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

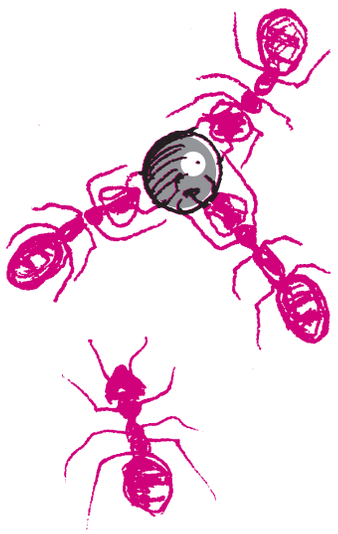
Kilka lat temu zapytałem Mordechaja „Motiego" Yunga (obecnie pracuje jako badacz naukowy w Google) o to, na ile zmienił się obraz badań naukowych z dziedziny kryptologii od czasów, gdy zaczynał, a więc od lat 80. W swej odpowiedzi (wyrażonej dość komunikatywną polszczyzną!) jako największą różnicę wskazał 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,

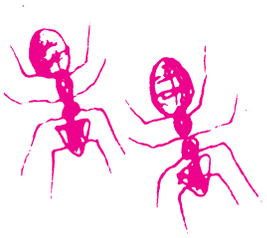
2) oraz by zaszyfrowanego komunikatu nie mógł odczytać nikt poza adresatem.

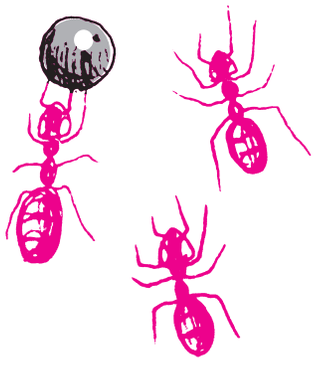
Do zbudowania takiego szyfru posłużono się teorią liczb. Oto nieskomplikowane twierdzenie: *Jeżeli liczba naturalna N jest iloczynem dwu liczb pierwszych p, q, to dla $M = (p-1)(q-1)+1$ i dla każdego $n < N$ zachodzi*

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

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

Stara Delta





Każda z osób, chcących mieć własny szyfr, wybiera sobie dwie dość duże liczby pierwsze (co najmniej kilkudziesięciocyfrowe) p, q, oblicza ich iloczyn N, oraz liczbę $M = (p-1)(q-1)+1$. Do wiadomości ogólnej podaje N i pewien dzielnik liczby M, oznaczmy go przez K. Dla siebie zachowuje rozkład N na p i q oraz liczbę M. Gdy nadawca NAD chce wysłać wiadomość do odbiorcy ODB, postępuje tak. Zamienia tekst słowny na ciąg cyfr w jakiś standardowy, ustalony i jawny sposób, np. $A = 1$, $B = 2$ itd. Otrzymaną tak dużą liczbę (komunikat nie może być długi) podnosi do potęgi K_{ODB} i bierze resztę z dzielenia przez N_{ODB}. Potrzebna jest do tego maszyna matematyczna, ale nic ponadto. Tak zakodowaną wiadomość (będącą teraz liczbą mniejszą niż N_{ODB}) wysyła się do odbiorcy lub publikuje w gazecie. Odbiorca winien podnieść tę liczbę do potęgi $\frac{M_{\mathrm{ODB}}}{K_{\mathrm{ODB}}}$ – otrzyma wtedy ciąg liczb wysłany przez nadawcę. Przetworzenie go na tekst słowny odbywa się we wspomniany jawny i standardowy sposób. Co w tym takiego rewelacyjnego? – zapytacie. A to, że podniesienie nawet bardzo dużej liczby do bardzo dużej potęgi M jest dla maszyny matematycznej mało pracochłonne, zwłaszcza że wszystkie obliczenia robi się i tak modulo N. Wynik dostaje się w ułamku sekundy. Osoba postronna nie zna jednak liczby M; mogłaby ją obliczyć, znając p i q. Ale zna tylko N, równe pq. Gdy p i q mają po kilkadziesiąt cyfr, N ma sto kilkadziesiąt. Znalezienie rozkładu takiej liczby na czynniki nawet najszybciej działającej maszynie zajęłoby (przy obecnym stanie techniki, informatyki i organizacji maszyn cyfrowych) wiele, wiele lat pracy. Szyfr ten nie daje się złamać najgroźniejszą bronią: analizą statystyczną, rozpracowującą szybko wszystkie szyfry polegające na stałym przyporządkowaniu litera-liczba. Autorzy tego szyfru napisali (w *Scientific American*), że są niezbicie pewni, iż nikt nie potrafi odczytać zaszyfrowanej przez nich do samych siebie wiadomości.

