Rok IV, numer 6(32) Do użytku wewnętrznego

INFORMATOR WYDZIAŁOWY

Wydział Matematyki i Informatyki UAM, ul. Matejki 48/49, 60–769 Poznań

marzec 1997

Rada Wydziału na posiedzeniu w dniu 7.03.1997 wszczęła przewód habilitacyjny pani dr Joannie Jędrzejowicz z Instytutu Matematyki Uniwersytetu Gdańskiego. Powołano komisję do przeprowadzenia tego przewodu w następującym składzie: prof. dr hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Tadeusz Batóg, prof. dr hab. Jacek Błażewicz, prof. dr hab. Lech Drewnowski oraz prof. dr hab. Marek Wisła. Jednocześnie na recenzentów powołano prof. dra hab. Wojciecha Buszkowskiego (UAM), prof. dra hab. Andrzeja W. Mostowskiego (Instytut Matematyki Uniwersytetu Gdańskiego) oraz prof. dra hab. Wojciecha Ryttera (Instytut Informatyki Uniwersytetu Warszawskiego).

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada Wydziału zatwierdziła prowizorium budżetowe na rok 1997. Przewiduje ono przychody Wydziału w kwocie 1 200 tys. złotych, w tym dotacja KBN na działalność statutową 315 tys., nadwyżka z dotacji KBN w 1996 roku 45 tys., dotacja KBN na badania własne 160 tys., dotacja na działalność dydaktyczną 180 tys. i wpływy z opłat za studia zaoczne 500 tys. Po stronie wydatków przewiduje się przeznaczenie 360 tys. na działalność statutową, 160 tys. na badania własne oraz 180 tys. na działalność dydaktyczną. Na studia płatne wydanych zostanie 500 tys., w tym 250 tys. to koszty ponoszone przez uczelnię związane z obsługą studentów, 160 tys. to płace, 90 tys. wydatkie rzeczowe i usługi Wydziału.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału zaopiniowała pozytywnie zasady dokonywania okresowych ocen nauczycieli akademickich zatrudnionych na naszym Wydziale. Głoszą one m.in, że podstawą oceny jest dorobek naukowo-badawczy, dydaktyczny i organizacyjny oraz opinia bezpośredniego przełożonego lub opiekuna naukowego. Końcowym efektem pracy zespołu oceniającego jest jedna z trzech następujących ocen: wyróżniająca, pozytywna i negatywna. W posiedzeniach zespołu bierze udział bezpośredni przełożony ocenianego pracownika.

⋆ ⋆ ⋆ ⋆ ⋆

Na posiedzeniu Rady Wydziału w dniu 7.03.1997 Prodziekan prof. dr hab. Zbigniew Palka przedstawił bieżące sprawy związane z reformą studiów oraz sprawozdanie z dotychczasowego wdrażania nowych zasad studiowania. Omówiono też sprawę seminariów w ramach nowego systemu studiów. Rada przyjęła uchwałę postanawiającą, że jednym z warunków otrzymania tytułu magistra matematyki lub magistra informatyki jest zaliczenie seminarium przeglądowego (w wymiarze 30 godzin) oraz seminarum magisterskiego (w wymiarze 90 godzin).

