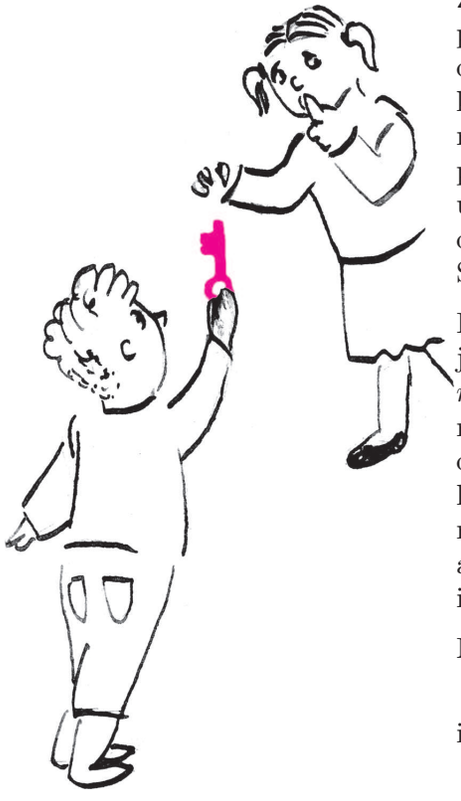
Jak znaleźć klucz?

Każdy od czasu do czasu potrzebuje metody przekazania komuś pewnych wiadomości tak, żeby niepowołane osoby nie miały szans na ich przechwycenie. Począwszy od zabaw z kolegami na podwórku, a skończywszy na operacjach bankowych, wojskowych czy wykorzystujących dane osobowe – bez szyfrów po prostu nie da się żyć. Do zaszyfrowania danych zwykle potrzebny jest klucz – pewne słowo czy liczba, które najpierw kierują procesem tworzenia szyfru, a później pozwalają odbiorcy wiadomości ją odkodować. Osoby, które chcą porozumiewać się za pomocą szyfru, muszą najpierw uzgodnić klucz między sobą. I tu pojawia się problem: jak ustalić klucz, tak żeby nikt oprócz nas nie mógł go poznać?

Można się w tym celu spotkać, ale każdy, kto oglądał filmy szpiegowskie, wie, jak łatwo jest podsłuchać rozmowę. Wysłanie klucza pocztą, wszystko jedno, czy papierową, czy elektroniczną, to pomysł tak samo skazany na porażkę. A gdyby wysłać klucz w formie zaszyfrowanej? Trzeba by najpierw ustalić klucz do szyfru, którym zaszyfrujemy klucz do tego szyfru, którego chcemy używać w korespondencji, czyli wróciliśmy do początkowego problemu... Nie załamujmy się jednak: banki mają się całkiem dobrze (co wyraźnie widać z szyldów lokali użytkowych), tajemnice wojskowe raczej też, i chociaż parę miesięcy temu pewna firma miała duże kłopoty z wyciekiem danych użytkowników konsoli do gier, to jednak ogólny obraz sytuacji wskazuje na to, że istnieją dobre metody zabezpieczania informacji.



Zobaczmy więc, jak ustalić klucz do szyfru w taki sposób, żeby szanse na poznanie go przez osoby niepowołane były bardzo, bardzo małe. Zacznijmy od tego, że ustalanie klucza będzie się odbywać publicznie – osoby A i B, które ten klucz ustalają, wszystkie informacje, które muszą wymienić, mogą ogłosić wszem i wobec. To oznacza, że przy tej metodzie problem podsłuchu nie istnieje. Metoda jest tak opracowana, żeby osoba, która usłyszy wszystkie informacje wymieniane przez osoby A i B, nie mogła odgadnąć ustalonego klucza. Powiesz, Czytelniku, że to niemożliwe? Sprawdźmy!

Będziemy potrzebowali operacji *modulo*, która daje resztę z dzielenia jednej liczby przez drugą. Zapis $m \bmod n$ oznacza resztę z dzielenia m przez n. Na przykład $17 \bmod 3 = 2$, a $21 \bmod 7 = 0$. W ten sposób możemy łatwo przerobić dowolną liczbę całkowitą na liczbę z zakresu od 0 do $n-1$. Niech teraz n oznacza pewną dużą liczbę, a m będzie pewną liczbą dodatnią mniejszą niż n. Osoby A i B uzgadniają tę parę liczb, nie ukrywając ich przed światem. Następnie wybierają jeszcze dwie liczby, ale tym razem tajne. Osoba A wymyśla liczbę a z zakresu od 0 do $n-1$ i nikomu o niej nie mówi; tak samo osoba B wybiera liczbę b.

