Diffie ja Hellmani avaliku võtme krüptosüsteemidest

Kalev Pihl, Andi Kivinukk
SK ID Solutions, Tallinna Ülikool

1 Eesti Vabariigi 2019. a teenetemärgi said krüptograafid Diffie ja Hellman

Mille eest antakse Eesti Vabariigis nimetatud USA teadlastele autasu? 6. novembril 1976. aastal, mis on vähem kui pool aastat pärast selle kirjutise esimese autori sündi, avaldasid Whitfield Diffie ja Martin Hellman artikli *New Directions in Cryptography*, IEEE Transaction on Information Theory, Vol. IT-22, Nov. 1976, pp. 644-654 (Invited Paper). 29. jaanuaril 2019. aastal teatab Vabariigi Presidendi Kantselei, et Whitfield Diffie ja Martin Edward Hellman saavad tunnustatud Maarjamaa Risti III klassi teenetemärgiga. Teenetemärgi annetamise alusena on kirjas: "Leiutanud koos ... Avaliku Võtme Krüpteerimise (Public Key Encryption), mis on meie X-tee/ID kaardi ja ülejäänud maailma kaasaegse krüpteerimise aluseks." Nii Diffie kui ka Hellman on öelnud, et lisaks neile oleks nendega koos alati vaja tunnustada ka Ralph Merkle'i (s 1952, IEEE Richard W. Hamming Medal 2010. a) tööd, kes oli juba 1974. aastal üliõpilastööna kirjutanud oma „Merkle's puzzles", mille omadused sarnanevad vägagi hilisemale avaliku võtme krüptograafiale, ent ta kasutas selle loomisel siiski ainult sümmeetrilist krüptograafiat.

Käesolev artikkel proovib selgitada kahe mehe tähendust krüptograafias ning kas ja kui palju on nende kanda ID-kaardi või ka X-tee realisatsioonide krüpteerimine. ID-kaart ehk isikutunnistus on Eesti kodaniku ja Eestis püsivalt elava Euroopa Liidu kodaniku kohustuslik isikut tõendav dokument, mis on osa Eesti Vabariigi elektrooniliste isikutunnistuste süsteemist, kuhu kuuluvad lisaks ID-kaardile veel ka Mobiil-ID ja digi-ID. X-tee on tehniline ja organisatsiooniline keskkond, mis võimaldab turvalist ja tõestusväärtust tagavat internetipõhist andmevahetust

riigiasutuste vahel ja erasektoriga. Lugeja võib aru saada, kui tähtis on mõlema süsteemi turvalisus. Käesoleva artikli autoritel pole õnnestunud teada saada, kas Diffie ja Helman on teinud midagi konreetset Eesti heaks, et neile oleks pidanud ülalnimetatud autasud andma. Kaldume arvama, et pigem oli see presidendi poliitiline žest USA suunal. Igal juhul ei Diffie ega ka Hellmani Wikipedia inglisekeelsetes artiklites (seisuga 19.02.2021) ei leidu nende arvukate autasude hulgas viidet EV presidendi annetatud teenetemärkidele.

Bailey Whitfield Diffie sündis 5. juunil 1944. a. USA pealinnas Washingtonis ja kasvas üles New Yorgis. 1965 aastal kaitses ta MIT's B.S. kraadi matemaatikas. Ta läks 1965. aastal tööle MITRE Corporationisse, mis pakkus kindlasti head erialast väljakutset, kuid tol ajal kaitseministeeriumile tehtavate tööde tõttu lubas tal kui veendunud patsifistil ka vältida Vietnami sõtta värbamist. Samal ajal võttis ta osa ka uurijana MIT tehisintellekti laboratooriumis, kus ta väidetavalt ajaliselt isegi rohkem viibis kui MITRE's. Tehisintellektist saadud suhete kaudu kutsus selle valdkonna üks alustalasid John McCarthy (1927-2011) Diffie Stanfordi tehisintellekti laborisse (SAIL – Stanford Artificial Intelligence Laboratory). McCarthy juures töötades puutus Diffie kokku arvutivõrkude, võtmehalduse ning elektroonilise tuvastuse problemaatikaga. Pärast David Kahni „The Codebreakers: The Story of Secret Writing" lugemist tekkis temas sügavam huvi krüptograafia ja privaatsuse vastu. Kahni raamat on krüptograafia ajaloost, alustades Vana-Egiptusega. Tolleaegne tugevaim teaduspotentsiaal selles vallas oli IBM laboritel. Diffie pöördus IBM'i poole 1974. aastal, et rääkida nende edusammudest ning enda ideedest sellel suunal. Suur osa IBM'i tööst oli rangelt salastatud, kuid Diffie arutelud avaldasid siiski teatud muljet ning talle anti soovitus pöörduda Stanfordi teadlase Martin Hellmani poole, kes saab rohkem rääkida ja kellel olevat sarnased mõtted. Kohtumine toimus ning sellest kasvas välja pikem koostöö kahe mehe vahel. Hellman kutsus Diffie enda juurde Stanfordi doktoriõppesse, kuhu 1975. aastal Diffie astuski, kuid ei lõpetanud seda kunagi –