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada zaopiniowała pozytywnie wniosek o nadanie prof. drowi hab. Romanowi Taberskiemu Krzyża Oficerskiego Orderu Odrodzenia Polski, jak również wniosek o nadanie drowi Wiesławowi Kurcowi Medalu Komisji Edukacji Narodowej.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału w miejsce prof. dra hab. Krzyśki powołała na członka komisji do spraw nagród prof. dra hab. Lecha Drewnowskiego. Rada zaopiniowała też pozytywnie wniosek komisji o przedstawieniu JM Rektorowi i Senatowi UAM kandydatury prof. dra hab. Macieja Wygralaka oraz prof. dra hab. Wojciecha Buszkowskiego do nagrody Ministra Edukacji Narodowej.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału powołała Komisję do spraw wydziałowych grantów naukowych. W skład komisji weszli: prof. dr hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Wojciech Buszkowski i prof. dr hab. Paweł Domański.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału powołała komisję w przewodzie doktorskim mgra Krzysztofa Feledziaka z Instytutu Matematyki Wyższej Szkoły Pedagogicznej w Zielonej Górze. Przewodniczącą komisji została prof. dr hab. Paulina Pych-Taberska, wiceprzewodniczącym zaś prof. dr hab. Henryk Hudzik. W skład komisji weszli: prof. dr hab. Marian Nowak (WSP, Zielona Góra) — promotor, prof. dr hab. Julian Musielak oraz prof. dr hab. Ryszard Grząślewicz (Instytut Matematyki Politechniki Wrocławskiej) — egzaminatorzy z dyscypliny podstawowej i recenzenci, prof. dr hab. Roman Murawski — egzaminator z dyscypliny pomocniczej oraz prof. dr hab. Ryszard Urbański — członek komisji.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału na posiedzeniu w dniu 7.03.1997 zaopiniowała limity przyjęć na studia na naszym Wydziale w roku akademickim 1997/98. Na studia dzienne zamierza się przyjąć 200 osób, w tym 150 osób na kierunek matematyka i 50 osób na kierunek informatyka. Na studia zaoczne ustalono następujące limity: studia 5-letnie z matematyki — 60 osób, studia licencjackie z informatyki — 80 osób, studia uzupełniające II stopnia z informatyki — 20 osób. Na studia podyplomowe przyjętych zostanie 150 osób, w tym na kierunek matematyka — 50, na kierunek informatyka — 50 i na kierunek matematyka z informatyką — 50.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała pozytywnie wniosek dra Wojciecha Gajdy z Zakładu Geometrii i Toplogii o bezpłatny urlop naukowy w okresie 1.09.1997–15.02.1998. Dr Gajda prowadzić będzie w tym czasie badania naukowe nma Uniwersytecie w Bielefeld w ramach stypendium Fundacji im. Aleksandra Humboldta.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała też pozytywnie wniosek mgr Małgorzaty Powierskiej o przedłużenie jej stypendium doktorskiego o 7 miesięcy.

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 7.03.1997 odbyło się uroczyste spotkanie z okazji 70-tych urodzin prof. dra hab. Romana Taberskiego.

Z historii . . .

Sto lat temu, 15.03.1897 roku zmarł w Londynie James Joseph Sylvester (ur. 3.09.1814 roku w Londynie). Studiował w latach 1833–1837 w Liverpoolu i w St. Johns College w Cambridge. W roku 1839 został profesorem filozofii naturalnej na Uniwersytecie w Londynie. W latach 1841–1845 był profesorem na University of Virginia (USA). Po powrocie do Anglii pracował przez 10 lat jako matematyk zajmujący się ubezpieczeniami i jako adwokat. W tym okresie poznał też A. Cayley'a, który na nowo rozbudził w nim zainteresowania matematyczne. W latach 1855–1870 był profesorem matematyki w Akademii Wojskowej w Woolwich. Tutaj założył Quaterly Journal. *Po kolejnych 6 lat, które przeżył bez żadnego stałego zatrudnienia, działał w okresie 1876–1884 w USA, gdzie był profesorem na J. Hopkins University w Baltimore. Tutaj w roku 1884 założył* American Journal of Mathematics. *W 1884 roku otrzymał sawiliańską katedrę geometrii w Oxfordzie, której kierownikiem był do roku 1892.*

Sylvester zajmował się algebrą i kombinatoryką oraz geometrią, rachunkiem prawdopodobieństwa i kinematyką. W swoich licznych pracach wprowadził podstawowe dziś pojęcia teorii eliminacji i teorii niezmienników oraz dowiódł wielu ważnych twierdzeń w tych teoriach. Zajmował się także podziałami liczb oraz teorią macierzy.

R.M.

