Matemaatikko kryptografina

Kaisa Nyberg
professori, Aalto-yliopisto

Opiskelin Helsingin yliopistossa matematiikkaa ja tilastotiedettä. Väittelin funktionaalianalyysin alalta ja olen sen jälkeen työskennellyt yliopiston lisäksi puolustusvoimissa, Nokialla, TKK:lla ja Aalto-yliopistossa, sekä lyhyempiä jaksoja ulkomailla, Wienin ja Karlsruhen teknillisissä yliopistoissa.

Opinnoistani olen voinut hyödyntää suoraan tilastotiedettä ja todennäköisyyslaskentaa sekä lineaarialgebraa. Algebraa ja diskreettiä matematiikkaa, sekä tietojenkäsittelytiedettä ja algoritmiikkaa opiskelen jatkuvasti edelleenkin tutkimustyön mukana. Matemaattisen koulutuksen suurin anti on minulle ollut sen suomat metodologiset valmiudet. Niiden pohjalta olen voinut paikata vastaantulevia aukkoja, joita on ollut useita pitkin matkaa. Tuskinpa niitä kaikkia olisi voinut opiskella etukäteen. Siinä olisi jäänyt jotain puuttumaan joka tapauksessa.

Viimeisessä työssäni TKK:n (nyt Aalto-yliopiston) professorina olen ollut kymmenen vuotta. Sitä ennen ja vielä pitkään sen ohella toimin Nokian Tutkimuskeskuksessa vastuualueenani matkapuhelinverkkojen tietoturvallisuuden kryptologiset menetelmät. Lähimmät työtoverini olivat matemaatikkoja ja matemaattisesti suuntautuneita tietoliikenneinsinöörejä. Kryptologian alalla voi toimia usealta eri koulutuspohjalta ja suuntautua eri tavoin. Mutta minun mielestäni matemaatikot puuhailevat yleensä hauskimpien ja mielenkiintoisimpien kysymysten parissa.

Työelämässä olen tarvinnut monenlaisia lisätaitoja esitystekniikasta ja käytännön projektien hallinnasta alkaen. Niitä olen opetellut työtehtävien mukana ja niihin on tarjolla myös tehokasta kurssimuotoista koulutusta. Mutta matematiikan ja fysiikan merkitys ei siitä vähene, se pysyy nykymaailmassa ja tulevaisuudessa suurena, kasvavana ja kiistämättömänä.

Matkustan työssäni paljon, lähes kuukausittain. Ohjaan diplomityöntekijöitä ja tohtorikoulutettavia ja osallistun kansainväliseen tieteelliseen toimintaan. Aikaisemmin Nokian tutkimuskeskuksessa luin ja kirjoitin määrittelyjä, standardeja ja keksinnöistäni patentteja. Nykyään professorina kirjalliset työni keskittyvät tieteellisiin artikkeleihin ja opinnäytteisiin. Tutkimusteni kohteena on salausmenetelmien matemaattiset ominaisuudet ja tilastolliset analyysimenetelmät. Joskus minua pyydetään asiantuntijaksi, kun suunnitellaan tietoturvallisuuden suhteen kriittisiä järjestelmiä kuten esimerkiksi kansalaisten nettiäänestystä. Unelmatyöni on aika lailla nykyisen työn kaltainen.