Pogovor z matematikom in kriptologom prof. dr. Aleksandrom Jurišićem

Kriptosistemi z eliptičnimi krivuljami – nov temelj digitalnega poslovanja

Dr. Mojca Vizjak Pavšič

V sodobni informacijski družbi, ki temelji na elektronskem poslovanju, postajajo orodja za zagotavljanje računalniške in komunikacijske varnosti, odločilnega pomena. Temeljni gradniki računalniške varnosti, ki so za uporabnike običajno popolnoma nevidni, so izjemno zapleteni kriptografski algoritmi in protokoli. Slovenija se z lastnim razvojem uporabe eliptičnih krivulj v kriptografiji uvršča med redke države na svetu, ki to ključno tehnologijo prihajajoče digitalne dobe obvladujejo.

Otej vrhunski tehnologiji, ki je bila še pred nekaj desetletji skoraj izključno pod nadzorom tajnih služb, je ekskluzivno za prilogo *Znanost* spregovoril matematik **prof. dr. Aleksandar Jurišić**, raziskovalec na Inštitutu za matematiko, fiziko in mehaniko v Ljubljani in predsednik pred kratkim ustanovljenega Društva kriptologov Slovenije.

Katere kriptografske algoritme v praksi najpogosteje uporabljate?

Gre za dve vrsti kriptografskih algoritmov: simetrične in asimetrične. Lastnost prvih je, da uporabljamo isti ključ za šifriranje in odšifriranje. Uporabljamo jih že od nekdaj. V digitalnem okolju so ti algoritmi hitri, ključi pa sorazmerno kratki. Uporabljamo jih za zaščito oziroma šifriranje daljših sporočil. Slabost sistemov s simetričnimi algoritmi je, da za izmenjavo ključev potrebujemo ločen, varen kanal, na primer kurirja ali pa sestanek na štiri oči. Tako postane sistem zelo zapleten in ranljiv, če se število oseb, ki komunicirajo med seboj, povečuje.

Ta problem sta leta 1976 rešila Whitfield Diffie in Martin Hellman z vpeljavo koncepta kriptografije javnih ključev. Po tem konceptu ima vsak uporabnik samo en par ključev: javnega, ki je praviloma znan drugim uporabnikom, in zasebnega, ki je znan le uporabniku, ki je lastnik ključa. Iz javnega ključa ni mogoče priti do zasebnega ključa. Če javni ključ nekega uporabnika uporabljamo za šifriranje sporočil, potem bo lahko odšifriral skrito sporočilo le on, nihče drug namreč ne more priti do njegovega zasebnega ključa. Par ključev lahko uporabimo tudi drugače. Sporočilo najprej zašifriramo s svojim zasebnim ključem, potem pa ga lahko katerikoli drugi uporabnik odšifrira z našim javnim ključem. V tem primeru govorimo o digitalnem podpisu, saj ni mogel nihče drug brez našega zasebnega ključa zašifrirati sporočila, ki ga odšifrira naš javni ključ. Glede na to, da uporabljamo par različnih ključev, govorimo o asimetričnih metodah kriptografije.

Vendar pa Diffie ne slovi le kot začetnik kriptografije javnih ključev, temveč ga širša javnost pozna tudi kot bojevnika za svobodo govora.

Whit Diffie je zares izjemna osebnost. Leta 1976 sta se Diffie in njegova žena Mary kot študenta le s težavo preživljala in živela kar v avtu. Revščini navkljub je Diffie kot študent Univerze Stanford sredi sedemdesetih let prejšnjega stoletja delal na kompleksnem matematičnem algoritmu, ki naj bi pomagal zaščititi svobodo govora in zasebnosti v bližajoči se digitalni dobi (več zanimivih informacij o tem lahko najdemo na spletnem naslovu časopisa *The New York Times* http://www.nytimes.com/books/first/l/levy-crypto.html; op. p.).

Stvari so se precej izboljšale, ko je Diffie skupaj s Hellmanom odkril rešitev teh problemov v obliki kriptografije javnih ključev, ki uporablja javni in zasebni digitalni ključ za šifriranje in odšifriranje podatkov. Toda medtem ko je Diffie čakal 20 let na pravo potrebo po Diffie-Hellmanovem algoritmu, se je neutrudno bojeval za odpravo zakonov o izvozni kontroli, ki so omejevali možnosti za uporabo šifriranja – predvsem zunaj ameriške celine. Te zakone so zares odpravili ob koncu devetdesetih let prejšnjega stoletja.

