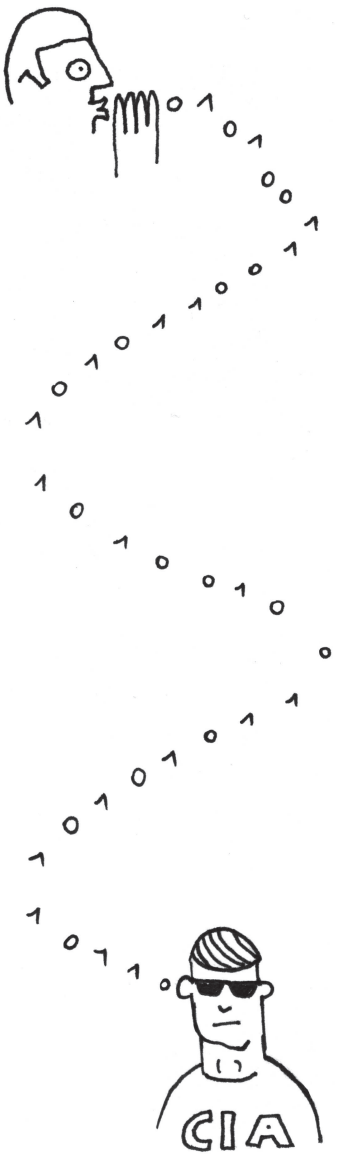
Tajemnica

Mam pewien sekret, może lepiej nawet powiedzieć: tajemnicę. Nie mogę sobie pozwolić, żeby ktoś ją poznał. Sprawa jest poważna, ujawnię ją dopiero za pewien czas, gdy tylko Świat będzie na to gotowy. Może to rozwiązanie pewnego ważnego problemu matematycznego, zresztą, nie będę dzwonił kluczami do tajemnic. W każdym razie nie mogę sobie również pozwolić, żeby na wypadek mojej śmierci ta informacja przepadła bezpowrotnie. Co robić?



Na szczęście, opracowałem pewien plan. Podzielę się tą informacją ze służbami specjalnymi. Wybrałem trzy: ABW, CIA i Mosad. Czy mogę jednak w pełni ufać służbom specjalnym? Chyba nie. Dlatego chcę dostarczyć im takie informacje, żeby żadna pojedyncza instytucja nie mogła samodzielnie odkryć nawet kawałka mojej tajemnicy. Co więcej, chcę to zrobić tak, by nawet dwie z nich, jeśli się potajemnie zmówią, nie zdołały odtworzyć ani litery z mojego sekretu. System musi być taki, że dopiero gdy wszystkie trzy służby udostępnią sobie dostarczone przeze mnie informacje, będą w stanie odtworzyć cokolwiek z tajemnicy. Co więcej, chcę, żeby wówczas odtworzyły już wszystko, bo mam nadzieję, że stanie się to jedynie na wypadek mojej śmierci.

Pozostaje pytanie: jak to zrobić? A może nawet właściwsze w tej sytuacji: czy to się w ogóle da zrobić? Okazuje się, że szczęśliwie się da. Zachęcam Ambitnych Czytelników do próby samodzielnego stworzenia takiego systemu.

A robi się to tak. Przedstawiam mój sekret w postaci ciągu zero-jedynkowego. Bitem będziemy nazywać dowolną cyfrę takiego ciągu, czyli zero lub jedynkę. Nietrudno zauważyć, że mogę znaleźć takie przedstawienie bez problemu, na przykład każdą literę alfabetu przedstawiam w postaci ciągu sześciu bitów, da się to zrobić, bo liter alfabetu jest nie więcej niż $2^6 = 64$. Teraz mogę się więc skupić na tym, jak podzielić pewien ciąg bitów na trzy kawałki. Nie mogę po prostu przekazać pierwszej jednej trzeciej ABW, drugiej CIA, a trzeciej Mosadowi, bo w sposób oczywisty bez wysiłku każdy z nich znałby sporą część tajemnicy.

Żeby wyjaśnić system, konieczne jest zdefiniowanie funkcji `xor`, która jako argumenty bierze pewną liczbę bitów, a zwraca jeden. Definiujemy ją jako

$$\texttt{xor}(b_1, \ldots, b_k) = (b_1 + \cdots + b_k) \mod 2,$$

czyli resztę z dzielenia sumy bitów przez dwa. Możemy rozszerzyć funkcję `xor` w taki sposób, że jako argumenty bierze ona pewną liczbę ciągów bitowych jednakowej długości, powiedzmy dla ustalenia uwagi, długości m. Wtedy

$$\texttt{xor}(w_1, \ldots, w_k) = \texttt{xor}(w_1[1], \ldots, w_k[1]) \ldots \texttt{xor}(w_1[m], \ldots, w_k[m]),$$

gdzie przez $w[i]$ oznaczamy i-tą literę słowa w. Czyli, innymi słowy, nowy `xor` po prostu xoruje argumenty litera po literze. Przykładowo

$$\texttt{xor}(11001, 01000, 10111) =$$
$$= \texttt{xor}(1,0,1)\,\texttt{xor}(1,1,0)\,\texttt{xor}(0,0,1)\,\texttt{xor}(0,0,1)\,\texttt{xor}(1,0,1) = 00110.$$

A teraz system – jest banalnie prosty! Powiedzmy, że moja tajemnica przedstawiona w postaci ciągu bitów ma długość m. Jej wartość oznaczmy przez t. Najpierw losuję dwa losowe ciągi bitów w_1 i w_2 długości m, to będą te przeznaczone dla ABW i CIA. Teraz definiuję trzeci ciąg, dla Mosadu, $w_3 = \texttt{xor}(w_1, w_2, t)$. Tylko dlaczego to działa?

