NA Kapitel 6

Arne Mejlholm

15th June 2004

1 Sikker kommmunikation

Dette er et bredt begreb, derfor introducerer vi nogle keywords:

- **Fortrolighed:** A og B ønsker at tale i fred(måske endda uden at andre er klar over at de taler). Ofte forståes dette ord som at andre ikke forstår hvad A og B siger, men dette er en indskrænkelse.
- **Authentication:** A vil være sikker på han rent faktisk snakker med B.
- **Integritet:** A vil være sikker på at en besked kommer fra B og ikke er ændret siden afsendelse.
- **Tilgængelighed og Access control:** Når B har en server og kun vil have at han og A har adgang.

1.1 Symmertiske nøgler

Ideen er at der findes en krypterings algoritme K_a og en dekrypterings algorithme K_b således at en besked m kan krypteres $K_a(m)$ og dekrypteres $K_b(K_a(m))$. Ved symmetriske nøgler bruges den samme nøgle i både algoritme K_a og K_b. Kendte algoritmer er Cæsars ciffer algoritme og DES/3DES.

1.2 Asymmetiske nøgler(public key)

I modsætning til symmetriske nøgler, er det her to forskellige nøgler. En person har en offentlig nøgle, K_a^+ og en private nøgle K_a^-. For at B kan sende en privat besked til A, skal B hente A's offentlige nøgle og kryptere sin besked m med denne, $K_a^+(m)$, og sende den til A. A kan så dekryptere beskede med sin private nøgle, som kun han kender, $K_a^-(K_a^+(m))$. Dette virker fordi der findes algoritmer der laver to nøgler således at $K_a^-(K_a^+(m)) = m$ men også $K_a^+(K_a^-(m)) =$ m. Ved denne teknik er der altså to svagheder: valg af keys og valg krypterings algoritme.

Valg af nøgler: Der vælges to store primtal, jo større jo bedre sikkerhed og længere tid til at kryptere/dekryptere. Ud fra disse laves der de operationer som står på side 617 resulterende i en offentlig og hemmelig nøgle.

RSA kryptering med udvælgelse af store primtal er desværre en tidskrævende operation, den bruges ofte i forbindelse med DES/AES. Man bruger en nøgle k til at kryptere sin besked m med DES/AES. Denne nøgle krypteres derefter med modtagerens offentlige nøgle, således at kun han kan pakke beskeden ud igen.

2 Authentificering

Der er adskillige faktorer der gøre det svært at sikre en persons identitet på et netværk.

En løsning på dette kan være den følgende protokol, der bruger public key princippet fra før:

1. "Jeg er Alice", sender Alice til Bob
2. Bob vælger en onetime key, og sender den til Alice
3. Alice bruger hendes private key til kryptere onetime key'en. Den krypterede besked der kommer ud af dette, kan kun Alice lave.
4. Bob bruger Alice's offentlige nøgle til at pakke onetime key'en ud og verificere at det er den samme som den han sendte.

Denne protokol vil virke, dog kun med den forudsætning at den offentlige nøgle er autentisk. Hermed bliver obvaring af offentlige nøgler essentiel.