Stanovski kolega Bruce Schneier je o Diffieju povedal naslednje: »Javno nastopanje in udejstvovanje Whita Diffieja pomeni boj za prave stvari. Internetna svoboda in zasebnost skozi kriptografijo pomenijo njegovo osebno vizijo. Govoril je z zelo vplivnimi ljudmi. Za marsikaj se lahko zahvalimo prav njegovi neustavljivi osebnosti.«

Za učinkovito šifriranje tajnih sporočil je bil velikega pomena tudi izum algoritma RSA, ki temelji na problemu faktorizacije oziroma iskanju deliteljev velikih števil.

Že leto potem, ko sta Diffie in Hellman predstavila koncept javne kriptografije, namreč leta 1977, so Rivest, Shamir in Adelman predstavili in patentirali algoritem RSA, ki temelji na problemu faktorizacije, kar je izjemno težko izračunljiv matematični problem. Čeprav se zdi naloga na prvi pogled preprosta, je izračun deliteljev v praksi težak problem. Matematikom namreč še vedno ni uspelo najti zares učinkovite metode faktorizacije. Algoritem RSA se je hitro uveljavil in ostal vse do zdaj dejanski temelj kriptografskih sistemov z javnimi ključi. Glede na monopol nad patenti v zvezi z algoritmom RSA, ki jih je imela družba RSA Inc., je ameriška vlada, ki je skušala zmanjšati stroške države, kar kmalu razvila nov algoritem DSA (Digital Signature Algoritem), ki pa ni temeljil na problemu faktorizacije velikih

> Digitalni podpis lahko izvedemo z algoritmom RSA in tudi z DSA, česar pa ni lahko realizirati s simetričnimi (konvencionalnimi) kriptografskimi sistemi. Omeniti je treba še eno dodatno prednost, ki bi lahko bila ključnega pomena v dobi vsesplošne uporabe javnih omrežij odprtega tipa, kot je internet. Za izmenjavo ključev ne potrebujemo ločenega varnega kanala, temveč lahko podpis pa tudi izmenjavo ključev vršimo na istem nezaščitenem kanalu. Vendar ima dodatna funkcionalnost asimetričnih kriptoalgoritmov svojo ceno. Ti sistemi so računsko izjemno zahtevni in so večstokrat počasnejši od primerljivih simetričnih sistemov!

Foto Mojca Vizjak Pavšič

PROF. DR. ALEKSANDER JURIŠIĆ

števil, temveč na problemu rešitve diskretnega logaritma nad velikimi števili. V primerjavi z RSA pa se DSA lahko porablja samo za digitalni podpis.

Izračun asimetričnih kriptografskih algoritmov je tako glavni del obremenitve komunikacijsko-računalniške infrastrukture pri vzpostavljanju varnih povezav. Problem je bil še posebno težaven v omejenih okoljih, denimo pri pametnih karticah, ki zahtevajo v teh primerih pomoč dodatnega koprocesorja, s tem pa tudi višjo ceno. Asimetrični kriptosistemi se zato uporabljajo za digitalni podpis, morebitno šifriranje kratkih sporočil in za uskladitev ključa s simetrično kriptosistema.

Izjemno hiter razvoj računalniške tehnologije pa zdaj v kriptografiji omogoča uporabo zelo zapletene teorije eliptičnih krivulj ...

