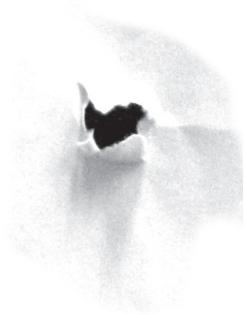
A jednak się da (II),

czyli saga kryptologiczna w odcinkach.
Tym razem: bez zobowiązań o zobowiązaniach.



Łukasz RAJKOWSKI

Zapewne każdy z czytających te słowa grał kiedyś w *marynarza*, ale na wypadek gdyby któryś z Czytelników miał smutne dzieciństwo pozbawione tej gry, pokrótce wyjaśnię zasady: na ustalony sygnał każdy z uczestników przedstawia wybraną przez siebie liczbę (najczęściej przy użyciu własnych palców). Następnie rozpoczyna się (cykliczne) wyliczanie uczestników aż do sumy przedstawionych przez nich liczb (oczywiście, należy zawczasu ustalić, od kogo rozpoczyna się wyliczanka). Osoba, na której zakończy się wyliczanie, jest „zwycięzcą" (wziętym w cudzysłów, gdyż „nagrodą" może być, na przykład, zmywanie naczyń). Niestety, przedstawiona procedura ma pewną techniczną trudność, która była źródłem niejednej podwórkowej kłótni – jeśli któryś z uczestników opóźni się z przedstawieniem swojej liczby, może zostać oskarżony o celową zwłokę, która przy pewnej sprawności rachunkowej mogłaby zostać wykorzystana w celu osiągnięcia z góry założonego wyniku gry. Aby tego uniknąć, uczestnicy mogliby zapisywać wybrane przez siebie liczby na kartkach, które wrzucane byłyby do jednego worka. Co jednak począć w sytuacji, kiedy taka operacja nie jest możliwa, na przykład gdybyśmy chcieli zagrać w marynarza przez telefon (lub raczej, ze względu na potencjalnie dużą liczbę uczestników, gdybyśmy chcieli to uczynić, prowadząc grupową konwersację na pewnym popularnym serwisie społecznościowym)? Okazuje się, że wciąż jest to możliwe; wystarczy użyć kryptologicznego narzędzia zwanego *zobowiązaniem*.

Aldonę i Bogumiła przedstawiliśmy już w pierwszej części naszej sagi, traktującej o szyfrowaniu z kluczem publicznym.

Kryptologiczne zobowiązanie jest „skrzynką", do otwarcia której potrzebny jest klucz. Najczęściej zamykamy w niej wiadomość, wysyłamy całość nadawcy, a po pewnym czasie dosyłamy mu klucz (gdy uznamy, że może on już zapoznać się z zawartością). Dokonujemy jednak w ten sposób pewnego zobowiązania – nie mamy do dyspozycji kilku różnych kluczy o tej własności, że w zależności od użytego klucza skrzynka odsłoni adresatowi inną zawartość. Opisana przed chwilą skrzynka reprezentowana jest przez funkcje `Commit` i `Open` takie, że jeśli Aldona chce „zobowiązać się" Bogumiłowi do wiadomości m, oblicza $(c,k) = \texttt{Commit}(m)$ i wysyła mu c. Aby odkryć zobowiązanie, musi ona jeszcze dosłać k, dzięki czemu Bogumił oblicza $m' = \texttt{Open}(c,k)$. Aby protokół był poprawny, muszą być spełnione następujące warunki:

(i) $\texttt{Open}(\texttt{Commit}(m)) = m$ (dzięki czemu Bogumił odczytuje m po dosłaniu klucza),
(ii) sama znajomość c nie dostarcza żadnej informacji o m,
(iii) Aldona nie może skonstruować takich dwóch kluczy k_1, k_2, że $\texttt{Open}(c,k_1) \neq \texttt{Open}(c,k_2)$.

Podobnie jak w poprzednim odcinku sagi, możemy dostrzec pewien szkopuł w przedstawionych warunkach. Podpunkty (ii) i (iii) nie mogą być bowiem spełnione jednocześnie. Istotnie, z punktu (iii) wynika, że istnieje tylko jedna wartość klucza k, dla której $\texttt{Open}(c,k)$ jest sensowną wiadomością – Bogumił po odebraniu wiadomości c mógłby zatem przeglądać wszystkie możliwe wartości kluczy, aż znajdzie ten właściwy. Innymi słowy, c jednoznacznie definiuje m, co przeczy podpunktowi (ii). Musimy zatem zgodzić się na pewien kompromis – któryś ze wspomnianych warunków będzie naruszony, jednak możemy zadbać o to, by realizacja tego naruszenia była bardzo trudna obliczeniowo. W świetle tego spostrzeżenia kryptologiczne zobowiązania możemy podzielić na *bezwarunkowo kryjące* i *bezwarunkowo wiążące*.