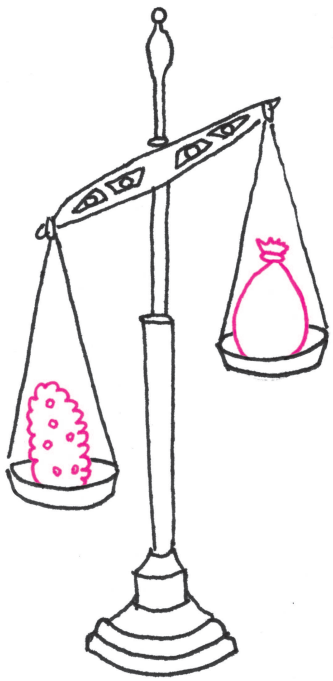
Zauważmy najpierw, że $t = \texttt{xor}(w_1, w_2, w_3)$. Żeby się przekonać, że to prawda, spójrzmy na i-ty bit. Wiemy, że $w_3[i] = \texttt{xor}(w_1[i], w_2[i], t[i])$. A więc suma $w_1[i]$, $w_2[i]$, $t[i]$ oraz $w_3[i]$ jest parzysta. Z tego zaś wynika, że $\texttt{xor}(w_1[i], w_2[i], w_3[i]) = t[i]$. Gdy powtórzymy rozumowanie dla każdego i między 1 a m, otrzymamy, że faktycznie $t = \texttt{xor}(w_1, w_2, w_3)$. Czyli ABW, CIA i Mosad współpracując, mogą odtworzyć moją tajemnicę.

Trzeba jednak jeszcze sprawdzić, czy istotnie żadne dwie służby bez trzeciej łącząc swoje siły, nie będą w stanie odkryć żadnej informacji. Jasne jest, że ABW i CIA mają ciągi losowe, więc nie zrobią z nimi niczego sensownego bez Mosadu. Pozostają pozostałe pary – skupmy się na parze CIA i Mosad, bo sytuacja jest identyczna dla pary ABW i Mosad. Przyjrzyjmy się i-temu bitowi. Wyobraźmy sobie, że CIA i Mosad patrzą na swoje bity i widzą $w_2[i] = 0$, $w_3[i] = 0$. To im jednak nie daje żadnej wiedzy o $t[i]$, bo może być tak, że $w_1[i] = 0 = t[i]$ oraz tak, że $w_1[i] = 1 = t[i]$ – każda z tych dwóch opcji jest równie prawdopodobna. Podobnie dla każdej kombinacji $w_2[i]$ i $w_3[i]$ oraz dla każdego innego indeksu i. Polecamy Czytelnikom Ambitnym doprecyzowanie tego argumentu.

Nietrudno zauważyć, że opisany system da się uogólnić na dowolne N służb. Jeszcze ciekawszym pytaniem jest, co zrobić, gdy chcę, by dowolne K z N służb, spotykając się, odtworzyło całą tajemnicę, ale już żadne $K-1$ służb nie mogło odkryć niczego. Wtedy potrzebne są bardziej zaawansowane techniki, pisaliśmy o tym w *Delcie* 2/2011.

Przygotował Wojciech CZERWIŃSKI

Sprawiedliwie, sprawiedliwiej, najsprawiedliwiej



Pewnego słonecznego lipcowego poranka Alfred i Berenika ochoczo wybrali się na gdańską plażę. Mieli nadzieję, że wczorajsza burza przysporzy im mnóstwa ciekawych znalezisk i spostrzeżeń. Piasek, fale oraz to, co zdołały wyrzucić na brzeg, to niezwykle bogate źródło ciekawostek. Natknęli się na kamień poprzetykany dziurami, jakby był zjedzony przez korniki, oraz muszlę, która kształtem przypominała kardioidę – całkiem niedawno poznali to słowo. Ale najciekawsze zdarzyło się na koniec. Kiedy właściwie chcieli już wracać do domu, zauważyli nieduży woreczek zawiązany starannie sznurkiem. Alfred podszedł z zaciekawieniem do kolejnego odkrycia, a Berenika, zauważywszy, że coś tam ma, w mig znalazła się obok niego.

– Co w nim jest? – zapytała podekscytowana znaleziskiem. – Rozwiąż!

Chłopiec otworzył worek, a sznurek włożył do kieszeni. W środku znaleźli mnóstwo starych monet. Alfred wyjął kilka z nich i przyglądał się im z uwagą.

– Wyglądają na stare, jeszcze sprzed denominacji. Raczej nie są warte za wiele. Trudno oszacować, ile ich może być. Setka, może więcej. Jak sądzisz?

Po parokrotnym zanurzeniu dłoni w zawartości woreczka dziewczynka orzekła:

– Więcej niż setka. Jak zwykle, dzielimy sprawiedliwie, żeby każdy był zadowolony.

– Sprawiedliwie... Czyli tym razem jak? – dzielenie się zdobyczą przerabiali już parokrotnie na różne sposoby.

– Mam nowy pomysł! Możemy wprowadzić do naszego podziału nutkę losowości. Proponuję, byśmy nie wysypywali zawartości. Nie będziemy wiedzieli, co i ile tak naprawdę dzielimy.