Računalniki so zelo olajšali iskanje racionalnih točk na eliptičnih krivuljah. Odkritje učinkovitega algoritma polinomske časovne zahtevnosti pa je omogočilo učinkovito štetje točk na (diskretni) eliptični krivulji. Tako je sledila rešitev prej opisanega problema uskladitve ključa in čim krajšega digitalnega podpisa že osem let po izumu RSA, ko sta Neil Koblitz in Victor Miller neodvisno predlagala uporabo eliptičnih krivulj v kriptografiji z javnimi ključi (ECC – Elliptic Curve Cryptography). Eliptične krivulje igrajo v teoriji števil in algebraične geometrije osrednjo vlogo že več kot sto let. Napisane so bile številne knjige, ki zajemajo to tematiko. Morda velja omeniti citat Serga Langa: »O eliptičnih krivuljah bi bilo mogoče pisati brez konca. (To ni mišljeno kot grožnja.)« Eliptične krivulje so imele pomembno vlogo tudi pri dokazu Fermatovega zadnjega izreka, ki ga je ne tako dolgo nazaj odkril Andrew Wiles. Čeprav so bile eliptične krivulje sprva študirane predvsem zaradi povsem (umetniških) matematično estetskih razlogov, pa jih v zadnjem času uporabljajo številni algoritmi za faktorizacijo, dokazovanje praštevilskosti in v kriptosistemih z javnimi ključi. V tem primeru so osnova matematična problema (diskretnega logaritma na eliptični krivulji), ki je še bistveno težje rešljiv kot problem faktorizacije celih števil. Zato in zaradi nekaterih drugih lastnosti so ključi, ki se uporabljajo v kriptosistemih z eliptičnimi krivuljami, krajši, računanje algoritmov pa je v splošnem bistveno hitrejše pri kriptosistemih z eliptičnimi krivuljami kakor pri RSA.

Vendar je bila kriptografija z eliptičnimi krivuljami kljub očitnim prednostim in navdušenju znanstvenih krogov v praksi sprva sprejeta z veliko previdnostjo. Ne nazadnje so bili vsi zadovoljni s preizkušenim algoritmom RSA, pri razmeroma majhnih ključih RSA pa prednosti zamenjave niso bile tako očitne. Z naraščanjem računske moči in odkrivanjem vedno novih algoritmov za učinkovito faktoriziranje se je večala tudi možnost napada na RSA. Leta 1999 je bila industrija po uspešno razbitem 512-bitnem ključu RSA – ki je, mimogrede, še vedno standard na pametnih karticah v sistemu Europay, Mastercard in Visa – prisiljena preiti na večje ključe, tipično 1.024 bitov in 2.048 bitov. S povečanimi zahtevami po procesorski moči (ta naraša približno s kubom rasti velikosti ključa), pojavom novih matematičnih napadov na RSA in s splošno rastjo računske moči so razmere počasi postajale zrele za alternativo.

Kriptosistemi z eliptičnimi krivuljami so se v dvajsetletnem obdobju od svojega odkritja počasi uveljavljali v industriji, predvsem tam, kjer so bili na voljo omejeni sistemi, na primer v pametnih karticah in nekaterih mobilnih komunikacijah. Do leta 2000 so bili kodificirani v vseh glavnih industrijskih standardih. Kljub številnim poskusom kriptološki znanstveni srenji v tem obdobju ni uspelo najti učinkovitega napada na kriptosisteme z eliptičnimi krivuljami. Vsem pozitivnim trendom navkljub pa je v razmeroma konzervativni kriptografski praksi algoritem RSA ostal prevladujoč standard.

Kakšni so rezultati evropskega in japonskega projekta, katerih namen je bil poiskati učinkovite postopke varovanja elektronskega poslovanja v prihodnjih desetletjih?

Prvo priznanje je kriptografija z eliptičnimi krivuljami doživela z izborom v preferenčno skupino algoritmov v evropskem programu NESSIE (New European Scheme for Signature, Identification and Encryption), ki je potekal med letoma 2000 in 2004, in japonskem CRYPTREC (Cryptographic Research and Evaluation Committee), ki je potekal med letoma 2000 in 2003. Cilj obeh projektov je bil enak: poiskati kriptografske algoritme, ki bodo hrbtenica infrastrukture e-poslovanja v desetletjih, ki prihajajo.

Kako ukrepajo Američani?

