Temat 16

„Współdzielenie” sekretów – O poufności informacji

Streszczenie

Zastosowanie technik kryptograficznych pozwala na „współdzielenie” sekretów przy zachowaniu zaskakująco wysokiego poziomu prywatności.

W czasie zajęć dzieci poznają metodę obliczania średniej wieku osób w grupie, która nie wymaga ujawniania sobie nawzajem wieku żadnej z osób.

Wiek

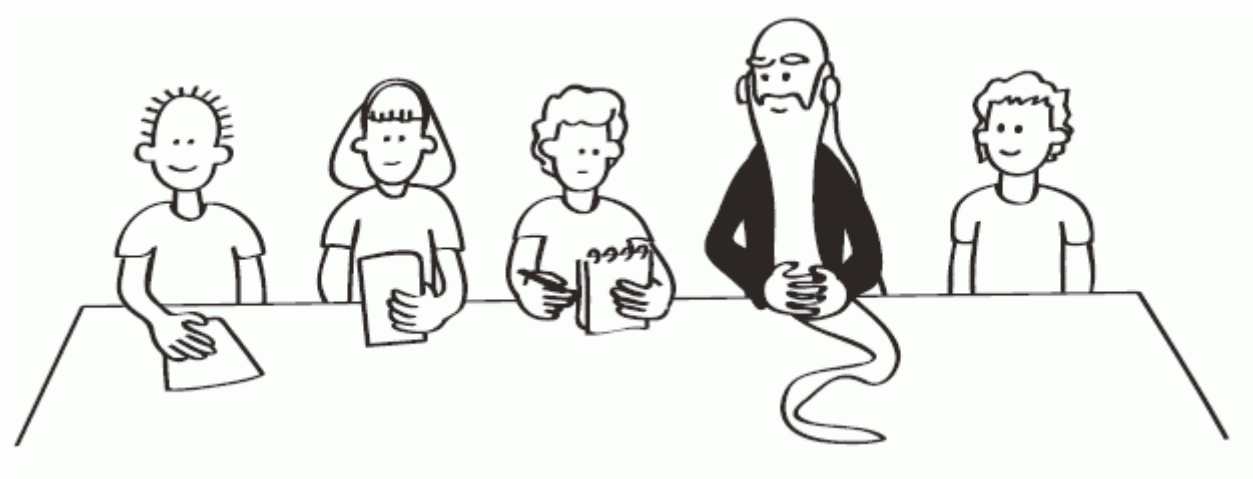
- ✓ 7 i więcej

Materiały

Każde z grup dzieci będzie potrzebować:

- ✓ bloczek kartek papieru
- ✓ długopis

„Współdzielenie” sekretów



Wprowadzenie

Zadanie polega na wyznaczeniu średniego wieku osób w grupie, w taki sposób, iż wiek poszczególnych członków grupy nie zostaje nikomu ujawniony!

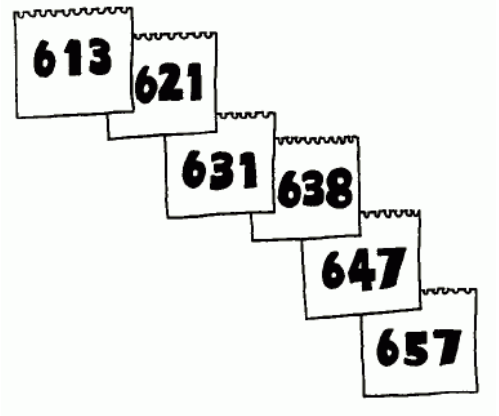
Równie dobrze ta metoda może być zastosowania w celu ustalenia średniej wartości liczbowych dotyczących innych informacji o dzieciach (np. wysokość kieszonkowego). Nic nie stoi na przeszkodzie, by tą metodą uzyskać informacje statystyczne w grupie dorosłych (np. o dochodach).

W grupie powinno się znajdować przynajmniej troje dzieci.

Przebieg zajęć

1. Wyjaśnij grupie, że zadanie polega na obliczeniu średniej wieku w grupie bez konieczności ujawniania komukolwiek swego wieku. Zapytaj o pomysły. Jeśli ich brakuje, to zapytaj o to, czy w ogóle wierzą w istnienie takiej metody…

2. Wybierz 6-10 dzieci. Podaj pierwszemu dziecku bloczek kartek i poproś je, by napisało na kartce dowolną trzycyfrową liczbę na pierwszej karteczce. Rysunek pokazuje sytuację, w której wybrano liczbę 613.



