Rok IV, numer 5(31) Do użytku wewnętrznego

INFORMATOR WYDZIAŁOWY

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

luty 1997

Rada Wydziału na posiedzeniu w dniu 7.02.1997 wszczęła przewód habilitacyjny drowi Wojciechowi Kordeckiemu z Politechniki Wrocławskiej. Powołano też komisję w następującym składzie: prof. dra hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Dobiesław Bobrowski, prof. dr hab. Mirosław Krzyśko, prof. dr hab. Julian Musielak, prof. dr hab. Zbigniew Palka. Na recenzentów powołano: prof. dra Jamesa Oxley'a (Luisiana State University, USA), prof. dra hab. Tomasza Rolskiego (Uniwersytet Wrocławski), prof. dra hab. Andrzeja Rucińskiego (UAM) i prof. dra hab. Zdzisława Rychlika (UMCS, Lublin).

⋆ ⋆ ⋆ ⋆ ⋆

Na tym samym posiedzeniu Rada Wydziału powołała komisję w sprawie wszczęcia przewodu habilitacyjnego pani dr Joannie Jędrzejowicz z Instytutu Matematyki Uniwersytetu Gdańskiego. W skład komisji weszli: prof. dr hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Tadeusz Batóg, prof. dr hab. Jacek Błażewicz, prof. dr hab. Lech Drewnowski i prof. dr hab. Marek Wisła.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału wszczęła przewód doktorski mgrowi Pawłowi Foralewskiemu, słuchaczowi IV roku Studium Doktoranckiego Matematyki. Zatwierdzono temat rozprawy, który brzmi: „O topologicznej i geometrycznej strukturze uogólnionych przestrzeni Calderona-Łozanowskiego". Na promotora powołano dotychczasowego opiekuna naukowego prof. dra hab. Henryka Hudzika. Powołano również komisję w następującym składzie: prof. dr hab. Paulina Pych-Taberska (przewodnicząca), prof. dr hab. Ryszard Urbański (wiceprzewodniczący), prof. dr hab. Henryk Hudzik (promotor), prof. dr hab. Roman Murawski, prof. dr hab. Witold Wnuk. Na recenzentów powołano: prof. dra hab. Juliana Musielaka (UAM) i prof. dra hab. Stanisława Prusa (UMCS, Lublin). Wyznaczono także zakres egzaminów doktorskich, które obejmą: analizę matematyczną (dysyplina podstawowa), filozofię matematyki (dyscyplina pomocnicza) i język angielski.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału wszczęła przewód doktorski mgrowi Sebastianowi Urbańskiemu, słuchaczowi II roku Studium Doktoranckiego Matematyki. Zatwierdzono temat rozprawy doktorskiej, który brzmi: „Liczby Folkmana", a na promotora powołano prof. dra hab. Andrzeja Rucińskiego, dotychczasowego opiekuna naukowego. Ustalono też zakres egzaminów doktorskich, które obejmą: rachunek prawdopodobieństwa i kombinatorykę, filozofię matematyki oraz język angielski.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału powołała komisję do spraw nagród w następującym składzie: prof. dr hab. Jerzy Kaczorowski (przewodniczący), prof. dr hab. Mirosław Krzyśko, prof. dr hab. Roman Murawski, prof. dr hab. Marek Nawrocki i prof. dr hab. inż. Aleksander Waszak.

⋆ ⋆ ⋆ ⋆ ⋆

Rada Wydziału zaopiniowała pozytywnie wniosek mgr Mirosławy Kołowskiej-Gawiejnowicz o przedłużenie o sześć miesięcy stypendium doktorskiego.

⋆ ⋆ ⋆ ⋆ ⋆

Rada zaopiniowała pozytywnie wniosek mgr Magdaleny Makowiak o udzielenie urlopu naukowego na okres semestru letniego.

Z historii . . .