Rozstrzygnięty został konkurs na wydziałowe granty dydaktyczne. Komisja w składzie: doc. dr hab. Magdalena Jaroszewska (przewodnicząca), prof. dr hab. inż. Aleksander Waszak i dr Dariusz Bugajewski przyznała granty następującym osobom: 1. dr G. Banaszak i dr W. Gajda — 3,0 tys. zł, 2. dr R. Doman — 2,0 tys. zł, 3. mgr St. Gawiejnowicz — 2,0 tys. zł, 4. dr St. Gniłka, dr D. Stachowiak-Gniłka i dr K. Nowakowski — 3,5 tys. zł, 5. dr J. Jaworski i prof. dr hab. Z. Palka — 2,5 tys. zł, 6. dr E. Marchow — 1,0 tys. zł, 7. dr K. Pawałowski — 2,5 tys. zł, 8. dr K. Świrydowicz — 1,5 tys. zł. Komisja nie widziała możliwości przyznania kontynuacji grantu dydaktycznego w roku 1997 drowi T. Frysce. Komisja przyznała w pozycji nr 5 grant na zakup sprzętu i honorarium autorskie dla dra J. Jaworskiego.

⋆ ⋆ ⋆ ⋆ ⋆

Na stronie domowej Wydziału `http://math.amu.edu.pl/welcome.html` znajduje się połączenie z (w języku informatyków: link do) *Mathematical Reviews* (od roku 1988).

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 7–9.03.1997 odbywały się na naszym Wydziale Warsztaty Matematyczne dla uzdolnionych uczniów szkół średnich. Uczniowie ci są pod opieką Krajowego Funduszu na Rzecz Dzieci. Ze strony Wydziału za organizację odpowiadał prof. dr hab. Wacław Marzantowicz. Zajęcia dla uczniów prowadzili (bezinteresownie) profesorowie Krystyna

Bartz, Paweł Domański, Wacław Marzantowicz i Andrzej Ruciński, dr Grzegorz Banaszak, dr Tadeusz Fryska, dr Krzysztof Pawałowski, dr Leszek Skrzypczak oraz studenci Andrzej Dudek i Maciej Radziejewski.

Prof. Mikael Lindström (Åbo, Finlandia) gościł w dniach 9–18.03.1997 w Zakładzie Analizy Funkcjonalnej.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 9–13.03.1997 gościem Zakładu Metod Numerycznych był prof. Ludwig Elsner z Uniwersytetu w Bielefeld (RFN).

⋆ ⋆ ⋆ ⋆ ⋆

Gościem Zakładu Matematyki Dyskretnej był w dniach 10–13.03.1997 prof. Zdenek Strakoš z Instytutu Informatyki CAN (Praga, Czechy).

W sieci

Piękno na to jest by zachwycało
Do pracy ...
C.K. Norwid, Promethidion

Wszystko zmierza ku wizualizacji. Ekspansja technik grafiki komputerowej połączonej z technologiami sieciowymi zaowocowała w ostatnich latach powstaniem takich produktów, jak Java, czy alternatywnego wobec niej ActiveX, a także powolnym wchodzeniem do Internetu wirtualnej rzeczywistości (VR). Pojęcie „wirtualny" zrobiło zresztą karierę samo w sobie. Odmieniane w najróżniejszych przypadkach, używane w najrozmaitszych sytuacjach i kontekstach, często zupełnie bez sensu, na dobre zadomowiło się w technicznej „polszczyźnie", obok wielu innych nieprzetłumaczalnych (z praktycznego punktu widzenia) określeń. Sieciowa VR odbiega jeszcze znacznie od tego, co oznaczało to pojęcie wcześniej, a czego jedną z udanych realizacji może być np. projekt symulacji środowiska teleskopu Hubble, wykonany w celu umożliwienia treningu przed jego rzeczywistą naprawą w kosmosie, która jak wiadomo zakończyła się względnym sukcesem. Naukowcy z NASA zaprogramowali w pamięci komputera całą geometrię kluczowych fragmentów teleskopu, a następnie ekipa treningowa posługując się specjalnymi hełmami z ciekłokrystalicznym wyświetlaczem (tzw. HMD) oraz równie dziwnymi rękawicami mogła do woli trenować każdy ruch, tak jakby przebywała w rzeczywistym środowisku przestrzeni kosmicznej. Projekt ten opisany został wielokrotnie, a jego szczegóły można znaleźć w Internecie, gdzieś w obszarze NASA. Niestety w sieci nie jest jeszcze tak dobrze. Wszystko się oczywiście rozbija o szybkość przesyłu danych. Właściwie to w ostatnim roku znowu nastąpił tak olbrzymi wzrost liczby użytkowników Internetu, iż linie są całkowicie zakorkowane (najgorzej jest z łączem do Stanów — linia NASK-u praktycznie cały tydzień ma 100% -owe obciążenie, co oznacza jej praktyczną nieużyteczność do wielu zastosowań). Sytuacja ta powoduje, iż nie ma mowy o interakcyjnym przesyłaniu olbrzymich ilości danych graficznych w czsie rzeczywistym.

