Stara Delta

W ramach cyklu Stara Delta prezentujemy przedruki archiwalnych artykułów z naszego miesięcznika, skupiając się na latach 70., 80. i 90. XX wieku, choć artykuły młodsze też się mogą pojawić. Wybór jest subiektywny, a kryteria jego dokonania naprawdę różnorodne.

Wspólnym mianownikiem tego cyklu jest to, że zawsze pytamy współczesnych naukowców o komentarz do proponowanego tekstu. Tu też nic redakcja nie narzuca. Chętnie usłyszymy zarówno polemikę, uwagi merytoryczne, jak i czysto emocjonalne impresje.

Dziś prezentujemy: *Uniwersalny szyfr* (autor trudny do ustalenia) (Δ^1_{80}) oraz *Czy przez telefon można grać w karty?* autorstwa Jerzego Rylla (Δ^{12}_{84}).

Komentarz współczesny

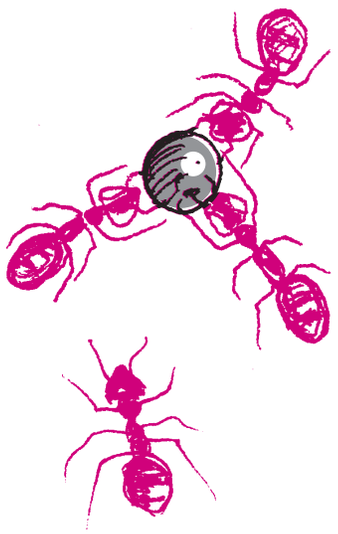
Kilka lat temu zapytałem Mordechaja „Motiego" Yunga (obecnie pracuje jako badacz naukowy w Google) o to, na ile zmienił się obraz badań naukowych z dziedziny kryptologii od czasów, gdy zaczynał, a więc od lat 80. W swej odpowiedzi (wyrażonej dość komunikatywną polszczyzną!) jako największą różnicę wskazał liczbę publikowanych prac. Stwierdził, że w początkach swojej kariery był w stanie, bez większego wysiłku, śledzić na bieżąco WSZYSTKIE artykuły dotyczące kryptologii, które ukazywały się na świecie. Dziś natomiast ciężko byłoby młodemu badaczowi przebrnąć w ciągu roku choćby przez połowę publikacji prezentowanych na jednej dużej konferencji kryptologicznej, których organizuje się przecież co najmniej kilka w roku.

Powyższa opinia Motiego dobrze koresponduje z obecnością kryptologii w *Delcie*. Do końca lat 80. (a więc przez 190 numerów) w *Delcie* ukazały się tylko dwa krótkie teksty dotyczące zagadnień kryptologicznych – oba prezentujemy w tym numerze. Wówczas była to dziedzina dostarczająca przede wszystkim eleganckich (często zaskakujących) wyników-ciekawostek, kojarzonych głównie ze sztuczkami z teorii liczb. W takim też duchu utrzymane są oba dziś prezentowane wyimki ze Starej Delty.

Oczywiście wraz z rozwojem komputerów i sieci komputerowych znaczenie kryptologii wzrosło niebotycznie. Dziś jest to ogromna gałąź informatyki teoretycznej. Również w *Delcie* artykułów z tej dziedziny w późniejszym okresie było znacznie więcej. Ostatnio prezentowaliśmy nawet niemal roczny cykl *A jednak się da* (od Δ^{10}_{18} do Δ^{8}_{19}), poświęcony w całości kryptologii. Co ciekawe: oba zagadnienia z lat 80. były obecne w tym cyklu (choć autorzy wybierali tematy zupełnie niezależnie), a artykuł otwierający cykl dotyczył dokładnie tego samego tematu, co pierwszy artykuł kryptologiczny w *Delcie* z roku 1980!

Tomasz KAZANA

Uniwersalny szyfr



W naszych czasach coraz więcej rzeczy staje się tajnych. To dlatego, że nasze życie jest coraz bardziej uzależnione od setek i tysięcy drobiazgów, a kontrolę nad nimi każdy chce zachować dla siebie. Przyjdzie może czas, kiedy na posiadanie tablic logarytmicznych wymagane będzie zezwolenie. Żarty? Mam nadzieję. Na razie grozi nam utajnienie tablic rozkładów liczb na czynniki pierwsze. A oto dlaczego. Każdy szyfr ma jedną zasadniczą wadę: jeżeli znamy sposób szyfrowania, to i deszyfrowania. Dlatego im więcej osób może przesyłać nam zaszyfrowane wiadomości, tym łatwiej policja rozpracuje naszą siatkę. Nawet, gdy używamy tak doskonałego szyfru, jak ten opisany w przygodach dzielnego wojaka Szwejka (tom III, „Przesławne lanie"). Każdy z nas bez wahania założyłby się, że znajomość sposobu szyfrowania umożliwia odczytanie każdej zaszyfrowanej wiadomości. A tymczasem rzecz ma się trochę inaczej. Oto jak grupa osób może ustalić system szyfrów tak, by

1) każda z osób mogła ogłosić publicznie (na przykład w gazecie): adresowane do mnie wiadomości proszę szyfrować tak a tak. Szyfrowaną wiadomość (adresowana do jednej z osób tej grupy) może wysłać dowolna, niekoniecznie wtajemniczona osoba. Dowolna osoba może ogłosić: przystępuję do spółki; proszę przeznaczone dla mnie wiadomości szyfrować tak a tak,

2) oraz by zaszyfrowanego komunikatu nie mógł odczytać nikt poza adresatem.

Do zbudowania takiego szyfru posłużono się teorią liczb. Oto nieskomplikowane twierdzenie: *Jeżeli liczba naturalna N jest iloczynem dwu liczb pierwszych p, q, to dla $M = (p-1)(q-1)+1$ i dla każdego $n < N$ zachodzi*

$$n^M \equiv n \pmod{N};$$

tj. n^M oraz n dają z dzielenia przez N tę samą resztę.