Zobowiązania bezwarunkowo kryjące naruszają podpunkt (iii), zatem znajomość c nie mówi zupełnie nic o m, a Aldona teoretycznie mogłaby znaleźć dwa klucze prowadzące do różnych odczytów ze skrzynki, choć będzie to dla niej bardzo trudne obliczeniowo. Przedstawimy przykład protokołu, który realizuje te założenia. Zauważmy najpierw, że wystarczy ograniczyć potencjalne wiadomości do 0 lub 1. Rzeczywiście, dowolnie skomplikowaną informację możemy rozbić na bity i zobowiązać się do każdego z nich z osobna. Aldona wybiera dużą liczbę

Rozwiązanie zadania F 963.
Gdyby prędkość wirowania Ziemi wzrosła, to najsilniejszy efekt tej zmiany byłby obserwowany na równiku. Oszacujmy, przy jakiej prędkości kątowej ω siła odśrodkowa zrównoważyłaby przyciąganie grawitacyjne na równiku:

$$\omega^2 R = g.$$

Biorąc pod uwagę, że $\omega = 2\pi/T$, gdzie T jest poszukiwaną długością najkrótszej doby, otrzymujemy:

$$T = 2\pi\sqrt{\frac{R}{g}} \approx 5000\,\mathrm{s},$$

czyli około 1/17 „obecnej" doby. Na szczęście rotacja Ziemi spowalnia i doba wydłuża się o niecałe 2 ms na stulecie.

Warto podkreślić, że „potęgowanie modulo" jest szybkie. Załóżmy, że chcemy obliczyć $(g^x \bmod p)$. Poprzez podnoszenie poprzednich wyników do kwadratu prędko obliczamy $(g^2 \bmod p), (g^4 \bmod p), (g^8 \bmod p), \ldots, (g^{2^m} \bmod p)$, gdzie $m = \lfloor \log_2 x \rfloor$, a mnożąc odpowiednie z tych reszt, możemy łatwo wyznaczyć $(g^x \bmod p)$.

pierwszą p oraz g niepodzielne przez p, po czym wysyła Bogumiłowi p i g. Bogumił wybiera dowolnie $x < p$ i odsyła Aldonie $s = (g^x \bmod p)$. Aby zobowiązać się do bitu b, Aldona wybiera dowolnie klucz $k < p$ i wysyła Bogumiłowi $c = (s^b g^k \bmod p)$. Widzimy, że liczba otrzymana przez Bogumiła to $(g^{bx+k} \bmod p)$, zatem bez znajomości k nie ma on bladego pojęcia o b. Kiedy jednak Aldona dośle k, sprawa jest dla Bogumiła jasna, wystarczy bowiem, że obliczy $(g^k \bmod p)$ i $(g^{x+k} \bmod p)$ i sprawdzi, która z tych liczb jest równa c. Zastanówmy się teraz, w jaki sposób Aldona mogłaby „oszukać system". Byłoby to równoznaczne ze znalezieniem dwóch kluczy k_1, k_2, przy których Bogumił odczytałby różne wartości b. Spełniona byłaby zatem równość

$$g^{k_1} = sg^{k_2} \pmod p, \quad \text{czyli } g^{k_1-k_2} = s \pmod p.$$

Zadanie dla niedowiarków: do jakiej potęgi należy podnieść 10, aby otrzymać 23428033658 przy dzieleniu przez liczbę pierwszą $10^{11} + 3$? Można korzystać z pomocy komputera.

Oznaczałoby to, że Aldona jest w stanie na podstawie g, s wybranych przez Bogumiła znaleźć l spełniające $g^l = s \pmod p$. Rozwiązałaby zatem problem *logarytmu dyskretnego*, o którym sądzimy, że jest trudny obliczeniowo. Wierzymy zatem, że nie byłaby w stanie dostarczyć dwóch różnych kluczy do wysłanej Bogumiłowi skrzynki.