Symbolem sieciowego rozumienia VR jest, specjalnie dla WWW napisany, język programowania obiektów trójwymiarowych — tzw. VRML. Jego początki, jak zwykle w takich

sytuacjach, nie są całkiem jasne. Idea rozszerzenia HTML-a i wykorzystania WWW pojawiła się m.in. w pracy D. Raggett'a z Hewlett-Packard Laboratories.Przedstawił on niezwykle śmiałą wizję VRML-a, który powinien umożliwiać wykorzystanie całego spektrum osiągnięć grafiki komputerowej, powinien móc zintegrować fizyczną przestrzeń z dźwiękiem, umożliwić swobodne przemieszczanie się w środowisku 3-wymiarowym wielu osobom poruszającym się w tym samym obszarze i mogącym na siebie oddziaływać poprzez interakcję fizyczną i głosową. Autor rozważa też oczywistą potrzebę wypracowania metod reprezentacji obiektów trójwymiarowych, które pozwoliłyby osiągnąć sukces w sferze fotorealizmu generowanych scen. Jakiej skali są to trudności, pokazuje przedstawiony przez Raggett'a przykład „zanimowania" w czasie rzeczywistym procesu powstawania fałdy na ubraniu, podczas unoszenia ręki. Klasyczne, ale bardzo kosztowne czasowo metody, takie jak np. raytracing, są tu absolutnie nie do wykorzystania. Tak naprawdę to obecnie nie ma systemu, który pozwoliłby na tworzenie animacji w czasie rzeczywistym (może z jednym wyjątkiem — systemu Onyx firmy Silicon Graphics). Osiągnięcie sukcesu w tej sferze wymaga jak zwykle równoległej pracy w wielu dziedzinach — od algorytmów, poprzez metody reprezentacji, konstrukcję procesorów i specjalizowanych układów graficznych itd. Bardzo łatwy jest natomiast do zrealizowania pomysł użycia adresu URL-owego, tzn. takiego, jaki jest używany do specyfikacji położenia plików w HTML-u. Jego ogólność umożliwia posługiwanie się nim zarówno w hipotetycznej sytuacji otwierania gazety (link do zwykłych dokumentów HTML-owych), włączania radia (link do plików dźwiękowych), otwierania drzwi i wchodzenia do innego pomieszczenia (link do plików opisujących nową scenę) itp. Zabawa, jak widać, może być przedniej jakości (tylko te zapchane sieci!). Obecnie VRML jest już w dość zaawansowanej formie rozwoju. Najpierw była poprzedzona długą dyskusją w Internecie, moderowaną przez Marc'a Pesce, wersja 1.0. Nie zawierała ona jednak implementacji ruchu, czyli tego, bez czego VR nie jest właściwie sobą. Potem pojawiła się propozycja wersji 2.0 pozwalająca już na pełną interakcję. Z geometrycznego punktu widzenia w VRML-u nie wymyślono niczego nowego. Zastosowano istniejącą już, opracowaną przez SGI bibliotekę do programowania grafiki trójwymiarowej — OpenGL. Istota jej leży w tym, że pozwala ona na bardzo szerokie wspomaganie sprzętowe, tzn. podział zadania generowania obrazu na fragmenty wykonywane przez specjalizowane układy procesorów, wykorzystujących dodatkowe, wbudowane bufory pamięciowe. Zużytkowanie tych możliwości wymaga jednak posiadania odpowiednich kart graficznych, a te cacka są niestety ciągle jeszcze nieco drogie (PC-towe wersje kosztują w granicach 2000-5000 dolarów, unixowe są zintegrowane ze stacjami graficznymi i ich cena jest dużo wyższa). Wszystkie te kłopoty powodują, iż popularność VRML-a w sieciach nie jest nazbyt ogromna. Jednak jego upowszechnienie jest tylko kwestią czasu, zwłaszcza gdy okaże się, że ma on również zastosowania komercyjne. W takich sytuacjach nawet specjaliści od robienia pieniędzy o mentalności yuppies pełnią pożyteczną rolę. Można sobie np. wyobrazić zwiedzanie muzeów, do których wchodzimy klikając myszką na klamkę drzwi wejściowych, wykupujemy bilet w wirtualnej kasie, a potem, już wolni, zanurzamy się w świat całkiem nie elektronicznego piękna smukłych postaci, o długich szyjach, subtelnych twarzach i oczach, w których nie ma pustki — postaci, które mistrz Modigliani „wygenerował" w całkiem nie elektroniczny sposób. I chwała mu za to.