3. Poproś to dziecko, by oderwało pierwszą karteczkę, dodało do wybranej liczby liczbę swoich lat i zapisało sumę na drugiej karteczce. Rysunek ukazuje sytuację, gdy dziecko ma 8 lat. Dziecko powinno zachować pierwszą z karteczek (i nie pokazywać jej nikomu).

4. Blok z kartkami trafia do drugiego dziecka, które po wyrwaniu pierwszej kartki, zapisuje na następnej liczbę powiększoną o jego wiek. W przykładzie jest to dziecko 10-letnie.

5. Czynności te powtarza się tak długo, aż wszystkie dzieci nie otrzymają bloku kartek i nie wpiszą liczby.

6. Następnie blok wraca do pierwszego dziecka. Ono odejmuje od liczby na kartce liczbę wybraną na początku. W przykładzie jest to: 657-613=44. Ta liczba jest sumą liczby lat dzieci. Po podzieleniu jej przez liczbę dzieci otrzymujemy średnią wieku: 8,8 lat.

7. Zwróć dzieciom uwagę na to, iż żadne z nich nie będzie w stanie poznać wieku innego, jeżeli każdy zniszczył otrzymaną kartkę papieru.

Modyfikacje

System podobny do przedstawionego mógłby zostać użyty w celu zrealizowania tajnego głosowania: głosujący na „tak” dodawaliby do otrzymanej liczby liczbę 1. Oczywiście dodanie przez kogoś liczby większej niż 1 (lub mniejszej niż 0) czyni głosowanie nieuczciwym (uzyskany wynik może nie budzić podejrzeń chyba że liczba głosów na „tak” przekroczy liczbę głosujących).

O co w tym wszystkim chodzi?

W komputerowych bazach danych przechowuje się wiele informacji o charakterze osobistym, np. stan konta bankowego (saldo), zobowiązania podatkowe i kredytowe, czas posiadania prawa jazdy, wyniki egzaminów, informacje o stanie zdrowia itd. Tajność (utrzymywanie w tajemnicy) informacji jest bardzo istotna w tych sytuacjach! Z drugiej strony czasem zachodzi potrzeba podzielenia się pewną informacją z innymi. Na przykład: kiedy korzystamy z karty bankowej płacąc za zakupy, sklep musi w jakiś sposób sprawdzić dostępność środków na naszym koncie.

Często ujawniamy więcej informacji niż to jest naprawdę konieczne w danej sytuacji.
Na przykład: elektroniczna transakcja w sklepie wiąże się prawdopodobnie z ujawnieniem nazwy banku, numeru naszego konta i naszego nazwiska. Jednocześnie bank uzyskuje informację o miejscu dokonanych zakupów. Właściwie nic nie stoi na przeszkodzie, by bank stworzył tzw. profil klienta rejestrując miejsce zakupu benzyny czy odwiedzane sklepy spożywcze, średni koszt zakupów w danym okresie i ich częstotliwość. Gdybyśmy płacili gotówką wtedy żadna z tych informacji nie byłaby ujawniona. Nawet jeśli fakt przekazania pewnych informacji nie martwi większości z nas, to jednak istnieje ryzyko nadużyć. Dla przykładu: do osób, które często kupują bilety lotnicze przesyłane będą oferty biur podróży; jakość obsługi (w tym czy innym miejscu) będzie uzależniana od stopnia zamożności klienta (przewidywanego na podstawie marki banku z którego korzysta); w skrajnych przypadkach dane osobowe ujawnione przy okazji kłopotliwej transakcji (której klient mógłby się wstydzić) mogą być użyte w celu szantażowania.

Choć utrata pełnej anonimowości jest dość powszechnie akceptowana, to warto wiedzieć, że istnieją protokoły kryptograficzne, które pozwalają uczynić transakcje elektroniczne równie poufnymi co płacenie gotówką. Trudno w to uwierzyć, ale pieniądze mogą być przelane z konta bankowego na konto naszego sprzedawcy bez potrzeby przekazywania stronom jawnie informacji o ich lokalizacji. Wyżej opisane zajęcia z dziećmi pozwalają pomóc im w to uwierzyć (czynią poprzednie rozważania bardziej wiarygodnymi).