Czy przez telefon można grać w karty?

Na podstawie artykułu *Poker bez kart* z książki „The Mathematical Gardner” (A. Shamir, R. Rivest, L. Adelman).

O telefonicznej czy korespondencyjnej grze w szachy słyszał każdy. Ale jak grać w ten sposób w brydża lub w pokera? Problemem jest oczywiście rozdawanie kart. Przypuśćmy, że grają dwie osoby i mają rozdać po pięć kart. Rozdać to znaczy:

Każdy ma wiedzieć, jakie pięć kart dostał.

Karty otrzymane przez graczy są różne.

Żaden z graczy nie ma dodatkowej informacji o kartach partnera, ale po grze może sprawdzić, czy partner nie oszukiwał, czy grał swoimi kartami.

Każdy rozkład kart jest jednakowo prawdopodobny.

Wszystko to należy wykonać porozumiewając się wyłącznie przez telefon i bez pomocy osób trzecich. Oto sposób umożliwiający w praktyce rozdawanie kart (liczb naturalnych $1, \ldots, 52$) przez telefon. Gracze wybierają najpierw dwie rodziny funkcji o argumentach i wartościach naturalnych: $\mathscr{K} = \{K_\alpha : \alpha \in \Omega\}$ – funkcje kodujące i $\mathscr{D} = \{D_\alpha : \alpha \in \Omega\}$ – funkcje dekodujące (zbiór Ω nazywamy zbiorem kodów – powinien on mieć dużo elementów). Rodziny $\mathscr{K}$ i $\mathscr{D}$ muszą mieć następujące własności:

Dziedzina każdej funkcji K_α zawiera zbiór $\{1, \ldots, 52\}$.

Dla dowolnego kodu α funkcja $\mathscr{D}_\alpha$ jest odwrotna do funkcji K_α (rozszyfrowuje ona sygnał zakodowany za pomocą funkcji K_α), tzn. $D_\alpha(K_\alpha(n)) = n$ dla liczb naturalnych z dziedziny funkcji K_α.

Dla dowolnych kodów α i β funkcje K_α i K_β są przemienne, tzn. $K_\alpha(K_\beta(n)) = K_\beta(K_\alpha(n))$.

Różne funkcje kodujące mają rozłączne zbiory wartości.

Znajomość liczb naturalnych n i $K_\alpha(n)$ nie daje *praktycznie* możliwości znalezienia kodu α.

Rozdawanie kart jest już proste. Gracze wybierają (w tajemnicy przed sobą) kody, np. A – kod α, B – kod β. Gracz A koduje liczby $1, \ldots, 52$ i przesyła je (w dowolnej kolejności) graczowi B. Ten wybiera wpierw pięć kart dla A: $K_\alpha(a_1), \ldots, K_\alpha(a_5)$ i odsyła mu je – A musi je rozszyfrować funkcją D_α. Następnie wybiera pięć kart dla siebie: $K_\alpha(b_1), \ldots, K_\alpha(b_5)$, szyfruje je funkcją K_β i wysyła do A. Gracz A rozszyfrowuje je funkcją D_α i odsyła do gracza B (tzn. przesyła $D_\alpha(K_\beta(K_\alpha(b_1)) = D_\alpha K_\alpha K_\beta(b_1) = K_\beta(b_1))$. Gracz B musi jeszcze rozszyfrować je funkcją D_β i ... karty zostały rozdane.

Po grze partnerzy ujawniają swoje kody. Z drugiej i czwartej własności rodzin $\mathscr{K}$ i $\mathscr{D}$ wynika, że jeśli $K_{\alpha_1}(m_1) = K_{\alpha_2}(m_2)$, to $\alpha_1 = \alpha_2$ i $m_1 = m_2$. Tak więc gracze nie mogą oszukiwać i podawać innego układu kart i innego kodu.

Powyższy opis umożliwia w *praktyce* rozdawanie kart. *Teoretycznie* bowiem jest to niemożliwe.

Jerzy RYLL