Martin Hellman on öelnud, et „'Whit' ei saa kellegi õpilane olla", millega Diffie ka nõus on olnud. 1975. aastal tutvusid nii Diffie kui Hellman ka Ralph Merkle'i töödega, mis lõpuks inspireerisid ka Diffie-Hellmani avaliku võtme krüptograafia väljatöötamist. 1977. aastal Diffie, Hellman ja Merkle esitasid patenditaotluse „avaliku võtmega krüptograafia" peale, mille nad 1980. aastal ka said. Aastail 1978 - 1991 töötas Diffie „Northen Telecom'is" turvaliste süsteemide uurimisgrupi juhina. Alates 1991 kuni 2009 töötas Sun Microsystems'is, oli seal lõpuks nii turvajuht kui ka asepresident.

Martin Edward Hellman sündis 2. oktoobril 1945. aastal New Yorgis ja kasvas ka New Yorgis üles. Ta lõpetas 1966. aastal New Yorgi Ülikooli elektrotehnika erialal. Oma magistri- ja doktorikraadi kaitses Hellman Stanfordi Ülikoolis samuti elektrotehnikas vastavalt aastatel 1967 ja 1969. 1968. aastal töötas Hellman lühikest aega IBM'i Thomas J Watsoni uurimiskeskuses. 1969. aastal lahkus ta IBM'ist ning asus õpetama MIT's, kust ta 1971. aastal tuli tagasi Stanfordi Ülikooli elektrotehnikat õpetama. Tema kasvav huvi krüptograafia vastu ei leidnud kolleegide toetust ning ka IBM'is oli krüptograafia-alane uurimistöö 70ndate keskpaigaks justkui läbi saanud seoses Luciferi nimelise algoritmi valmimisega. Selle tõttu oli tema ja Diffie kohtumine 1974. aastal tõeline valguskiir pimeduses ja nende esimene kohtumine venis planeeritud poolest tunnist poolepäevaseks. Hellman kutsus Diffie 1975. aastal enda juurde doktoriõppesse, mille käigus nad alustasid oma sisulist koostööd krüptograafias. 1976. aastal kutsus Hellman enda juurde doktoritööd kirjutama ka Ralph Merkle'i. Merkle kaitseski doktorikraadi Stanfordis 1979. a. Martin Hellman oli 1970ndatel ja 1980ndatel üks olulisemaid teadlasi, kes võitles krüptograafide õiguste eest avaldada oma töid ning avalikkuse õiguse eest omada tugevat krüptograafilist kaitset, mis kaitseb ka riiklikult rahastatud ründaja eest. Hellman on avaldanud üle 70 teadusartikli ja omab 12 patenti.

2 Avaliku võtme krüptograafia loomine

W. Diffie ja M. Hellmani kohtumine 1974. a toimus ajal, kui esimene töötas SAIL'is ja teine oli tagasi Stanfordi Ülikoolis. Diffie proovis teada saada, mida IBM on välja mõelnud krüpteerimise vallas. Selmet talle selget vastust anda, suunas labori juhataja Alan Konheim (1934–2019, elektrotehnika- ja matemaatikaharidusega USA krüptograaf) ta Hellmaniga kohtuma ning ülejäänu on ajalugu, nagu öeldakse.

