A jednak się da (IV),

czyli saga kryptologiczna w odcinkach.

Tym razem: odtajniamy transfer utajniony

Łukasz RAJKOWSKI

Ence-pence w której ręce? – za moich dziecięcych lat przedstawiona formułka, której towarzyszyły często dwie wyciągnięte przez wypowiadającą ją osobę ręce, była zwiastunem jakiejś bardzo przyjemnej (najczęściej słodkiej) niespodzianki. Każda wyciągnięta dłoń skrywała bowiem coś dobrego, jednak jako szkrab i tak poświęcałem chwilę zastanowienia nad jej wyborem, będąc świadomym ryzyka, że niewskazana przeze mnie ręka zawiera bardziej atrakcyjny podarek i powędruje on do mojego brata. Ta dziecięca wyliczanka będzie dla nas punktem wyjścia do rozważań nad problemem pozornie niemającym zastosowania w rzeczywistości. Zapytajmy bowiem, czy dziecko jest w stanie dowiedzieć się, co znajduje się w wybranej przez nie ręce, tak aby spełnione były dwa warunki:

1. dziecko nie dowiaduje się, co znajduje się w drugiej ręce rodzica,
2. rodzic nie dowiaduje się, którą rękę wybrało dziecko.

Powyższe założenia wydają się sprzeczne, a procedura, która miałaby je spełniać, zakrawa o sztuczkę magiczną. Jest to jednak możliwe – stosowny protokół nazywa się *transferem utajnionym*. Pisał o nim Tomasz Kazana w *Delcie* 5/2012. Transfer utajniony jest jednak na tyle ważną „cegiełką” kryptograficzną, że dla pełności naszego cyklu postanowiliśmy przypomnieć go w tym krótkim artykule.

Rozpocznijmy od przedstawienia naszego problemu w bardziej matematycznym języku. Aby biedny rodzic nie musiał utrzymywać przez cały czas rąk w górze, załóżmy, że przyporządkowuje on wartości dwóm zmiennym: x_0 (lewa ręka) i x_1 (prawa ręka); dla ułatwienia opisu załóżmy, że wartości te są liczbami naturalnymi. Dziecko wybiera natomiast $s \in \{0,1\}$. Jego zadaniem jest poznanie wartości x_s bez ujawniania s, natomiast rodzic nie może wyjawić wartości x_{1-s}.

Pierwszym krokiem protokołu jest stworzenie bazy do szyfrowania z kluczem publicznym, tak jak opisane to zostało w pierwszym odcinku serii, opublikowanym w *Delcie* 10/2018. Rodzic wybiera dwie duże liczby pierwsze p, q tak, aby $n = pq$ było większe od każdej z liczb x_0 i x_1. Następnie rodzic oblicza $m = (p-1)(q-1)$ i znajduje takie dwie liczby naturalne e i d, że $ed \equiv 1 \pmod m$ (tzn. ed daje resztę 1 z dzielenia przez m). Ponadto rodzic losuje liczby y_0 i y_1 i wyjawia dziecku wartość każdej z nich. Dziecko natomiast losuje liczbę k, której nigdy nie ujawni rodzicowi. Zamiast tego przesyła mu wartość $v = (y_s + k^e \bmod n)$. Na jej podstawie rodzic oblicza $k_0 = \big((v-y_0)^d \bmod n\big)$ oraz $k_1 = \big((v-y_1)^d \bmod n\big)$. Zauważmy, że wówczas $k_s = (k^{ed} \bmod n) = k$ (po szczegóły odsyłamy do pierwszej części sagi). Jeśli zatem rodzic prześle dziecku wartości $\tilde{x}_0 = x_0 + k_0$ oraz $\tilde{x}_1 = x_1 + k_1$, to dziecko będzie mogło obliczyć wartość $x_s = \tilde{x}_s - k$.

Wiemy już, że w opisany wyżej sposób dziecko poznaje wartość x_s. Jedyna informacja, jaką rodzic dostaje od dziecka, to wartość v. Na jej podstawie rodzic nie jest w stanie powiedzieć niczego o s ze względu na losowy wybór k. Pozostaje wykazać, że dziecko nie jest w stanie obliczyć wartości x_{1-s}. Zauważmy, że

$$(\tilde{x}_{1-s} - x_{1-s})^e \equiv k_{1-s}^e \equiv \big((y_s + k^e - y_{1-s})^d\big)^e \equiv y_s + k^e - y_{1-s} \pmod n.$$

Ponieważ y_0 i y_1 były losowane przez rodzica, to z punktu widzenia dziecka liczba $y_s + k^e + y_{1-s}$ jest losowa. Gdyby dziecko potrafiło obliczyć x_{1-s}, to ponieważ zna $\tilde{x}_{1-s}$ – potrafiłoby obliczyć lewą stronę powyższej równości. Rozwiązałoby zatem równanie $a^e \equiv b \pmod n$ dla losowo wybranej wartości b. Z pierwszego odcinka sagi wiemy, że zadanie to jest równie trudne, co złamanie szyfru RSA, jeśli zatem wierzymy w bezpieczeństwo tego ostatniego, nie powinniśmy mieć skrupułów w używaniu przedstawionego protokołu transferu ujawnionego. A o tym, że kryptologia opiera się na wierze (lecz również zrozumieniu!) pisaliśmy już w *Delcie* niejednokrotnie...

