prosesserings-perioden – den tiden en spesifikk nøkkel er autorisert for bruk).

1. Kort liste over de viktigste prosesser/trinn i nøkkelhåndtering (Key Management):

* 1. Størrelsen på nøklene.
* 2. Styrken på de kryptografiske algoritmene/protokollene.
* 3. Beskyttelsen og behandlingen av nøklene:
  + Sikker generering, lagring/oppbevaring, distribuering, ødeleggelse av nøklene.

**Oppgave 2**

1. Forklar diagrammet for nøkkeltilstander og overganger mellom nøkkeltilstander, som illustrert i NIST SP800-57, figur 5, s. 85.
2. Nøkkelen er i en ‘pre-operational’ fase før generering.
3. Nøkler som ikke blir brukt blir ødelagt, ved å flyttes direkte fra ‘pre-operational’ tilstand til ‘destroyed’ fase.
4. Hvis en nøkkel i den pre-operasjonelle fasen blir kompromittert, kan nøkkelen bli ødelagt ved å flytte den direkte til den post-operasjonelle fasen.
5. Etter at metadata er på plass, nøkkelmaterialet er generert, og metadataen er assosiert med nøkkelen under den pre-operasjonelle fasen, er nøkkelen klar til bruk og kan gå over til den operasjonelle fasen til riktig tid.
6. Når en nøkkel i den operasjonelle fasen blir kompromittert, blir den overført til den post-operasjonelle fasen.
7. Når nøkler ikke lenger er i normal bruk, men tilgangen til nøklene må opprettholdes, blir nøklene overført til den post-operasjonelle fasen.
8. Noen applikasjoner krever at tilgangen blir opprettholdt i en viss periode før materialet blir ødelagt. Når det er klart at en nøkkel i den post-operasjonelle fasen ikke lenger trengs, kan den bli overført til ødelagt fase.