1970ndad aastad olid endiselt varjutatud külma sõja ohuga ning USA sõjaväe ning tsiviilkasutuses olevad krüpteerimise võimalused olid ühtlustamata ja seda isegi üsna sihipäraselt. Krüpteerimise olulisemaks väljakutseks oli kõneside krüpteerimine, ning mitte üksiku sõnumi, vaid kestva sessiooni salastamine. 1975. aastal toimus selles kõiges suur hüpe, kui Ameerika Ühendriikide standardite instituut ANSI kuulutas välja esimese avaliku krüpteerimisstandardi DES ehk Data Encryption Standard, mille väljatöötaja oli IBM ja mis baseerus krüpteerimissüsteemil Lucifer (vt nt https://derekbruff.org/blogs/fywscrypto/tag/lucifer/). Diffie ja Hellman olid avalikult selle standardiseerimise vastu, kuivõrd pidasid 56 bitist võtit selgelt liialt nõrgaks. Luciferi originaalne võtme pikkus oli 128 bitti. Standardiks see siiski sai, kuid selle võtmepikkus sai ikkagi sajandi vahetuseks saatuslikuks.

Nagu eelpool öeldud, siis ei olnud peale ANSI konkursi võitja väljakuulutamist paljude arvates krüptograafia kui uurimisvaldkond enam oluline. Töö oli justkui tehtud ja seetõttu kadus rahastus IBMis selle valdkonna tagant ning Martin Hellman ei leidnud toetust ka Stanfordis. Diffie ja Hellman nägid aga suurt hulka lahendamata probleeme ja lisaks muidugi polnud nad rahul DES turvalisusega. Nende IEEE Transaction on Information Theory artikkel lahendas ülesannet senisest absoluutselt teistmoodi. See pani aluse krüptograafia jõudmisele igapäevasesse kasutusse ja loomulikult on see inspireerinud suurel hulgal täiendavaid algoritmide uurimisi.

Kontekst, milles Diffie ja Hellmani töö toimus, on samuti oluline.

Juba 1969. aastast loetakse Interneti ajalugu, sest siis käivitus ARPANET: USA kaitseministeeriumi koostööpartnerite vaheline arvutivõrk, mis 1970. aastate jooksul kasvas jõudsalt ning millest sai ka esimene laiatarbeline pakettkommuteerimisel (saadetav info jagatakse pakettidesse, mis edastatakse sõltumatult) põhinev süsteem. ARPANETi juures toimetavad töögrupid defineerisid ka nn TCP/IP andmevahetusprotokollide komplekti, millega tagatakse võrgu toimimine. Arvutite levik suurettevõtetest kodudesse oli samuti alanud – 1975. a alustas tegevust Microsoft ning 1976. a Apple, kui termin PC oli veel sündimata. Kokkuvõtvalt aga võib öelda, et arvutivõrkude turvalisus ei olnud veel 1970ndate keskel tegelikult aktuaalne teema. Kuid telefonivõrgud olid 1970. aastate alguses täiesti olemas ning *phone phreaking* (telefoni keskjaamade ründed läbi helisignaalide) olid mõne aasta jooksul saanud kõvasti tähelepanu ning selle võrgu turvalisus oli päevakorral. Seega võrgu otspunktide turvamise probleem oli laialdaselt tuntud just telefonide najal ja lahendust selleks ei paistnud esialgu olevat. Selleks, et n osalejaga võrgus saaks lubada privaatset krüpteeritud sõnumivahetust, oli tolleaegsete meetoditega vaja $(n^2-n)/2$ võtme genereerimist ja edastamist vaadeldavast võrgust väljaspool – kas „tigupostiga“ või päriselt kokku saades. Selline mudel muidugi ei sobi telefoniga helistamisel privaatsuse tagamiseks – võtmeid ei saa ei ette genereerida (kuna võrgus osalejate arv kasvab pidevalt) ega ka vajaduse ilmnedes mõistliku aja jooksul tekitada. Seega ilma avaliku võtme krüptograafiata oleks üsna võimatu ette kujutada tänast internetti tervikuna - mitte ainult Eesti X-teed või ID kaarti.

3 Avaliku võtme krüptograafia matemaatikast

Oma artikli III peatükis „Public Key Cryptography“ defineerisid Diffie ja Hellman avaliku võtme krüptosüsteemi algoritmid perede paarina $\{E_K\}_{K\in\{K\}}$ ja $\{D_K\}_{K\in\{K\}}$, mis kujutavad pööratavaid teisendusi

$$E_K : \{M\} \to \{M\},$$

$$D_K : \{M\} \to \{M\}$$

lõplikus sõnumiruumis $\{M\}$.

Tähistuste E, D, K, M selgitus tuleneb vastavatest inglisekeelsetest sõnadest: E on krüpteerimisalgoritm, lüh „Encrypt“, D on dekrüpteerimisalgoritm, lüh „Decrypt“, K on võti, Key, $\{M\}$ on sõnumiruum, „Message“.