Sto lat temu, 19.02.1897 roku, zmarł w Berlinie Karl Theodor Wilhelm Weierstrass (ur. 31.10.1815 w Ostenfelde, Westfalia). W 1834 rozpoczął studia ekonomiczne z zakresu finansów. Po 8 semestrach przerwał je, aby móc całkowicie poświęcić się matematyce. Ponieważ rodzice nie byli w stanie finansować jego studiów, uczęszczał w roku 1839 do Akademii Teologicznej i Filozoficznej w Monastyrze (Münster), gdzie już po roku zdał egzaminy pozwalające na podjęcie pracy nauczycielskiej. Tutaj też studiował u C. Gudermanna teorię funkcji eliptycznych, dalszemu rozwijaniu której miał poświęcić wiele lat życia. Po zdaniu w 1841 roku egzaminów końcowych i pomyślnym zaliczeniu stażu jako nauczyciel w gimnazjum w Monastyrze, pracował w latach 1842–1848 w Progimnazjum Katolickim w Wałczu, a w latach 1848–1855 w Gimnazjum Katolickim w Braniewie. Cały czas prowadził badania naukowe w zakresie matematyki i w roku 1854 opublikował pracę na temat funkcji abelowych, która przyniosła mu sławę. W 1854 roku otrzymał doktorat honorowy Uniwersytetu w Królewcu. Od roku 1856 działał w Berlinie, najpierw jako profesor w Gewerbeinstitut (poprzednik Wyższej Szkoły Technicznej), a od 1864 jako profesor zwyczajny Uniwersytetu Berlińskiego. W 1856 został członkiem Berlińskiej Akademii Nauk.

Wraz ze swym przyjacielem E.E. Kummerem założył w 1861 roku (oficjalnie zaś w 1864) pierwsze na uniwersytecie niemieckim seminarium badawcze poświęcone matematyce. Weierstrass poprzez swoje wykłady, seminaria i działalność w Akademii w sposób istotny wpłynął na rozwój matematyki nie tylko w Niemczech. Berlin był w tym okresie jednym z najważniejszych ośrodków matematyki w Europie (ściągającym tłumy studentów dzięki wykładom Weierstrassa). Ze szkoły Weierstrassa wyszli m.in. S. Kowalewska, G. Mittag-Leffler, G. Cantor, H.A. Schwarz. Weierstrass zajmował się głównie teorią funkcji eliptycznych i teorią funkcji abelowych.

R.M.

Prof. dr hab. Jerzy Kaczorowski został wybrany do Komisji Rektorskiej d/s Współpracy z Zagranicą.

⋆ ⋆ ⋆ ⋆ ⋆

Cytat

Dowód opuszczam ze względu na jego monotonię.

Z egzaminu pisemnego

W wydawnictwie Walter de Gruyter ukazała się książka *Functional Analysis*, której jednym ze współredaktorów jest prof. dr hab. Paweł Domański z Zakładu Analizy Funkcjonalnej naszego Wydziału.

O książkach . . .

John D. Barrow, π razy drzwi. Szkice o liczeniu, myśleniu i istnieniu*, Prószyński i S-ka, Warszawa 1996, ss. 438, tłum. z ang. K. Lipszyc.*

Recenzowana książka mówi o rozmaitych problemach związanych z historią, z podstawami i z filozofią matematyki. Jest to książka raczej popularna, daje więc przystępny przegląd różnych tematów. Możemy tu znaleźć bardzo interesującą historię rozwoju pojęcia liczby i systemów liczbowych, dyskusję różnych poglądów i tendencji w filozofii matematyki, uwagi na temat twierdzeń Gödla o niezupełności i wiele, wiele innych. Czyta się ją lekko i przyjemnie.

Pewnym brakiem książki jest (programowe?) unikanie wzorów matematycznych, co powoduje, że niektóre wywody są nie do końca precyzyjne i jasne (por. na przykład wykład twierdzeń Gödla). Rażą także nieuzasadnione uogólnienia i wyciąganie zbyt ogólnych wniosków z prezentowanych twierdzeń (czemu sprzyja wspomniany brak precyzji). Denerwuje też brak odsyłaczy do literatury przy podawanych cytatach.

