UVOD

Leta 1976 sta matematika Whitfield Diffie in Martin E. Hellman v reviji *IEEE Transactions on Information Theory* objavila desetstranski članek z naslovom »New Directions In Cryptography«. V članku sta opisala protokol za varno izmenjavo šifrirnih ključev prek nezaščitenega medija in rodila se je zamisel o sistemu šifriranja z javnimi ključi.

Leto pozneje, neke aprilske noči, se je Ronald L. Rivest med hudim glavobolom (Dupuis 1999) domislil novega šifrirnega algoritma, ki bi temeljil na sistemu javnih ključev, omogočal pa bi tudi digitalno podpisovanje. Algoritem si je zapisal in ga zjutraj poslal kolegoma Adiju Shamirju in Leonardu M. Adlemanu. Vsi trije avtorji, ki so bili tedaj popolni novinci v kriptografiji, so opisali problem v znanstvenem članku, ki so ga poslali reviji *Scientific American*. Članek je bil objavljen septembra 1977, avtorji pa so v njem zapisali, da bodo tehnične podrobnosti algoritma brezplačno poslali vsakomur, ki jim bo poslal kuverto z znamko. Prejeli so na tisoče zahtevkov z vsega sveta, in leto zatem so v reviji *Communications of the ACM* objavili šeststranski članek z naslovom »A Method for Obtaining Digital Signatures and Public-Key Cryptosystems«. V članku je bil opisan celotni algoritem, ki so ga po začetnicah avtorjev poimenovali RSA (RSA Laboratories 2000, 12). Izkazalo se je, da je algoritem RSA kriptografsko izjemno močan, kar pomeni, da je sporočila, zašifrirana z njim, izjemno težko zlomiti.

Minilo je štirinajst let in leta 1991 je računalniški programer Philip R. Zimmerman napisal računalniški program PGP (*Pretty Good Privacy*), namenjen šifriranju elektronskih sporočil in računalniških datotek. PGP je za šifriranje uporabljal algoritem RSA. Program je tekel na popolnoma običajnih računalnikih PC in je bil za tedanje standarde uporabniške prijaznosti razmeroma preprost, predvsem pa zelo učinkovit. Ker je tega leta ameriški senat obravnaval zakon,

ki bi močno omejil uporabo kriptografije v civilne namene, je Zimmerman – da bi izničil učinke tega zakona, če bi bil sprejet – program javno objavil na internetu in dovolil njegovo brezplačno kopiranje. V razmeroma kratkem času se je program razširil po vsem svetu.

Tako so se v petnajstih letih zgodili trije na videz nepomembni dogodki, ki bi praviloma morali zanimati le peščico matematikov in računalničarjev. Ampak obrnilo se je drugače. Na videz drobno matematično odkritje je v resnici imelo veliko večji pomen, kakor bi si konec 70. let kdo lahko mislil. Kajti po odkritju, predvsem pa računalniški implementaciji algoritma RSA, so se v ZDA aktivirali pravosodni sistem in tudi tajne službe. In potem ni bilo nič več tako kot prej.