Algoritmidelt nõutavad omadused on:

1. Iga $K \in \{K\}$ korral teisendus D_K on E_K pöördteisendus.

2. Iga $K \in \{K\}$ korral algoritmid $E_K\{M\}$ ja $D_K\{M\}$ on lihtsalt arvutatavad.

3. Peaaegu iga võtme K korral on arvutuslikult keeruline tuletada algoritmist E_K algoritm D_K (või mõni viimasega samaväärne algoritm).

4. Iga $K \in \{K\}$ korral on mõistliku pingutusega leitavad teineteise pöördteisendused D_K ja E_K lähtudes ainuüksi võtmest K.

Esimesed kaks omadust on üsna ootuspärased kõigile krüptosüsteemidele. Kolmanda omaduse tõttu on aga võimalik E_K avalikuks tegemine, ilma et dekrüpteerimise võimekus oleks avaldatud. Neljanda omaduse tõttu on olemas piisavalt ja mõistlikult arvutatavaid võtmepaare, et süsteem saaks toimida vaid juhuarvude generaatori olemasolul.

Sellise krüptosüsteemi korral on senisega võrreldes võtme jagamine oluliselt lihtsustatud. Iga kasutaja genereerib võtmed E ja D enda kontrollitavas keskkonnas. Võtit E on siis võimalik levitada avalikus kanalis, mida tuleb kaitsta vaid volitamata muutmise eest, ning võti D ei pea kunagi lahkuma kasutaja kontrollitavast keskkonnast.

W. Diffie ja M. Hellman pakuvad välja ka esimese algoritmi, mis sobiks ülalkirjeldatuga. Nad võtavad aluseks arvutuslikult keeruka logaritmi leidmise lõplikus (või teise nimega Galois') korpuses $GF(q)$, kus q on algarv. (Kõige lihtsam Galois' korpus on $GF(2)$, milles on kaks elementi 0 ja 1, liitmine selles korpuses toimub nagu loogikas disjunktsioon ja korrutamine nagu loogikas konjunktsioon) Korpuse $GF(q)$ elemente tähistatakse arvudega $0, 1, \ldots, q-1$ ja võrdus $a = b$ korpuses $GF(q)$

on samaväärne võrdusega $a = b \ mod \ q$. Korpuse $GF(q)$ mittenullelemendid moodustavad tsüklilise multiplikatiivse rühma, seega leidub element, nimetatakse primitiiviks, mille astmete abil saab esitada korpuse kõik mittenullelemendid.

Diffie – Hellmani idee seisab järgnevas arutelus. Olgu

$$Y = \alpha^X \ mod \ q, \ 1 \leq X \leq q,$$

kus α on fikseeritud primitiiv korpusest $GF(q)$. Siis logaritm määratakse võrdusega

$$X = \log_\alpha Y \ mod \ q, \ 1 \leq Y \leq q.$$

Y arvutamine X abil on lihtne, kuid X arvutamine Y abil on oluliselt keerukam. Et ülaltoodud Diffie-Hellmani ideedest paremini aru saada, lisame siia õppekirjanduse abil kompileeritud arvulise näite.

Näide 1.6.1. *Olgu meil* $GF(29)$, *st* $q = 29$. *Arvutused näitavad, et korpuse* $GF(29)$ *üheks primitiiviks on* $\alpha = 2$, *me selgitame seda allpool. Nii öelda lihtsa algoritmi rakendusena võtame näiteks* $X = 5$ *ja arvutame* $Y = 2^5 \ mod \ 29$. *See nõuab kolme korrutamist, sest* $2^5 \ mod \ 29 = (2^2)^2 \times 2 \ mod \ 29 = 3$. *Diffie ja Hellman viitavad D. Knuthi raamatu "Programmeerimise kunst" 2. köitele, et maksimaalselt on vaja* $2 \times \log_2 q$ *korrutamist; meie juhul siis* $2 \times \log_2 29 = 2 \times 4.857... = 9.715...$, *seega kindlasti mitte üle 10 korrutamise suvalise* X *jaoks.*