Następnym krokiem jest wykonanie potęgowania. Osoba A oblicza wartość

$$a_1 = m^a \bmod n$$

i ją udostępnia. Analogicznie, osoba B oblicza i udostępnia

$$b_1 = m^b \bmod n.$$

Kolejne obliczenie pozwala już otrzymać klucz. Osoba A bierze wartość b_1 obliczoną przez osobę B, podnosi do potęgi a i wykonuje na wyniku operację $\bmod n$:

$$k = (b_1)^a \bmod n = (m^b \bmod n)^a \bmod n = m^{ab} \bmod n.$$

(Sprawdź dokładnie, Czytelniku, dlaczego końcowa równość jest prawdziwa.) Osoba B oblicza

$$(a_1)^b \bmod n = (m^a \bmod n)^b \bmod n = m^{ab} \bmod n = k,$$

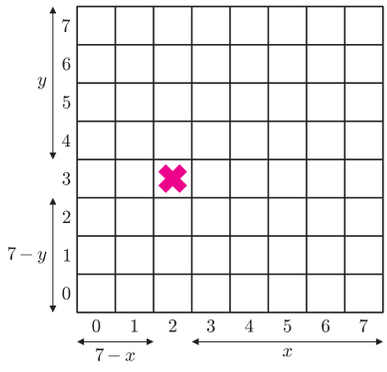
czyli obie osoby otrzymały tę samą wartość k, która będzie ich tajnym kluczem do szyfru. Ta procedura uzgadniania klucza to *protokół Diffiego–Hellmana*.

A co wie osoba z zewnątrz, która chciałaby odgadnąć klucz i złamać szyfr? Otóż, wbrew pozorom, bardzo niewiele. Publicznie zostały podane wartości n, m, $a_1 = m^a \bmod n$ i $b_1 = m^b \bmod n$. Żeby odtworzyć klucz, potrzebna jest znajomość liczby a lub b – mając jedną z tych liczb, osoba podsłuchująca może przeprowadzić takie obliczenie, jak osoby A i B pod koniec ustaleń. Problem sprowadza się więc do pytania, czy znajomość liczb m, n i $m^a \bmod n$ wystarcza do wyznaczenia liczby a. Okazuje się, że ogólnie nie wystarcza, czyli można dobrać liczby m, n, a i b w taki sposób, żeby odgadnięcie klucza przez osobę z zewnątrz było praktycznie niemożliwe przy naszym obecnym stanie wiedzy. Oczywiście, może się zdarzyć, że za kilka lat powstaną algorytmy i programy radzące sobie świetnie z tym problemem, ale na razie opisane metody można z powodzeniem stosować.

Problem odtworzenia liczby a z liczb n, m i $m^a \bmod n$ nazywa się *problemem logarytmu dyskretnego*. Szukając wartości a, próbujemy wykonać operację odwrotną do potęgowania modulo n i stąd logarytm w nazwie. Potęgowanie modulo n jest tak zwaną funkcją jednokierunkową – samą potęgę można obliczyć łatwo i szybko, ale odwrócenie tej operacji jest dla nas (na razie) bardzo trudnym problemem obliczeniowym. Tak trudnym, że dla odpowiedniego doboru danych (potrzebne są naprawdę duże, kilkusetcyfrowe liczby) uznaje się go właściwie za niewykonalny i jego trudności powierza się ważne tajemnice.

Małą Deltę przygotowała Maria DONTEN-BURY

Rozwiązanie zadania M 1332.
Odpowiedź: nie.



Załóżmy, że pole (x, y) jest zatrute. Pokażemy, że Lolek ma strategię wygrywającą. Gra polega tak naprawdę na zmniejszaniu przez graczy w każdym ruchu jednej z liczb a_1, a_2, a_3, a_4, które na początku mają wartości $x, 7-x, y, 7-y$, odpowiednio, a oznaczają liczbę kolumn na prawo, na lewo, liczbę wierszy w górę, w dół od zatrutego pola w aktualnej tabliczce czekolady. Rozważmy liczbę $s = a_1 \oplus a_2 \oplus a_3 \oplus a_4$, gdzie $u \oplus v$ oznacza dodawanie liczb u i v zapisanych binarnie, bez przeniesienia (np. $7 \oplus 3 = (111)_2 \oplus (011)_2 = (100)_2 = 4$).

Na początku gry, przed ruchem Bolka, mamy

$$s = x \oplus (7-x) \oplus y \oplus (7-y) = (x \oplus ((111)_2 - x)) \oplus (y \oplus ((111)_2 - y)) = (111)_2 \oplus (111)_2 = 0.$$

Ogólnie, gdy $s = 0$, w następnym ruchu będziemy mieli $s > 0$ (któraś z liczb a_i zmieniła się). Gdy $s > 0$, zawsze istnieje taki ruch, że po jego wykonaniu $s = 0$. Istotnie, bez utraty ogólności możemy zakładać, że $(a_1)_2$ ma niezerowy bit na pozycji pierwszego bitu znaczącego liczby $(s)_2$. Wówczas $a_1 \oplus s < a_1$, więc wystarczy zmniejszyć liczbę a_1 o $a_1 - (a_1 \oplus s)$, bo wtedy liczba s wyniesie

$$(a_1 \oplus s) \oplus a_2 \oplus a_3 \oplus a_4 = s \oplus s = 0.$$

Zatem Lolek po każdym ruchu zostawi Bolka w sytuacji, w której $s = 0$, więc w końcu Bolek zastanie sytuację, w której $a_1 = a_2 = a_3 = a_4 = 0$ (w każdym ruchu któraś liczba się zmniejsza), co odpowiada temu, że Bolek zostanie z zatrutą kostką i przegra.

Uwaga. To zadanie jest wariantem gry nim, o której można przeczytać w *Delcie* 7/2010, w artykule Tomasza Idziaszka *Gra o wielu obliczach*.