Mgr Wojciech Kowalewski

Dnia 4.03.1997 prof. dr hab. Jacek Błażewicz (Politechnika Poznańska) wygłosił wykład zatytułowany „Biologia molekularna a zagadnienia optymalizacji kombinatorycznej".

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 7.03.1997 prof. dr hab. Michał Kurzyński (Wydział Fizyki UAM) wygłosił wykład zatytułowany „Dynamika białek i stystystyczna teoria procesów biochemicznych".

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 11.03.1997 gościnne wykłady na Wydziale wygłosili: prof. Ludwig Elsner (Universität Bielefeld, RFN), tytuł wykładu: „The theorem of Hoffman-Wielandt and its variations", prof. M. Lindström (Åbo, Finlandia), tytuł wykładu: „Gleason parts and weakly compact homomorphisms between uniform algebras", oraz prof. Zdenek Strakoš (CAN, Praga, Czechy), tytuł wykładu: „On the convergence of the Krylow space methods".

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 14.03.1997 odbył się Czwarty Wykład im. Wojtka Pulikowskiego. Wydział gościł dra hab. Zbigniewa Marciniaka z Uniwersytetu Warszawskiego, którego wystąpienie było zatytułowane „O problemie izomorfizmu pierścieni grupowych".

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 21.03.1997 w ramach kolokwiów wydziałowych prof. dr hab. Stanisław Balcerzyk (UMK, Toruń) wygłosił wykład zatytułowany „O powstawaniu pojęć algebraicznych".

Notatka

KILKA UWAG O KRYPTOLOGII — część III

Kryptografia z kluczem publicznym

Jeśli stosujemy tradycyjny kryptosystem, to sytuacja wygląda tak, że jeżeli ktoś potrafi zaszyfrować informację w tym systemie, to wie dostatecznie dużo, by również odszyfrować przechwyconą informację. W 1976 roku W. Diffie i M. Hellman zaproponowali kryptografię z kluczem publicznym, która jest oparta na spostrzeżeniu, że procedury szyfrowania i deszyfrowania nie muszą posługiwać się tym samym kluczem. Usuwa to konieczność utrzymywania w tajemnicy klucza szyfrującego. Przekształcenie szyfrujące f musi być stosunkowo łatwe do wyliczenia, ale wyznaczenie f^{-1} musi być skrajnie trudne, o ile nie mamy dodatkowej informacji. Tym samym ten, kto zna jedynie klucz szyfrujący, nie jest w stanie odkryć klucza deszyfrującego bez stosowania obliczeń, praktycznie niewykonalnych. Jak dotychczas w przypadku żadnego z proponowanych systemów nie udowodniono, że faktycznie przekształcenie jest jednokierunkowe, a więc nie pokazano dla żadnego z istniejących kryptosystemów, że nie jest możliwe przeliczenie przekształcenia odwrotnego i odszyfrowanie informacji przy znajomości jedynie przekształcenia szyfrującego.