Jest to więc kolejna z popularnych ostatnio i publikowanych (nie tylko w wydawnictwie Prószyński i S-ka) w dużej liczbie książek opowiadających o różnych ważnych dziedzinach nauk ścisłych. Pozycje takie są bardzo potrzebne — nie tylko dla szerokich kręgów czytelników-niefachowców, ale i dla fachowców (choćby po to, by w lekkiej i przyjemnej formie zapoznać się z osiągnięciami kolegów z sąsiednich działek własnej dziedziny czy też dziedzin pokrewnych). Szkoda tylko, że książki te to w zasadzie tylko tłumaczenia prac autorów obcych (głównie anglosaskich), że nie ma wśród nich prawie w ogóle dzieł autorów polskich. Ciągle jednak umiejętność popularnego pisania, na przykład o matematyce, jest u nas rzadka i, co gorsze, zupełnie niedoceniana!

M.K. & R.M.

Od stycznia do marca 1997 staż naukowy na Wydziale odbywa mgr Ralf Sausen z Uniwersytetu w Trewirze (RFN). Opiekunem naukowym mgra Sausena jest prof. dr hab. Paweł Domański.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 1–9.02.1997 gościła na Wydziale prof. Maria de Prada z Uniwersytetu w Bilbao (Hiszpania).

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 5–9.02.1997 gościem Zakładu Matematyki Dyskretnej był A. Panconesi z Uniwersytetu Humboldta w Berlinie.

⋆ ⋆ ⋆ ⋆ ⋆

W dniach 16–22.02.1997 gościem Wydziału był prof. Olivier Ramaré z Uniwersytetu w Lille (Francja).

W sieci

Wszystko należy robić tak prosto, jak to jest możliwe,
ale nigdy nie prościej.
Albert Einstein

Agencje prasowe doniosły, iż student Uniwersytetu w Berkeley Ian Goldberg , posługując się 250 komputerami połączonymi w sieć lokalną, złamał kod przedstawiony jako zadanie dla hackerów przez firmę RSA Security Dynamics. Zadanie polegało na odszyfrowaniu tekstu zakodowanego słowem długości 40 bitów, a więc maksymalnej długości, którą oferuje oprogramowanie niestrzeżone w USA embargiem. Potrzebował on na to tylko 4 godzin. W wyraźny sposób unaocznia to słabości tak krótkich słów kodowych w stosunku do możliwości szybkościowych sprzętu, który przecież ciągle się rozwija. Nie wiadomo, jaka będzie ostateczna odpowiedź ludzi decydujących o dopuszczeniu wysokich technologii do sprzedaży, ale oczywiście nie jest to problem jedynie amerykański. Coraz silniejsza ekspansja handlu sieciowego, włączenie do sieci banków (smutny kabaret, który rozegrał się na przełomie roku w PKO BP pokazuje, jak to wszystko jeszcze kuleje) i związane z tym transfery pieniężne oraz wiele innych inwestycji, stawiają problem bezpieczeństwa przesyłanych danych wśród kwestii zasadniczych i decydujących o dalszym rozwoju sieci. Bezwzględny wyścig firm produkujących oprogramowanie sieciowe o prymat na rynku i eliminację konkurencji, oprócz chwilowych korzyści polegających na darmowym rozdawnictwie programów w celu przyzwyczajenia do nich klientów, niesie w sobie także problem — na ile te produkty są bezpieczne w użyciu. Zwykle jest tak, że im szybciej się coś tworzy, im więcej się rozdaje, tym gorszy jest to półprodukt. Kłopoty Microsoftu z Active X, który ma być alternatywą dla Javy, symbolizują niejako całe zjawisko. Może Bill Gates powinien zastosować do siebie i swojej firmy, przypisywaną mu (w dowcipach) zasadę, iż należy wyjść i wejść ponownie. Ochrona integralności danych dotyczy w równej mierze sieci rozległych, jak i lokalnych, w których istnieje potrzeba stworzenia mechanizmów blokujących ingerencje z zewnątrz, dokonywane przez ludzi czasami ciekawych i zdolnych, ale częściej złośliwych i pozbawionych wyobraźni. Banalne i dostępne dla każdego oszustwa w wysyłaniu fałszywych mail'i (z oczywistych powodów nie podaję narzędzi i szczegółów umożliwiających to), mechanizmy „integrujące" różne sieci lokalne w jedną, w których bezpieczeństwo opiera się na zasadach zaufania do innych użytkowników, bądź ich nieświadomości, są tylko przykładami kłopotów, które będą być może narastały. Oczy się otwierają zwykle w momencie kiedy się osobiście doświadczy skutków istnienia