Rozwiązanie zadania F 969.
Zgodnie z prawem Hooke'a ciało o długości h i powierzchni przekroju poprzecznego S pod wpływem rozciągającej je siły F doznaje względnego wydłużenia

$$\frac{\Delta h}{h} = \frac{F}{YS}.$$

Podzielmy długość L rury na n jednakowych odcinków wysokości h. Każdy z tak otrzymanych odcinków rury będzie ściskany ciężarem znajdującej się nad nim części rury, a więc zmiana długości odcinka i – numerujemy od górnego końca rury – wyniesie:

$$\Delta h_i = -h\frac{(i-1)\,hS\rho g}{YS}$$

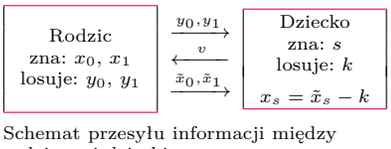
(znak minus, bo chodzi o siłę ściskającą). Całkowitą zmianę długości otrzymamy, sumując wszystkie Δh_i. Obliczenie sumy szeregu arytmetycznego prowadzi do wyrażenia:

$$\Delta L = \sum_{i=1}^{n} \Delta h_i = -\frac{L^2\rho g(n^2-n)}{2n^2Y}.$$

Przechodząc z n do nieskończoności, otrzymujemy:

$$\Delta L \xrightarrow[n\to\infty]{} -\frac{L^2\rho g}{2Y}.$$

Dla danych zadania $\Delta L = -1,9\cdot 10^{-4}\,\mathrm{m} \approx -0,2\,\mathrm{mm}$.



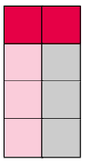
Schemat przesyłu informacji między rodzicem i dzieckiem.

Parkietaże

*Michał ADAMASZEK**

* MOSEK ApS, Kopenhaga

W autorskim tygodniku internetowym *Trapez* [1] Jarosław Wróblewski proponuje serię zadań (nr 75–126) o parkietowaniu prostokątów. Na przykład: czy planszę 15×15 da się szczelnie pokryć klockami o wymiarach 8×1, 1×8, 11×1 oraz 1×11 (oczywiście klocki nie mogą na siebie zachodzić). W tego typu zadaniach odpowiedź zazwyczaj brzmi „nie”, a typowa strategia polega na zgadnięciu numeracji lub kolorowania pól planszy i użyciu argumentu w stylu „każdy klocek pokrywa trzy pola zielone, ale liczba pól zielonych na całej planszy jest niepodzielna przez 3”. Spróbujmy jednak ogólniej zastanowić się, jak systematycznie, od podstaw, można zaatakować problem: czy planszę o wymiarach $n \times m$ da się wyparkietować klockami ustalonych typów $a_1 \times b_1, \ldots, a_\ell \times b_\ell$.



Przykład parkietażu

Niech (i, j) oznacza pole w i-tym wierszu i j-tej kolumnie. Każde pokrycie planszy możemy zakodować za pomocą zmiennych

$$x_{i,j}^{a\times b} = \begin{cases} 1 & \text{jeśli pewien klocek typu } a \times b \text{ ma lewy górny róg na polu } (i,j), \\ 0 & \text{wpp.} \end{cases}$$

Na przykład pokrycie planszy 4×2 z rysunku obok opisujemy następująco:

$$x_{1,1}^{1\times 2} = x_{2,1}^{3\times 1} = x_{2,2}^{3\times 1} = 1,$$

a wszystkie inne zmienne $x_{i,j}^{a\times b}$ są równe zero.

Zapytajmy teraz, kiedy zestaw zmiennych $x_{i,j}^{a\times b}$ opisuje poprawny parkietaż. Przede wszystkim musimy usunąć wszystkie zmienne

$$x_{i,j}^{a\times b} \text{ dla } i > n+1-a \text{ lub } j > m+1-b,$$

ponieważ klocek o wymiarach $a \times b$ z lewym górnym rogiem na polu (i, j) wystawałby poza planszę. Po drugie, wszystkie zmienne muszą przyjmować wartości 0 lub 1. W końcu, musimy zagwarantować, że każde pole planszy jest pokryte przez dokładnie jeden klocek. Ten warunek można zapisać następująco:

$$\sum_{k=1}^{\ell} \sum_{i'=\max(1,i-a_k+1)}^{\min(i,n-a_k+1)} \sum_{j'=\max(1,j-b_k+1)}^{\min(j,m-b_k+1)} x_{i',j'}^{a_k\times b_k} = 1 \tag{1}$$

dla każdego $i = 1, \ldots, n,\ j = 1, \ldots, m$. Ten nieprzyjemny wzór oznacza po prostu, że spośród wszystkich legalnych położeń dostępnych klocków, które potencjalnie mogą zahaczać o pole (i, j), dokładnie jedno jest faktycznie w użyciu. A zatem zerojedynkowe rozwiązania układu nm równań liniowych (1) odpowiadają jednoznacznie parkietażom.