Kryptosystem RSA. *Nazwa tego kryptosystemu pochodzi od autorów R. Rivesta, A. Shamira i L. Adlemana. Powstał on w 1978 roku i jest oparty na trudności rozkładu dużych liczb na czynniki pierwsze. Mimo, że nie jest trudnym zadaniem znalezienie w sposób losowy dwu dużych liczb pierwszych i przemnożenie ich, to operacja odwrotna, a*

więc odtworzenie rozkładu liczby wielocyfrowej okazuje się być procesem niezwykle powolnym. Z tego powodu rzucono nawet wyzwanie publikując w 1977 roku iloczyn dwu liczb pierwszych (64 i 65 cyfrowej) - tzw RSA–129 i twierdząc, że znalezienie tego rozkładu zajmie 40×10^{15} *lat. Wyzwanie podjęto i w 1994 roku rozkład ten został znaleziony przez zespół pod kierunkiem A. Lenstry i przy pomocy 1600 komputerów pracujących przez 8 miesięcy. (Okazuje się, że w roku 1996 dokonano rozkładu liczby 130 cyfrowej, a więc postęp jest o wiele szybszy, aniżeli przypuszczano.)*

Kryptosystem RSA pracuje w sposób następujący. Przypuśćmy, że obierzemy losowo dwie 150 cyfrowe liczby pierwsze p *i* q*. Następnie obliczamy ich iloczyn* $n = pq$ *oraz dodatkowo* $m = \varphi(n) = (p-1)(q-1)$*, gdzie przez* φ *rozumiemy funkcję Eulera. Następnie przystępujemy do szukania losowo liczby* E *takiej, która jest względnie pierwsza z* m*; to znaczy obieramy* E *takie, że* $\mathrm{nwd}(E, m) = 1$*. Teraz przy pomocy algorytmu Euklidesa możemy znaleźć taką liczbę* D*, że* $DE \equiv 1 \pmod{m}$*. Liczby* n, E *mogą być opublikowane.*

Przypuśćmy teraz, że osoba B *chce przesłać osobie* A *jakąś wiadomość przez kanał publiczny. Ponieważ każdy zna liczby* E, n*, to każdy może przy ich pomocy przeprowadzić proces szyfrowania. Najpierw* B *przetwarza informację na postać liczbową, jak to opisaliśmy poprzednio, a więc zastępuje litery alfabetu ich odpowiednikami liczbowymi. Jeśli to będzie potrzebne, to podzieli jeszcze informację na kawałki takie, że każdy taki kawałek będzie reprezentowany liczbą mniejszą niż* n*. Przypuśćmy, że* x *jest jednym z takich kawałków.* B *oblicza liczbę* $y = x^E \bmod n$ *i przesyła* y *do* A*. Odbiorca dla odtworzenia* x *musi jedynie obliczyć* $x = y^D \bmod n$*. Dokonać tego może jedynie* A*, gdyż tylko on zna swój klucz prywatny* D*.*

Przykład. *Zanim przebadamy teorię kryjącą się za kryptosystemem RSA, czy spróbujemy użyć dużych liczb, zastosujemy kilka małych liczb, by zobaczyć, że system istotnie działa. Przypuśćmy, że chcemy przesłać pewną informację, która przetworzona do postaci numerycznej daje liczbę* 23*. Obierzmy liczby pierwsze* $p = 23, q = 29$*. Ich iloczyn wynosi*

$$n = pq = 667,$$

zaś funkcja Eulera ma wartość

$$m = \varphi(n) = (p-1)(q-1) = 616.$$

Teraz szukamy liczby E*, względnie pierwszej z* 616*, powiedzmy, że będzie to* $E = 487$*. Kodujemy informację* $x = 23$*, obliczając*