Võtame nüüd $Y = 5$ *ja leiame logaritmi, st katsume leiutada arvu* X, *et* $5 = 2^X \ mod \ 29$. *Kuna korpuse* $GF(29)$ *üheks primitiiviks on oletatavasti* $\alpha = 2$, *siis antud* $Y = 5$ *sisaldub hulgas*

$$\{2^1 \ mod \ 29, \ 2^2 \ mod \ 29, \ ..., 2^{22} \ mod \ 29, \ ..., 2^{28} \ mod \ 29\}.$$

Selle hulga konstrueerimine on n-ö logaritmi tabeli koostamine, muu hulgas, kuna konstrueeritud hulk ühtib hulgaga $\{1, 2, ..., 28\}$, *siis sellega on näidatud ka, et* $\alpha = 2$ *on korpuse* $GF(29)$ *multiplikatiivse rühma primitiiv. Antud juhul konstrueeritud hulga*

element 2^{22} *mod* $29 = 5$ *määrab etteantud arvu* $Y = 5$. *Selle elemendini jõudmiseks on vaja teha 21 sammu (esimene samm on triviaalne), kus i-ndal sammul vajalik korrutamiste arv on ligikaudu* $2 \times \log_2 i$. *Seega kokku on korrutamisi ligikaudu* $2 \times \sum_{i=2}^{22} \log_2 i = 2 \times \log_2 22! \approx 140$. *Näeme tõesti, et logaritmi leidmine on astendamisest oluliselt keerulisem.*

Diffie-Hellmani artikkel esitas seega idee ühesuunalistest funktsioonidest, see nimetus on samuti nende artiklis olemas. Artikli ilmumine käivitas loomulikult ka selleteemalise suurema uurimise ja eriti fookusega tagauksega ühesuunalistel funktsioonidel.

Definitsioon 1.6.1. Ühesuunaline funktsioon *f on funktsioon hulgast X hulka Y, kui $f(x)$ on kergelt arvutatav iga $x \in X$ korral, kuid "peaaegu iga" $y \in Y$ korral on "arvutuslikult ebamõistlik" leida sellist $x \in X$, et $f(x) = y$.*

Definitsioon 1.6.2. Ühesuunaline tagauksega funktsioon *f on funktsioon hulgast X hulka Y, mille korral spetsiifilise teadmise T omamine, mida kutsutakse tagaukseks, võimaldab funktsiooni kergesti pöörata, st et iga $y \in Y$ jaoks on kergelt leitav $x \in X$, et $f(x) = y$. Kõigile, kellele T ei ole teada, on f ühesuunaline.*

4 Diffie-Hellmani võtmekehtestus ja digiallkiri

Vaatame nüüd, millise võimaluse pakkusid Diffie ja Hellman sõnumite krüpteerimiseks ühesuunaliste funktsioonide abil.

Kui q on teada, siis kasutaja i genereerib juhusliku X_i hulgast $\{1, 2, \ldots, q-1\}$ ja hoiab seda saladuses. Samas avaldab koos oma nime ja aadressiga suuruse

$$Y_i = \alpha^{X_i} \ mod \ q, \ 1 \leq X_i \leq q.$$

Kui avalik nimekiri inimestest ja nende võtmetest on olemas, siis kasutajad i ja j saavad kokku leppida avalikus kanalis suhtlemiseks omavahelise saladuse K_{ij} kujul

$$K_{ij} = \alpha^{X_i X_j} \ mod \ q.$$

Kasutaja i saab K_{ij} arvutada järgmiselt:

$$K_{ij} = {Y_j}^{X_i} \ mod\ q = (\alpha^{X_j})^{X_i} \ mod\ q = \alpha^{X_j X_i} \ mod\ q = \alpha^{X_i X_j} \ mod\ q.$$

Analoogiliselt kasutaja j saab arvutada K_{ij} kasutades selleks väärtust Y_i, mille ta leiab avalikust nimekirjast, ja väärtust X_j, mis on ainult tema valduses. Samas ei ole K_{ij} arvutatav mõistliku ajaga kasutades ainult väärtusi Y_i ja Y_j.

Seda nimetatakse Diffie-Hellmani võtmekehtestuseks ning see on kasutusel tänaseni.

Artikli IV peatükis „One-way authentication“ on Diffie ja Hellman esitanud ka sisuliselt elektroonilise allkirjastamise skeemi eelmises peatükis esitatud avaliku võtme krüptograafia abil. Nimelt saab kasutaja A „dekrüpteerida“ sõnumi M oma dekrüpteerimisvõtmega ja saata kasutajale B sõnumi $D_A(M)$. Kasutaja B saab omakorda „krüpteerida“ saadud sõnumi omades kasutaja A avalikku võtit E_A ning seetõttu lugeda sõnumit M, kuna $E_A(D_A(M)) = (E_A D_A)(M) = M$. Selle juures on kasutaja B kindel, et kasutaja A just selle sõnumi saatis nii allika kui ka sisu mõttes.

