Eksamen i 11174 Datasikkerhet

14. mai 2002

Hjelpemidler: Ingen

Eksamen består av fem oppgaver over to sider..

Faglig kontakt under eksamen: Martin Gilje Jaatun, tlf. 900 26 921

OPPGAVE 1 SYMMETRISK KRYPTOGRAFI

a) Tegn en modell for symmetrisk kryptering mellom to parter.
b) Hva er et blokk-chiffer? (kort)
c) Beskriv noen vanlige "byggeklosser" som brukes i moderne blokk-chiffer. (kort)
d) Hva menes med Avalanche-effekt i et blokk-chiffer? (kort)
e) Nevn ett eksempel på hvordan man kan implementere et flyt-chiffer vha. et blokk-chiffer, og forklar hvordan kryptering og dekryptering av 4 etterfølgende blokker foregår.
f) Hvordan kan de to partene i a) løse nøkkelfordelingsproblemet?

OPPGAVE 2 ASYMMETRISK KRYPTOGRAFI

a) Er det mulig å bruke Diffie-Hellman-algoritmen til å kryptere en tilfeldig valgt sesjonsnøkkel? Begrunn svaret kort.
b) Hvis hvordan Diffie-Hellman kan utsettes for et "Man-in-the-middle"-angrep.
c) Hva kan man gjøre for å forhindre angrepet i b) ? (kort)

OPPGAVE 3 DIGITALE SIGNATURER

a) Hva er forskjellen mellom en MAC og en digital signatur?
b) Hvilke komponenter inngår i et digitalt signatursystem?
c) To av de mest brukte algoritmene for digitale signaturer er RSA og DSA. Beskriv virkemåten for en av dem.
d) Hva er det matematiske fundamentet for at protokollen du beskrev i c) er sikker? (kort)
e) Forklar hva et "sertifikat" er, og hva det kan brukes til. (kort)
f) Beskriv en *metode* for distribusjon av offentlige nøkler.
g) Hvordan håndterer metoden du beskrev i f) tiltro ("trust")?

OPPGAVE 4 AUTENTISERINGSPROTOKOLLER

a) Hva er en autentiseringsprotokoll?
b) Følgende autentiseringsprotokoll burde være kjent:
   1. $A \rightarrow KDC: ID_A \,||\, ID_B \,||\, N_1$
   2. $KDC \rightarrow A: E_{Ka}[K_s \,||\, ID_B \,||\, N_1 \,||\, E_{Kb}[K_S \,||\, ID_A]]$
   3. $A \rightarrow B: E_{Kb}[K_S \,||\, ID_A]$
   4. $B \rightarrow A: E_{Ks}[N_2]$
   5. $A \rightarrow B: E_{Ks}[f(N_2)]$

   Forklar hva som skjer i denne protokollen, og beskriv sikkerhetsproblemet/svakheten den lider av.
c) Skisser aktørene i Kerberos-protokollen, og beskriv hvordan en bruker på en klient autentiserer seg ovenfor en server som tilbyr en tjeneste.

d) Hvordan takler Kerberos problemet til protokollen i b)? (kort)

OPPGAVE 5 BRANNMURER OG IDS

a) Hva er en brannmur?
b) Hva er NAT? (kort)
c) Hvilke to teknikker (utenom NAT) utgjør basisfunksjonaliteten i de fleste brannmurer (dvs. minst en av disse teknikkene er i bruk i de fleste brannmurer)? Diskutér forskjeller mellom disse teknikkene.
d) Hvilke to hovedtyper av NIDS (Network Intrusion Detection System) finnes? Diskutér forskjeller mellom dem.