Pravi šok je nastal, ko je ameriška NSA (National Security Agency) letošnjega 16. februarja objavila tako imenovano Suite B. Sestavljajo jo kriptografski algoritmi, ki se uporabljajo v ameriških državnih organih ob vključno »top secret level«. Na presenečenje vseh so kriptosistemi z eliptičnimi krivuljami edina možnost za asimetrični algoritem, trenutno prevladujoči algoritem RSA pa ni omenjen več niti kot alternativa. Kriptosistemi z eliptičnimi krivuljami so že zdaj standardni algoritem v ameriškem globalnem informacijskem omrežju (Global Information Grid), do leta 2008 pa naj bi se zgodil prehod na kriptosisteme z eliptičnimi krivuljami tudi v okviru Natove informacijske infrastrukture. Pričakuje se, da bo v naslednjih letih treba zamenjati kar tri četrtine vse kriptografske infrastrukture v razvitih državah!

Prednosti kriptosistemov z eliptičnimi krivuljami pred RSA lepo prikaže tabela s spletne strani NSA (http://www.nsa.gov/ia/industry/crypto_suite_b.cfm?MenuID=10.2.7), iz katere je razvidna primerjava varnostno primerljivih nivojev RSA, kriptosistemov z eliptičnimi krivuljami (ECC) in simetričnih sistemov.

Če želimo za izmenjavo (zaščito) 128-bitnega asimetričnega ključa (na primer algoritma AES) uporabiti algoritem RSA ali DSA, potem moramo ob predpostavki, da ohranjamo varnost na isti ravni, uporabiti 3.072-bitne ključe. Primerljivi ključ ECC, ki zagotavlja isto raven varnosti, je velik le 256 bitov in je torej več kot desetkrat manjši. Če nam ta raven varnosti (3.072 bitov RSA ali 256 bitov ECC je minimalna dolžina asimetričnega ključa za zaščito prihajajočih biometričnih potnih listov) ne zadošča in se želimo povzpeti na ameriški standard za raven »top secret«, potem bi morali uporabiti ključe RSA dolžine kar 15.360 bitov do ekvivalentnih 512 bitov za ECC. Vidimo, da raven varnosti z dolžino ključa pri ECC naraša bistveno hitreje kot pri RSA. Ker bi bilo pri tej velikosti razmerje med obre-

Priporočljive velikosti ključev za različne nivoje varnosti

Simetrični algoritmi (bitov)	RSA in DSA (bitov)	ECC (bitov)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15.360	512

menitvijo računskih zmogljivosti kar 60 : 1 v škodo RSA, ni čudno, da je priporočilo NSA, da se nad ravnijo varnosti 1.024-bitnih ključev RSA uporablja izključno kriptosisteme z eliptičnimi krivuljami. Ti torej zagotavljajo največjo varnost na bit ključa med asimetričnimi sistemi in najcenejši način doseganja višjih ravni varnosti.

Leta 1991 je pri Društvu matematikov, fizikov in astronomov Slovenije izšla knjiga ugledenega slovenskega matematika, akademika prof. dr. Ivana Vidava z naslovom Eliptične krivulje in eliptične funkcije. Kako bi z današnje perspektive ocenili pomen tega dela?

Za tako majhen narod, kakor je naš, je vsaka knjiga v domačem jeziku dragocena. Ko pa piše tak mojster, kakor je prof. Vidav in ki ima pri tem še toliko očitnega veselja in veščine, kako predstaviti težko področje širokemu krogu bralcev, postane hitro očitno, da bi kazalo prevesti knjigo prof. Vidava še v kakšen svetovni jezik.

Kakor omeni v uvodu že sam avtor, je zdaj študij eliptičnih krivulj postal pomemben tudi zunaj matematičnih znanosti, bolj natančno v kriptografiji javnih ključev. Zato se je začelo neobičajno veliko ljudi ukvarjati s tem področjem. Na letošnjem Eurocryptu (glavni evropski konferenci na področju kriptografije) je takorekoč vsak drug sogovornik že počel kaj v zvezi s kriptosistemi z eliptičnimi krivuljami, pa naj je šlo za uslužbenca nemškega Telekoma, ki je implementiral eliptične krivulje že pred leti, za mladega poljskega matematika, ki dela v kriptografskem podjetju in se je pravkar začel ukvarjati z optimizacijo algoritmov z eliptičnimi krivuljami, za izraelskega inženirja, ki je iskal učinkovite implementacije digitalnega podpisa z eliptičnimi krivuljami na pametnih karticah, ali pa za uglednega nizozemskega matematika Reneja Schoofa, ki je prvi predlagal učinkovit algoritem za štetje točk na eliptični krivulji in je imel prav na tej konferenci osrednje vabljeno predavanje. Z redkimi izjemami, kot je matematik Rene Schoof, pa večina med njimi nima potrebnega matematičnega predznanja. Zato to bi jih knjiga prof. Vidava še dodatno motivirala in prepričala, da je to področje vredno njihove pozornosti.