5 Diffie-Hellmani skeemi realiseerimisest

Hämmastava kiirusega pärast Diffie-Hellmani artikli ilmumist, juba 1977. aastal, valmis algoritm, mis vastas Diffie ja Hellmani poolt esitatud ootustele ning on kasutuses kuni tänase päevani. Ron Rivest, Adi Shamir ja Leonard Adleman Massachusettsi Tehnoloogiainstituudist võtsid alusprobleemiks faktoriseerimise ning lõid RSA (lühend perenimedest Rivest, Shamir ja Adleman) krüptosüsteemi. Selleni jõudmine on kindlasti omaette lugu, me tutvustame ainult algoritmi olulisemaid osi vastavalt Diffie-Hellmani artiklile.

Võtmeruum K koosneb kolmikutest (e, d, n), kus $n = p \times q$, ning p ja q on algarvud, kusjuures n pikkus bittides vastab RSA süsteemi võtme pikkusele. Väärtus d on vabalt valitud suur juhuarv vahemikust $(1, t)$, st $1 < d < t$, kus on $t = (p-1)(q-1)$. Mõelge analoogiale meie kirjutise alguses, et kui kasutuses on korpus $GF(q)$,

kus q on algarv, siis sõnumi väärtused peavad olema vahemikus $(1, q-1)$. Siin aga $n = p \times q$, kus p ja q on algarvud, seega võiks loogiline olla, et $1 < d < (p-1)(q-1)$. Täiendavalt peab d vastama tingimusele, et d ja t suurim ühistegur *modulo* t on 1. Suurus e on sobivalt valitud arv nii, et $d \times e = 1 \; mod \; t$.

Krüptosüsteemi osadeks on

$$E_K : C = M^e \; mod \; n,$$

$$D_K : C^d = M \; mod \; n.$$

Soovitud neli omadust meie kirjutise alguses on kõik täidetud:

1. Kuivõrd meie valitud e ja d on sobivalt valitud, siis

$$\begin{aligned} D_K(E_K(M)) &= (M^e)^d \; mod \; n = M^{e \times d} \; mod \; n = M^{d \times e} \; mod \; n \\ &= (M^d)^e \; mod \; n = E_K(D_K(M)) = M. \end{aligned}$$

2. Iga K ja M korral on E_K ja D_K arvutatavad korrutamise abil, st lihtsalt arvutatavad.

3. E_K kaudu on teada e ja n ning D_K arvutamiseks on vajalik d teadmine. Selleks kõige otsesem tee oleks n tegurite leidmine ja selle kaudu t arvutamine ning siis juba teades e väärtust sobiva d leidmine. Faktoriseerimine (siin on $n = p \times q$, kus praktikas võetakse algarvud p ja q ülisuured) on aga praeguse ajani arvutuslikult keeruline. Aastate jooksul ei ole dekrüpteerimise algoritmiga D_K samaväärset, aga lihtsamini arvutatavat alternatiivset funktsiooni leitud.

4. Kuna me lugesime võtmeks K kolmikuid (e, d, n), siis on nii E_K kui ka D_K leidmine lihtne. Samas keerukus ongi kolmikute koostamine. Kolmikute jaoks esitatavad tingimustest ei ole triviaalsed sobiva pikkusega algarvude p ja q leidmine, suurima ühisteguri leidmine ning e leidmine, kuid need on siiski teostatavad mõistliku pingutusega.

Praegusel ajal defineeritakse avaliku võtme krüptosüsteem formaalselt järgmisel viisil.

Definitsioon 1.6.3. Avaliku võtme krüptosüsteem *on krüpteerimisteisenduste hulk* $\{E_e : e \in K\}$ *ja dekrüpteerimisteisenduste*

hulk $\{D_d : d \in K\}$. *Iga* $e \in K$ *jaoks eksisteerib* $d \in K$ *nii, et* $D_d(E_e(M)) = M$ *iga* M *korral. Kui paar* (e, d) *on valitud, siis võti* e *on avalik ja sellega seotud võti* d *on salajane.*

Selleks, et süsteem oleks turvaline, peab olema ebamõistlikult keeruline arvutada suurust d või ka pöördteisendust E_e^{-1} teades avaliku võtme e väärtust. Avaliku võtme krüptosüsteem on konstrueeritud tagauksega ühesuunaliste funktsioonide hulga $\{f_i\}$ abil. Praktikas kõige laiemat kasutust on leidnud faktoriseerimine - RSA krüptosüsteemis, ja diskreetse logaritmi arvutamine - ECC (Elliptic Curve Cryptography) krüptosüsteemides.

