11174 Datasikkerhet

Øving 3

1. Er Cæsar-chifferet et eksempel på monoalfabetisk substitusjon? Hvordan knekkes i så fall et Cæsar-chiffer?

2. Hva er hensikten med de to påfølgende "kryssingene" til slutt i Feistel-strukturen? Siden de kansellerer hverandre, hvorfor er de ikke ganske enkelt utelatt?

3. Forklar hva begrepene "diffusion" og "confusion" betyr i forbindelse med design av et blokkchiffer.

4. Hva menes med "key schedule" for et blokkchiffer?

5. I en annonse i PCWorld Norge presenteres et mailkrypteringssystem som bruker DES i ECB modus for å kryptere hvert tegn i en melding. Sjefen din er veldig opptatt av sikkerhet, og ønsker å kjøpe systemet. Hva bør du råde ham til, og hvorfor? I hvilken grad ville bruk av f.eks. Triple-DES representere en forbedring av systemet?

6. I boken beskrives tre forskjellige måter å implementere et flytchiffer ved hjelp av et blokkchiffer. Tegn opp en av dem, og forklar hvordan kryptering og dekryptering foregår.

7. Forklar med egne ord hva som er poenget med ”ciphertext stealing mode” i RC5, og forklar hvordan det virker. Kommenter spesielt bruken av XOR for å gjenvinne den delen av chifferteksten som ”kastes” (Blokken merket ”X” på figur 4.13 i boka).

8. Hva er en S-boks?