Sodobno modeliranje in prototipiranje na Fakulteti za strojništvo v Ljubljani

Snemanje s hitrostjo do 30.000 točk na sekundo

Tomaž Švagelj

Kdor hoče nov izdelek čim hitreje spraviti na trg, mora izvesti vrsto zahtevnih izračunov in tehnoloških operacij, med katerimi je še zlasti zanimiva avtomatizirana izdelava zelo natančnih replik fizičnih predmetov. V Sloveniji so s prenosom znanja iz akademske v gospodarsko in tržno sfero še vedno težave, ni pa mogoče reči, da se na tem področju nič ne dogaja.

Pri nas imamo na primer že vrsto tako imenovanih (raziskovalnih) centrov odličnosti, ki se dopolnjujejo, ali »so komplementarni«, z omrežji odličnosti v šestem okvirnem programu EU (sofinancirajo jih evropski strukturni skladi). Njihov cilj je vzpostavitev in zagotovitev uspešnega delovanja vsaj osmih mednarodno konkurenčnih centrov odličnosti na prednostnih področjih raziskav in tehnološkega razvoja.

V vsakem centru te vrste mora biti vrhunska večdisciplinarna skupina raziskovalcev iz akademske sfere in gospodarstva, torej kritična masa znanja z ustrezno raziskovalno infrastrukturo za preboj centra v sam vrh svetovne znanosti in/ali njegovo vključevtev v mednarodno omrežje odličnosti. V sedanjem obdobju je za centre odličnosti v Sloveniji predvidenih dobre tri milijarde tolarjev (obdobje sofinanciranja je 2004–2006 z možnostjo črpanja do leta 2008).

Fotografije Tomaž Švagelj

Na levi je »tiskalnik« Stratasys Dimenison 3D, na desni pa laserski 3D skener Kreon Zephyr KZ50 na petosni mehanični roki Faro Gold Arm (med laserskim modeliranjem kavlja).

Od ideje do prototipa

V skladu s tem projektom so na Fakulteti za strojništvo v Ljubljani, v okviru svojega laboratorija LECAD, pred kratkim zasnovali še Center za celostni razvoj izdelkov (GPRC, Global Product Realization Center), kjer bodo raziskovali še zlasti razvoj izdelkov v sistemu PLM (Product Life Cycle Management). Tehnično je namreč povsem opremljen za spremljanje izdelka v celotnem življenjskem ciklu, od prve ideje do izločitve iz uporabe »nazaj v naravo«. Vodi ga **prof. dr. Jože Duhovnik**.

Center je glede strojne kot tudi programske opreme zasnovan tako, da je v njem mogoče izvajati vse, od ideje do izdelave prototipa. Preden se razvojniki res lahko lotijo prototipa, jih seveda čaka še marsikaj, od analiz funkcij in funkcionalnosti, prek meritev oblik in oblikovanja modelov, do virtualnega prikazovanja v realnem prostoru. V primeru zahtevnejših oblik iz trših materialov jim priskoči na pomoč fakultetni LABOD, to je **La**boratorij za **od**rezavanje, ki ga vodi **prof. dr. Janez Kopač**.

Pri analizi izdelkovih funkcij si pomagajo s programsko opremo, deloma svojo deloma kupljeno. Obliko posnamejo in izmerijo z gibljivo mehanično roko, opremljeno z laserskim merilnikom. Ta lahko posname do 30.000 točk na sekundo (!), kar ne zadošča samo za površine različnih tehničnih izdelkov, velikih do 3,5 metra, pa naj so še tako zapleteni, temveč tudi za predmete živalskega ali rastlinskega izvora, arheološke izkopanine in tudi za izdelavo natančnih kopij starih kipov. Na primer katerega od tistih z Robbovega vodnjaka. Najprej bi ga lasersko posneli, s tem dobili njegov digitalni prostorski model, zatem, na njegovi podlagi, zelo natančno repliko iz umetne snovi, manjkajoče dele pa bi nazadnje dopolnili po navodilih umetnostnih zgodovinarjev. Vendar to še ni vse, saj obstaja tudi možnost neposrednega frezanja replike v kamen.