Dla zupełnej jasności rozważmy przykład. Zapiszmy w tym języku problem parkietowania planszy 3×4 klockami typu 1×3 i 2×1. Mamy 12 równań, z których każde wymienia legalne sposoby pokrycia jednego z pól:

$$\begin{aligned}
&(1,1)\ x_{1,1}^{1\times 3} + x_{1,1}^{2\times 1} = 1 \\
&(1,2)\ x_{1,1}^{1\times 3} + x_{1,2}^{1\times 3} + x_{1,2}^{2\times 1} = 1 \\
&(1,3)\ x_{1,1}^{1\times 3} + x_{1,2}^{1\times 3} + x_{1,3}^{2\times 1} = 1 \\
&(1,4)\ x_{1,2}^{1\times 3} + x_{1,4}^{2\times 1} = 1 \\
&(2,1)\ x_{2,1}^{1\times 3} + x_{1,1}^{2\times 1} + x_{2,1}^{2\times 1} = 1 \\
&(2,2)\ x_{2,1}^{1\times 3} + x_{2,2}^{1\times 3} + x_{1,2}^{2\times 1} + x_{2,2}^{2\times 1} = 1 \\
&(2,3)\ x_{2,1}^{1\times 3} + x_{2,2}^{1\times 3} + x_{1,3}^{2\times 1} + x_{2,3}^{2\times 1} = 1 \\
&(2,4)\ x_{2,2}^{1\times 3} + x_{1,4}^{2\times 1} + x_{2,4}^{2\times 1} = 1 \\
&(3,1)\ x_{3,1}^{1\times 3} + x_{2,1}^{2\times 1} = 1 \\
&(3,2)\ x_{3,1}^{1\times 3} + x_{3,2}^{1\times 3} + x_{2,2}^{2\times 1} = 1 \\
&(3,3)\ x_{3,1}^{1\times 3} + x_{3,2}^{1\times 3} + x_{2,3}^{2\times 1} = 1 \\
&(3,4)\ x_{3,2}^{1\times 3} + x_{2,4}^{2\times 1} = 1
\end{aligned} \tag{2}$$

Na przykład równanie dla pola $(2, 4)$ czytamy następująco: pole to można przykryć klockiem 1×3 z pola $(2, 2)$ lub klockiem 2×1 z jednego z pól $(1, 4)$ lub $(2, 4)$.

Jak łatwo sprawdzić, prostokąta 3×4 klockami 1×3 i 2×1 pokryć się nie da. Możemy tego faktu dowieść algebraicznie, mianowicie mnożąc równania (2)

Rozwiązanie zadania M 1593.
Skoro $2n-1$ jest liczbą złożoną, to $2n-1 = pq$ dla pewnych (niekoniecznie różnych) liczb nieparzystych p, q większych od 1. Niech

$$a_i = 1 \text{ dla } i = 1, 2, \ldots, p$$

oraz

$$a_i = 2i - 1 - p \text{ dla } i = p+1, p+2, \ldots, n.$$

Wówczas $a_1 < a_2 < \ldots < a_n$.
Jeżeli $1 \leqslant i \leqslant j \leqslant p$, to

$$\frac{a_i + a_j}{\mathrm{NWD}(a_i, a_j)} \leqslant a_i + a_j = i + j \leqslant$$
$$\leqslant 2p < pq = 2n - 1.$$

Jeżeli $p+1 \leqslant i \leqslant j \leqslant n$, to $2 \mid \mathrm{NWD}(a_i, a_j)$, skąd

$$\frac{a_i + a_j}{\mathrm{NWD}(a_i, a_j)} \leqslant \frac{a_i + a_j}{2} = i + j - 1 - p \leqslant$$
$$\leqslant 2n - 1 - p < 2n - 1.$$

Jeżeli $1 \leqslant i \leqslant p$, $p+1 \leqslant j \leqslant n$ oraz $(i, j) \neq (p, n)$, to

$$\frac{a_i + a_j}{\mathrm{NWD}(a_i, a_j)} \leqslant a_i + a_j =$$
$$= i + 2j - 1 - p <$$
$$< 2n - 1.$$

W końcu jeśli $(i, j) = (p, n)$, to

$$\frac{a_i + a_j}{\mathrm{NWD}(a_i, a_j)} = \frac{pq}{q} = p < 2n - 1.$$