dziur w systemie. Niestety jest to nauka, która boli (czasami również materialnie). Obecnie najpopularniejszą technologią ochrony sieci lokalnych przed ingerencją z zewnątrz jest stosowanie tzw. firewall. Rozwiązania te bazują zwykle na algorytmach opartych o DES (Data Encription Standard) i mogą być zaimplementowane na kilka sposobów, różniących się poziomem bezpieczeństwa. Począwszy od prostych — routerów filtrujących transmitowane pakiety, aż po bardzo silne, jak wydzielone podsieci realizujące filtrację pakietów. To ostatnie rozwiązanie polega na dwukrotnym wykorzystaniu układu: router filtrujący oraz komputer o funkcjonalności twierdzy sieciowej (Bastion Host). Wewnątrz sieci lokalnych mechanizmy ochrony nie muszą być oczywiście tak silne, niemniej jakieś powinny istnieć. Na razie jedynym dostępnym rozwiązaniem wykraczającym poza zasadę wzajemnego zaufania są bardzo drogie narzędzia w rodzaju Kerberos. W każdym razie pozostaje tylko mieć nadzieję na to, że w tworzonej właśnie sieci wydziałowej nie zdarzą się poważne wpadki przed jej uszczelnieniem.

Chciałbym poruszyć jeszcze jedną sprawę natury trochę subtelniejszej. Skłaniają mnie do tego dwa fakty. Po pierwsze obejrzany przypadkowo bardzo piękny film o życiu Jana Karskiego, po drugie 60-lecie urodzin i związana z tym sesja poświęcona Michałowi Hellerowi. Pierwszy z nich — słynny kurier, którego zasługą jest m.in. dostarczenie aliantom dokumentów o eksterminacji Żydów, później wybitny politolog i znawca problematyki wschodniej, profesor jednego z uniwersytetów w Waszyngtonie, nauczyciel wielu znaczących ludzi, w tym obecnego prezydenta Stanów Zjednoczonych. Drugi — znakomity fizyk kosmolog, pracujący w dziedzinie, w której jak mało gdzie unaocznia się siła i piękno matematyki, ksiądz, nieograniczający się w poszukiwanich naukowych do wąskiej specjalności, umysł iście renesansowy, autor ponad 700 prac naukowych dotyczących szerokiego spektrum zagadnień daleko wykraczających poza ukochaną kosmologię, w poświęconym mu zbiorze esejów nazwany Księdzem Cogito i rzeczywiście posiadający coś wspólnego z herbertowskim pierwowzorem. Pomyślałem sobie, jak mało wiemy o ludziach, którzy mogą nas ubogacić nie tylko swoją wiedzą naukową, ale również tą znacznie ważniejszą. W związku z tym ośmielam się poddać pod rozwagę Szanownym Redaktorom (i nie tylko) pomysł nowej, stałej rubryki w Informatorze (co wobec jego powrotu do Internetu posiada dodatkowy walor) prezentującej sylwetki profesorów naszego Wydziału od strony nie tylko naukowej (także sylwetki tych, którzy już odeszli, a o których pamiętają już tylko nieliczni). Wszak pamięć o tych, których dłużnikami jesteśmy, stanowi również o cząstce naszego człowieczeństwa.