Z umetno snovjo gre seveda lažje in hitreje, saj lahko model iz polimera ABS, v velikosti do 200 x 250 x 200 milimetrov, naredijo že v 48, izjemoma celo v 24 urah. Če so zahteve pri takem iz orodne plastike ali aluminija glede natančnosti strožje, lahko naredijo prototip, natančnosti do 0,05 milimetra. Če potrebujejo samo zunanjo obliko, natančnosti do 0,5 mm, si pomagajo s toplim vlekom umetne snovi do velikosti 600 x 600 x 400 mm.

Medakademijsko sodelovanje

Te dni je bil na dvodnevnem obisku pri Slovenski akademiji znanosti in umetnosti (SAZU) podpredsednik Britanske akademije iz Londona **prof. dr. Nicholas Mann**. Prof. Mann je v Britanski akademiji, ki pokriva družbene in humanistične vede in s katero je Slovenska akademija leta 2000 podpisala sporazum o znanstvenem sodelovanju, odgovoren za mednarodne stike. Med delovnim srečanjem z vodstvom SAZU so se dogovorili, da bodo v bodočem sodelovanju predvsem poudarjeni skupni projekti med akademijama, in manj individualne izmenjave znanstvenikov in raziskovalcev. Prof. Mann je s predsednikom SAZU **prof. Žekšem** podpisal podaljšanje sporazuma o bilateralnem sodelovanju do leta 2009. **D. B.**

Ustrezni sistemi za vse

Center za celostni razvoj je še zlasti primeren za *ad hoc* skupine različnih strokovnjakov. V mednarodnem sodelovanju s skupinami za strojništvo in mikroelektroniko, z industrijskimi oblikovalci in ekonomisti, specializiranimi za poslovno ekonomiko, ima že štiriletne izkušnje. Opremljen je tudi z videokonferenčnima sistemoma, ki po hitrosti prenosa povsem zadošča za neposredno sodelovanje v virtualni sobi.

V centru so trenutno dejavne tri skupine, ki snujejo nove izdelke v okviru dveh domačih in enem mednarodnem projektu. Vendar njegova zmogljivost zadošča za vsaj še tri skupine vse do aprila 2006, ko ga bodo za šest mesecev zasedli sodelujoči v dveh drugih mednarodnih projektih. Podjetja, ki že sodelujejo, so Niko in Domel Železniki, Iskraemeco Kranj, LIV Postojna in BSH Nazarje, sodelujejo pa tudi s tujimi univerzami, in sicer s tehničnima univerzama Lulea na Švedskem in TU Delft na Nizozemskem ter s Politehniko Wroclaw.

Z uporabo novih tehnologij lahko podjetja bistveno izboljšajo delo in izdelke. Vprašanje pa je, kako različnim podjetjem, tudi malim in srednje velikim, omogočiti ustrezne sisteme. Velika potrebujejo zelo zmogljive sisteme PDM, ki so ne le dragi, temveč zahtevajo tudi veliko dodatnih dejavnosti – vzdrževanje, uvajanje, izobraževanje, integracijo v poslovne in proizvodnje sisteme –, mala pa se lahko zadovoljijo s cenejšimi in enostavnejšimi sistemi PDM. V majhni razvojni skupini s komunikacijo med člani ni težav, po drugi strani pa enostaven sistem PDM omogoča še zlasti lažje arhiviranje, enostavno uporabo in vzdrževanje, dostop prek interneta, določen način dela ima že vgrajen itd. Do izraza pridejo nove možnosti, ki jih nudi internet: delo poteka prek splošno razširjenega brskalnika in odjemalcu ni treba namešča nobenih novih programov. To so dobre strani enostavnih sistemov PDM, med slabimi pa je na prvem mestu omejitev pri prilagajanju konfiguracije. Enostaven PDM sistem temelji na podatkovni bazi datotek, do katerih lahko uporabniki dostopajo pač glede na razvojno fazo projekta in svojo vlogo. Podatke v bazi lahko ne le iščejo temveč tudi spreminjajo. Do strežnika lahko dostopajo s spletnim brskalnikom, edinim potrebnim programom na strani odjemalca. Sisteme vsebinsko in celovito razvijajo v mednarodnem združenju laboratorijev LECAD Group s sedežem v Ljubljani.