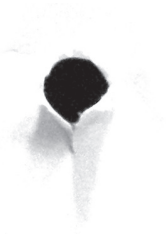
Zobowiązania bezwarunkowo wiążące to takie, w których „skrzynka" może zostać otwarta tylko na jeden sposób, w związku z czym teoretycznie Bogumił mógłby wyznaczyć c na podstawie m. Postaramy się jednak, by w praktyce było to niemożliwe. Aby przedstawić przykład takiego protokołu, przypomnimy (lub nauczymy się) kilku interesujących faktów z teorii liczb.

Niech n będzie liczbą naturalną. *Resztą kwadratową* z dzielenia przez n nazwiemy taką liczbę naturalną r, że istnieje x, dla którego $r = x^2 \pmod n$. Dla przykładu, 2 jest resztą kwadratową z dzielenia przez 7, gdyż $2 = 3^2 \pmod 7$, ale 3 już nią nie jest. Łatwo sprawdzić, czy r jest resztą kwadratową z dzielenia przez liczbę pierwszą p – na mocy *kryterium Eulera* wystarczy obliczyć $(r^{\frac{p-1}{2}} \bmod p)$; już wiemy, że jest to szybkie. Jeśli wyjdzie 1, i tylko w takim przypadku, mamy do czynienia z resztą kwadratową (w przeciwnym przypadku dostajemy -1). Wracając do naszego przykładu, mamy $2^3 = 1 \pmod 7$, ale $3^3 = -1 \pmod 7$. Sprawa komplikuje się, gdy n jest liczbą złożoną (na przykład $n = pq$, gdzie p i q są pierwsze). Wiemy co prawda, że r jest resztą kwadratową z dzielenia przez n wtedy i tylko wtedy, gdy jest resztą kwadratową z dzielenia przez p oraz z dzielenia przez q, jeśli jednak nie dysponujemy rozkładem n na czynniki pierwsze (jak wiemy, dla dużych n jest to trudne obliczeniowo), nie mamy do dyspozycji tak wygodnego warunku, jak kryterium Eulera dla liczb pierwszych. Decyzja, czy dana liczba jest resztą kwadratową względem dużej liczby złożonej, uznawana jest za trudną obliczeniowo, co wykorzystamy poniżej.

O kryterium Eulera piszemy więcej w następnym numerze.

Oto, co powinna tym razem zrobić Aldona, aby zobowiązać się do bitu b. Podobnie, jak w opisanym w poprzedniej części sagi protokole RSA, wybiera ona dwie duże liczby pierwsze p, q i oblicza $n = pq$. Jeśli chce zobowiązać się do 1, wybiera r będące resztą kwadratową z dzielenia przez n. Wybór r **nie**będącego resztą kwadratową z dzielenia przez n oznacza zobowiązanie do 0. Sposób wyboru odpowiedniego r polega na „losowaniu do skutku" – nietrudno wykazać, że nie trzeba zbyt długo czekać na sukces, a ponieważ Aldona zna liczby p, q, jest w stanie rozstrzygać, czy wylosowane liczby są resztami kwadratowymi z dzielenia przez n. Następnie Aldona wysyła Bogumiłowi liczby n, r. Aby przekonać się o wartości b, Bogumił musiałby rozstrzygnąć, czy r jest resztą kwadratową z dzielenia przez n; wiemy już, że jest to dla niego trudne, gdyż nie zna on rozkładu n na czynniki pierwsze. Oczywiście, w ramach klucza Aldona wysyła Bogumiłowi liczby p, q; wówczas bez trudu sprawdza on „kwadratowość" reszty r względem każdego z czynników pierwszych, tym samym odczytując zobowiązanie Aldony.

Kolejne zadanie, do rozwiązania którego można wykorzystać komputer: czy 10 jest resztą kwadratową z dzielenia przez 151951844572340170652293?



A tak na poważnie, po co to wszystko?

Oczywiście, przedstawienie gry w marynarza jako przykładu zastosowania kryptologicznych zobowiązań miało raczej żartobliwy charakter. Poważniejszym wykorzystaniem są przetargi; łatwo wyobrazić sobie, dlaczego zobowiązania są bardzo pożyteczne w tym kontekście. Tak naprawdę jednak waga tego narzędzia jest związana z faktem, że jest bardzo wygodną „cegiełką" stosowaną przy konstrukcji innych kryptologicznych protokołów. Protokoły te często mają bardzo nieoczekiwane własności – będziemy o nich pisać w kolejnych odcinkach cyklu „A jednak się da!".