Mgr Wojciech Kowalewski

Dnia 28.02.1997 o godzinie 12.00 prof. dr hab. Paweł Domański wygłosi wykład pt. „Holomorficzna zależność od parametru rozwiązania równania różniczkowego cząstkowego".

⋆ ⋆ ⋆ ⋆ ⋆

Dnia 7.03.1997 prof. dr hab. Michał Kurzyński z Wydziału Fizyki UAM wygłosi wykład pt. „Dynamika białek i statystyczna teoria procesów biochemicznych".

⋆ ⋆ ⋆ ⋆ ⋆

KILKA UWAG O KRYPTOLOGII — część II

Kryptografia z kluczem prywatnym (klasyczna)

W kryptosystemach z kluczem prywatnym (pojedynczym), ten sam klucz jest używany tak do szyfrowania, jak i odtajniania informacji. By zaszyfrować dany tekst jawny, stosujemy pewne przekształcenie, powiedzmy f, które utrzymujemy w tajemnicy. Zastosowanie go pociąga otrzymanie kryptogramu. Jeśli mamy do czynienia z zaszyfrowaną informacją, to jej odtworzenie wymaga zastosowania transformacji odwrotnej f^{-1}. Tak f, jak i f^{-1} muszą być stosunkowo proste do wykonania; jednakże muszą to być transformacje krańcowo trudne do wykrycia, jeżeli dostępny jest jedynie tekst zaszyfrowany.

Przykład 1. *Jeden z pierwszych i najsławniejszych kryptosystemów klasycznych nosi nazwę* szyfru Cezara *i faktycznie był stosowany przez tego rzymskiego męża stanu. Należy on do tzw.* szyfrów podstawieniowych, *co polega na tym, że za każdą jednostkę tekstu jawnego podstawia się zawsze tę samą jednostkę szyfrującą. Algorytm szyfrowania E_K u Cezara polegał na cyklicznym przesuwaniu liter alfabetu w tekście jawnym o trzy pozycje do przodu. Oznacza to, że w miejsce* A *pisze się* D, *w miejsce* B *pisze się* E *itd., wreszcie w miejsce* X *piszemy* A, *w miejsce* Y *piszemy* B *i w miejsce* Z *piszemy* C. *Oczywiście konkretna realizacja zależy od stosowanego alfabetu (czy dołączamy cyfry, znaki interpunkcyjne itd), ale zasada jest zawsze taka sama. Najpierw porządkujemy litery alfabetu, a następnie stosujemy cykliczne ich przesuwanie. Dla łatwiejszej analizy matematycznej dobrze jest wpierw alfabet przetransponować na postać liczbową, tzn. każdej literze przypisać jej numer. Jeśli przykładowo weźmiemy tylko duże litery od* A *do* Z *i nie uwzględnimy znaków diakrytycznych (ą, ę, ć itd.), to będziemy mieli 26 znaków, którym przyporządkujemy liczby od 0 (=*A*) do 25 (=*Z*). Wówczas funkcja szyfrująca będzie miała postać*

$$f(p) = r_{26}(p+3)\,(= p+3 \bmod 26).$$

(Przez $r_x(u)$ lub też $u \bmod x$ rozumiemy resztę z dzielenia u przez x.) Łatwo sprawdzić, że istotnie mamy dla f: $\mathsf{A} \mapsto \mathsf{D}, \mathsf{B} \mapsto \mathsf{E}, \ldots, \mathsf{Z} \mapsto \mathsf{C}$. Funkcja dekodująca jest wyznaczona jednoznacznie przez klucz $K = 3$ i ma postać

$$f^{-1}(p) = r_{26}(p-3) = r_{26}(p+23)\,(= p+23 \bmod 26).$$

Przypuśćmy, że dostaliśmy zaszyfrowaną informację postaci DOJHEUD. *Dla jej odtajnienia przetwarzamy ją najpierw do postaci „numerycznej" uzyskując ciąg*