Ko je izdelek razvit, pride v proizvodnjo in končno na trg. Tam se začne njegova tržna vrednost zaradi konkurenčnih izdelkov takoj zmanjševati, kar lahko uspešno omejujemo z njegovim stalnim izboljševanjem in dopolnjevanjem. Podaljšana prodajna doba mu tržno uspešnost seveda poveča, saj je razvoj nove družine izdelkov zelo drag. V ta okvir sodijo drobni popravki pa tudi priprava povem novih različic.

> Cilj sistema PDM (Product Data Management, tudi PLM, Product Life Cycle Management) je kar se da skrajšati pot od prve zamisli prek prodaje in uporabe pa vse do odpisa in recikliranje izdelka. Ves čas je treba imeti nadzor in pregled nad potrebnimi podatki in jih dostavljati tistim, ki (in ko) jih potrebujejo. Ključni podatki v takem sistemu so samo enkrat, to je v enem »izvodu«, shranjeni na enem mestu, tako da jih nepoklicani ne morejo spreminjati ali brisati, hkrati pa je vse dovoljene spremembe mogoče ves čas nadzorovati, slediti, preverjati in seveda shranjevati. Kopije teh podatkov prosto krožijo med oddelki za oblikovanje, konstruiranje in različne analize ter med udeleženci delovnega procesa, spremenjeni oziroma novi podatki pa prihajajo nazaj na kraj varnega shranjevanja. Vsakokrat, ko se kaj spremeni, se modificirana kopija, podpisana in datirana, shrani v »digitalnem sefu« poleg prejšnjih, ki ostanejo v svoji prvotni obliki kot stalno arhivirani zapisi.

Slovenski (ISKRA) petosni hitrofrezalni stroj Flexmatic X/Z/Y SA 1000 (z delovnim območjem 800 x 600 x 300 mm) v zaščitni komori in motorizirano projekcijsko platno za LCD projektor visoke svetilnosti.

Miza za računalniško modeliranje s štirimi delovnimi postajami za grafično in računsko zahtevne operacije.

Problem vibracij

Za primer lahko vzamemo sesalno enoto, to je sklop motorja in turbine. V razvoju takih enot obstaja izrazita tendenca po povečanju števila vrtljajev in zmanjšanju mase in prostornine, pri čemer pa so, še zlasti pri višji napetosti, problem vibracije. Temeljno vprašanje se glasi, kakšen je vpliv posameznih sestavnih delov na kritično hitrost, dodatni pa sta povezani z uporabnostjo posameznih metod za analizo lastnih frekvenc in z vplivom lastnosti sestavnih delov na tresljaje med obratovanjem, ugotavljata prof. Duhovnik in **doc. Jože Tavčar**.

Za konec še kratek pregled hitrega modeliranja in prototipiranja. Prvotni stereolitografiji je sledilo lasersko »sežiganje« koviskih prašnih delcev. Prah iz kovine s talilčem pri 400 do 500 stopinjah Celzija z laserskim žarkom lokalno segrejejo, tako da se začne taliti in sprijemati. V bistvu gre torej za nekakšno lokalno varjenje. Treba je samo iti po modelu in vključiti laser le tam, kjer je model poln. Laserskemu »sežiganju« se sledila tako imenovana praškasta tehnologija, pri kateri se uporablja navaden prah, ki je lahko tudi keramičen. Nanj brizgajo tekočo plastiko v plasteh debeline od 0,07 do 0,15 mm, in potem »počakajo, da lepo počasi reagira«. Če hočejo proces pospešiti in utrditi, model še dodatno žgejo. To je praškasta tehnologija, v Centru za celostni razvoj izdelkov pa uporabljajo umetno snov termoplast ABS, ki jo raztalijo, zatem v majhnih količinah brizgajo skozi šobo in z računalniško vodeno 2D napravo nanašajo v obliki plastnic.