6 Lõpetuseks

Autorsuse üle vaidlemise skandaalina võiks öelda, et Diffie, Hellmani, Rivesti, Shamiri ja Adlemani revolutsioon oli mõni aasta hilisem Suurbritannia salateenistuste omast. GCHQ (Government Communications Headquarters) töötajad olid sarnase probleemiga tegelenud, kuid oma töö salastatuse tõttu mitte seda avaldanud. Üldsusele sai teatavaks see alles 1990. aastate lõpus. Nimelt 1970. a vormistas James H. Ellis (1924-1997, Briti insener ja krüptograaf) GCHQ siseraporti "The Possibility of Secure Non-Secret Digital Encryption" („Turvalise mittesalajase digitaalse krüpteerimise võimalus“), mille idee 1973. a Clifford Cocks (s 1950, Briti matemaatik ja krüptograaf) realiseeris oma raportis „A note on Non-Secret Encryption“, mis on olemuslikult RSA analoog. See info edastati ka USA julgeolekuagentuurile NSA, kuid selle kasutusest ei ole palju teateid. Seda peeti siiski ka liialt kalliks kaitsevaldkonna jaoks, väidetavalt kuni 1980ndateni.

Kuigi üldiselt ei ole enam põhjust arvata, et Diffie ja Hellman olid esimesed, kes avaliku võtme krüptograafia välja mõtlesid, siis ikkagi on nende teene selle tegelik kasutus ja levik. Selle eest on neid pärjatud 2015. a Turingi auhinnaga (peetakse arvutiteaduse Nobeliks) ning 13 aastat varem oli RSA kolmik samuti selle auhinna saanud. Eesti e-edukusele vaadates on Diffie, ja eelkõige just Hellman, seotud krüptograafia väljumisega puhtalt sõjalisest ja

luure kasutusest. See võitlus on pikalt kestnud ning kestab ju senini. Arvamus, et teatud riikide teatud asutustel peab olema võimalik tungida isiku privaatsfääri, ei ole kuhugi kadunud ning pigem leiab taas uusi toetajaid. Samas tahavad valdavalt needsamad teatud riikide teatud asutused, et nende enese kommunikatsioonile selline omadus ei rakenduks.

Diffie ja Hellmani tööd aitasid ka kaasa krüptograafiat edendavate teadlaste koostööle ning avalikule tunnustusele töö eest, mis seni oli jäänud saladuseks. Nõukogude Liidu lagunemise järel oli Eesti tutvus lääneliku krüpteerimise teadmistega päästikuks mitme teadus- ja ettevõtluskogukonna tekkeks. Ligipääs Nõukogude Liidu vastavale infole oli ju olematu ning usk nende kasutatavusse Eesti Vabariigis, isegi võimaluse ilmnedes, oli väike. Seega kui oli vaja ehitada üles Eesti Vabariigi luureorganisatsioonid, valitsusside ja turvata kaitseplaane, siis olime üsna asjade alguses. Tänu krüptograafia-alaste teadmiste avalikule publitseerimisele said eestlased lahendada nii tekkinud praktilisi probleeme kui ka osaleda aktiivselt uurimistes ning äris. Eestist on täna selle põhjal sündinud nii tipptasemel teadlasi kui ka rahvusvahelist tuntust kogunud tooteid ja teenuseid. Diffie ja Hellman olid selle taga, et teadmised krüptograafia arengutest olid avalikult saadavad ning nendeni jõuti nii FidoNeti (Eestis oli FidoNet populaarne ajal, kui internetiühendust veel ei olnud) kui ka raamatute kaudu, mistõttu noor Eesti sai jõuliselt alustada.

Kirjandus

1. W. Diffie, M. Hellman, New Directions in Cryptography (Invited Paper). *IEEE Transactions on Information Theory*, **IT-22 Nov.**(1976), 644-654.

2. D. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms.* Addison-Wesley, 1969 (1981, 1997, 2016, vene k 1977).