$$23^{487} \bmod 667 = 368$$

i przesyłamy ją do odbiorcy. Potęgowanie „modularne" daje się przeprowadzić bardzo szybko. Odbiorca musi oczywiście znać liczby p, q *i dzięki temu stosując algorytm Euklidesa określa* $D = 191$ *takie, że* $191E = 1 + 151m$*, tzn* $DE \equiv 1 \pmod{m}$*. Może wobec tego odtworzyć przesłaną informację* 368*, podnosząc ją do potęgi* 191*:*

$$368^{191} \bmod 667 = 23.$$

Teraz możemy sprawdzić, dlaczego system RSA funkcjonuje. Wiemy, że $DE \equiv 1 \pmod{m}$*, a więc istnieje takie* $k \in \mathcal{Z}$*, że*

$$DE = km + 1 = k\varphi(n) + 1.$$

Podnosząc przesłany kryptogram $y = x^E$ do potęgi D dostajemy

$$y^D = (x^E)^D = x^{km+1} = (x^{\varphi(n)})^k x = x \bmod n$$

na podstawie twierdzenia Eulera, które stwierdza, że $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Zapytajmy teraz, jak można przełamać system RSA. Trzeba by znaleźć D (n, E są publicznie znane). Należy więc jedynie rozłożyć n na czynniki $p \cdot q$, co pozwoli znaleźć $m = (p-1)(q-1)$ i przy pomocy znanego E znaleźć kluczową wartość D rozwiązując kongruencję $Ex \equiv 1 \pmod{m}$. Zatem cała trudność leży właśnie w znalezieniu rozkładu liczby n, co uważa się za problem niezwykle trudny obliczeniowo przy obecnym stanie wiedzy, chociaż nie wiadomo, jak to będzie wyglądać np. za 10 lat.

Sprawdzenie autentyczności. *W kryptosystemach z kluczem publicznym nie ma problemu ze sprawdzeniem autentyczności informacji. Ponieważ klucz szyfrowania jest publicznie dostępny, więc dowolna osoba jest w stanie przesłać informację do danego odbiorcy w postaci zaszyfrowanej. Jeżeli osoba* A *otrzymuje informację od* B*, to chciałaby ona być w stanie upewnić się, że pochodzi ona istotnie od* B*. Przypuśćmy, że klucz szyfrujący (publiczny) dla* B *ma postać (n', E'), zaś kluczem deszyfrującym (prywatnym) jest (n', D'). Analogicznie* A *ma klucze (n, E) i (n, D). W tej sytuacji* B *może upewnić* A*, że to on jest autorem przesłanej informacji w sposób następujący: Właściwą informację x przekształca najpierw przy pomocy swego klucza tajnego, obliczając*

$$x' = x^{D'} \bmod n'.$$

Wprawdzie każdy może przekształcić x' z powrotem w x, gdyż klucz szyfrujący E' jest publiczny, więc wystarczy wyliczyć $x = (x')^{E'} \bmod n'$, ale tylko B *był w stanie przekształcić właściwą informację x do postaci x'. W następnym kroku* B *szyfruje x' przy pomocy klucza publicznego przewidzianego odbiorcy* A*, a więc oblicza*

$$y' = (x')^E \bmod n.$$

Tę informację rozszyfrować jest w stanie jedynie A*, obliczając*

$$x' = (y')^D \bmod n,$$

a stąd już łatwo odtwarza właściwą informację

$$x = (x')^{E'} \bmod n',$$

jako że te parametry znów są publiczne. Dzięki tym dwóm fazom szyfrowania uzyskuje się zatem nie tylko utajnienie informacji, ale również weryfikację autentyczności.

Dr Tadeusz Fryska

Opracowanie Informatora: Maciej Kandulski (mkandu@math.amu.edu.pl)
Roman Murawski (rmur@math.amu.edu.pl)

http://math.amu.edu.pl/~mathem/info/new/welcome.htm