$$3, 14, 9, 7, 4, 20, 3.$$

Następnie stosujemy transformację odwrotną uzyskując ciąg

$$0, 11, 6, 4, 1, 17, 0.$$

Te numerki po podstawieniu odpowiadających im liter dają nam słowo ALGEBRA. *Zwróćmy uwagę na fakt, że liczba 3 obrana za klucz szyfrowania niczym specjalnie się*

nie wyróżnia i z równym powodzeniem możemy wziąć każdą inną od 1 do 25. Przy tym samym algorytmie E mamy tu zatem 25 przekształceń szyfrujących E_K. Również liczba 26 jest w tym schemacie nieistotna i zależy jedynie od alfabetu, w jakim są pisane teksty jawne i kryptogramy i jest równa ilości liter tego alfabetu.

Sposobami przełamywania szyfrów (a więc metodami odczytywania kryptogramów bez znajomości funkcji deszyfrującej) zajmuje się nauka „bliźniacza" do kryptografii, zwana **kryptoanalizą**. *W tym przypadku wielkie znaczenie mają rachunek prawdopodobieństwa i statystyka matematyczna; przykładowo bardzo często złamanie szyfru (a przynajmniej odczytanie przechwyconego kryptogramu) umożliwia analiza częstości występujących w nim znaków.*

Przykład 2. *Przypuśćmy, że otrzymaliśmy informację, iż przechwycony przez nas kryptogram jest zaszyfrowany opisaną wyżej metodą przesunięcia cyklicznego, a nie jest nam znany klucz, a więc nie wiemy, o ile liter następuje przesunięcie w trakcie szyfrowania poszczególnych liter alfabetu 26 literowego. By wykryć dokładną postać tego przesunięcia, musimy wyliczyć b w równaniu $f(p) = p+b \bmod 26$. Możemy to zrobić przy użyciu analizy częstości. Przypuśćmy, że $\mathsf{S} = 18$ jest najczęściej występującą literą w kryptogramie. Wówczas uzasadnione jest podejrzenie, że litera ta szyfruje najczęściej występującą literę w tekstach napisanych w danym języku. W języku angielskim byłoby to $\mathsf{E} = 4$ (w języku polskim najczęściej występuje litera* A*). Możemy zatem sprawdzić to podejrzenie przez przeliczenie $18 = 4 + b \bmod 26$, skąd $b = 14$, co daje nam funkcję szyfrującą postaci*

$$f(p) = p + 14 \bmod 26.$$

Odpowiadająca jej funkcja deszyfrująca ma postać

$$f^{-1}(p) = p + 12 \bmod 26.$$

Stosując ją do całego kryptogramu możemy się upewnić, czy mieliśmy rację, jeżeli w efekcie uzyskamy tekst jawny, który będzie miał treść dla nas zrozumiałą.

Te proste szyfry polegające na przesunięciu cyklicznym są przykładem szyfrów mono-alfabetycznych. *W takich szyfrach pojedynczy znak kryptogramu reprezentuje dokładnie jeden znak tekstu jawnego. Takie szyfry nie są specjalnie skomplikowane i bardzo łatwe do złamania. Prawdę mówiąc, szyfr Cezara przy zastosowaniu dowolnego z 25 kluczy można złamać w sposób całkiem banalny, poprzez wypróbowanie wszystkich 25 możliwości, co pewnie byłoby szybsze od stosowania opisanej wyżej analizy częstości.*

Pewną komplikację wprowadzi zastosowanie funkcji szyfrującej postaci

$$f(p) = ap + b \bmod 26.$$

Najpierw musimy rozstrzygnąć, kiedy istnieje funkcja deszyfrująca f^{-1}. Będzie ona istnieć wtedy, gdy potrafimy zawsze rozwiązać względem p równanie

$$c = ap + b \bmod 26.$$

Sprowadza się to do rozwiązania kongruencji

$$ax \equiv c - b \pmod{26},$$

co jest możliwe wtedy, gdy $\mathrm{nwd}(a, 26) = 1$. *Jeśli mamy do czynienia z taką sytuacją, to oznaczywszy przez* a^{-1} *rozwiązanie tej kongruencji dostajemy*

$$f^{-1}(p) \equiv a^{-1}(p - b) \pmod{26},$$

czyli

$$f^{-1}(p) = a^{-1}(p - b) \bmod 26,$$

Szyfr takiej postaci nazywamy szyfrem afinicznym.

Przykład 3. *Rozważmy szyfr afiniczny określony przez funkcję* $f(p) = ap+b \bmod 26$. *By móc pracować w takim systemie, musimy obrać takie* $a \in \mathcal{Z}_{\in\prime}$ *które jest elementem odwracalnym tego pierścienia. Możliwe to jest jedynie wtedy, gdy* $\mathrm{nwd}(a, 26) = 1$. *Wiedząc o tym, możemy obrać* $a = 5$, *gdyż* $\mathrm{nwd}(5, 26) = 1$. *Łatwo też sprawdzić, że* $a^{-1} = 21$. *Zatem obieramy przekształcenie szyfrujące postaci* $f(p) = 5p + 3 \bmod 26$. *W tej sytuacji słowo* ALGEBRA *zakoduje się ciągiem liczb* $3, 6, 7, 23, 8, 10, 3$, *co w efekcie daje wyraz* DGHXIKD. *Przekształcenie deszyfrujące otrzymuje postać*

$$f^{-1}(p) = 21(p - 3) \bmod 26 = 21p + 15 \bmod 26$$

Kryptosystem stałby się bezpieczniejszy, gdyby dany znak w kryptogramie mógł reprezentować więcej niż jeden znak z tekstu otwartego. By podać przykład tego typu kryptosystemu, rozpatrzmy tzw. szyfr typu polialfabetycznego. *W tym celu uogólnimy szyfry afiniczne poprzez zastosowanie macierzy. Idea jest z grubsza ta sama, co poprzednio, jednakże zamiast szyfrować po jednej literze, będziemy brać za każdym razem parę znaków. Taką parę* p_1, p_2 *możemy zapisać w postaci wektora*

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

Niech $\mathcal{A}$ *będzie odwracalną macierzą kwadratową typu* 2×2 *o wyrazach z pierścienia* $\mathcal{Z}_{26}$. *Możemy teraz zdefiniować przekształcenie szyfrujące wzorem*

$$f(\mathbf{p}) = \mathcal{A}\mathbf{p} + \mathbf{b},$$

gdzie $\mathbf{b}$ *jest ustalonym wektorem, zaś operacje macierzowe wykonujemy nad pierścieniem* $\mathcal{Z}_{26}$. *Przekształcenie deszyfrujące musi mieć postać*

$$f^{-1}(\mathbf{p}) = \mathcal{A}^{-1}\mathbf{p} - \mathcal{A}^{-1}\mathbf{b}.$$

Przykład 4 *Przypuśćmy, że chcemy zaszyfrować słowo* HELP. *Odpowiadający mu ciąg liczb ma postać* $7, 4, 11, 15$. *Jeżeli weźmiemy*

$$\mathcal{A} = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix},$$

wówczas

$$\mathcal{A}^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}.$$

Jeśli przyjmiemy $\mathbf{b} = (2, 2)^t$, *to kryptogram odpowiadający naszej wiadomości ma postać* RRCR. *Jak widać, litera* R *nie ma w tym tekście jednoznacznego przyporządkowania któremuś ze znaków tekstu jawnego.*

Jednak i w przypadku tego szyfru można by się posłużyć analizą częstości, gdyż występowanie digramów *czyli par znaków jest dość charakterystyczną cechą języka. Przykładowo w języku angielskim niezwykle często występuje zestaw* th, *natomiast para* qz *nie występuje nigdy. Używając większych macierzy, możemy rozkładać informację do szyfrowania na dłuższe bloki, co znacznie utrudnia analizę częstości i efektywność tej analizy, jako że częstości poszczególnych n–gramów stają się bardzo zbliżone w miarę wzrastania n.*

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