Scenariusz 18. Mały kryptograf

Szyfrowanie to zasadnicza sprawa dla zapewnienia bezpieczeństwa informacji.

Osiągnięciem współczesnej kryptografii jest to, że potrafimy zaszyfrować wiadomość jednym kluczem (publicznie dostępnym) ale do jej odczytania konieczny jest iiny klucz (prywatny) posiadany tylko przez odbiorcę wiadomości.

Posłużmy się analogią: Wszyscy kupują kłódki, zapisują na nich swoje imię i kładą je wszystkie na tym samym stole. Klucze zabierają oczywiście ze sobą – nie są potrzebne do zamknięcia kłódki zatrzaskowej (z zapadką). Ktoś, kto chce w bezpieczny sposób przekazać wiadomość do kogoś innego, wkłada ją do skrzynki, którą zamyka przy pomocy kłódki należącej do adresata. Nawet gdyby skrzynka trafiła w niepowołane ręce, nie będzie mogła zostać otwarta. Zauważmy, że nie było potrzeby wcześniejszego przekazania żadnych kluczy pomiędzy zainteresowanymi stronami.

W czasie tych zajęć ukazany zostanie sposób realizacji powyższego modelu szyfrowania. W świecie cyfrowym nie ma konieczności używania oryginalnych „kłódek". Zamiast tego możemy łatwo wykonać ich kopię, a oryginał „zostawić na stole" (do wykorzystania przez inną osobę). W przypadku tradycyjnej kłódki tworzenie jej kopi wiązałoby się z odkryciem tajemnicy pasującego do niej klucza. W świecie cyfrowym ten problem nie istnieje.

Zajęcia przeznaczone są dla dzieci w wieku 11 lat i więcej.

Przed lekcją należy przygotować odpowiednią liczbę kserokopii karty pracy.

1.5. Przebieg lekcji

1.5.1. Wprowadzenie

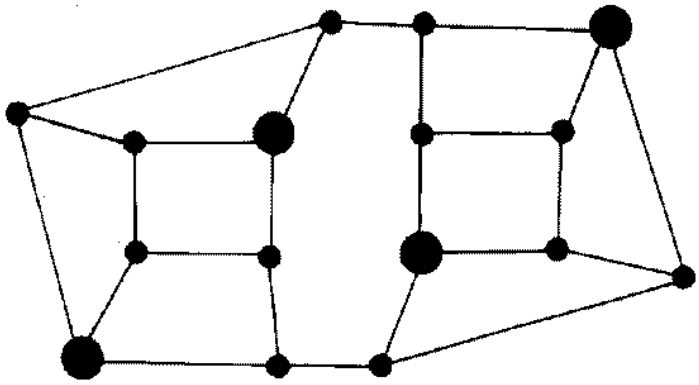
Te zajęcia należą do najbardziej wymagających wśród propozycji projektu „CS Unplugged". Uważna praca i skupienie są warunkiem ich powodzenia. Dzieci powinny wcześniej uczestniczyć w zajęciach dotyczących pojęcia funkcji jednokierunkowej (Miejscowość turystyczna).

Emilia zamierza przekazać Wojtkowi poufną wiadomość. Pewnie spodziewalibyśmy się, że ma ona postać zdania czy nawet całego akapitu tekstu. Tym razem jest inaczej – cała wiadomość to tylko jedna litera (a dokładniej jej kod liczbowy). Oczywiście Emilia mogłaby przesłać cały ciąg takich jednoznakowych wiadomości, które w konsekwencji dałyby całe zdanie (to całkiem dobre wyobrażenie działania komputera przesyłającego wiadomość). Czasami jednak nawet bardzo krótkie (zwięzłe) wiadomości mogą mieć duże znaczenie – takie przypadki są znane z historii. Zobaczymy jak Emilia, stosując zasady określone publicznie przez Wojtka („kłódka"), może zaszyfrować przesyłany komunikat. Przechwycenie tej wiadomości przez niepowołaną osobę nie oznacza poznanie jej jawnej treści. Tylko Wojtek jest w stanie odtworzyć wiadomość, bo tylko on zna potrzebne do tego zasady odszyfrowania (klucz do „kłódki").

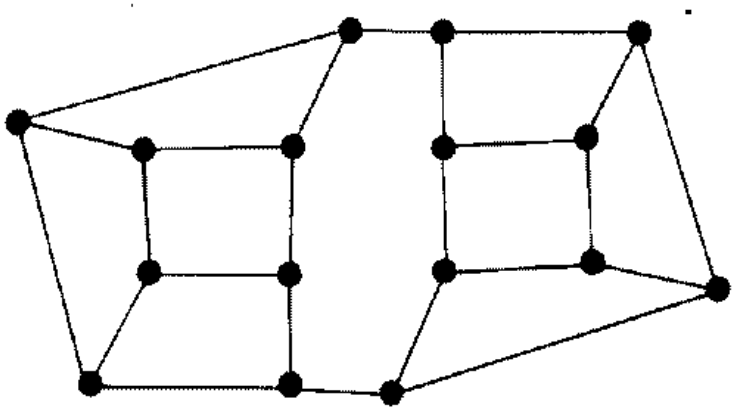
Koncepcja ta będzie zaprezentowana z użyciem map, podobnych do tej z zajęć Miejscowość turystyczna: krawędzie oznaczają ulice a wierzchołki skrzyżowania. Taka mapa będzie w dwóch odmianach: w wersji publicznie dostępnej służącej do szyfrowania (rodzaj kłódki) oraz w wersji publicznej (rodzaj klucza do kłódki).

1.5.2. Etapy lekcji

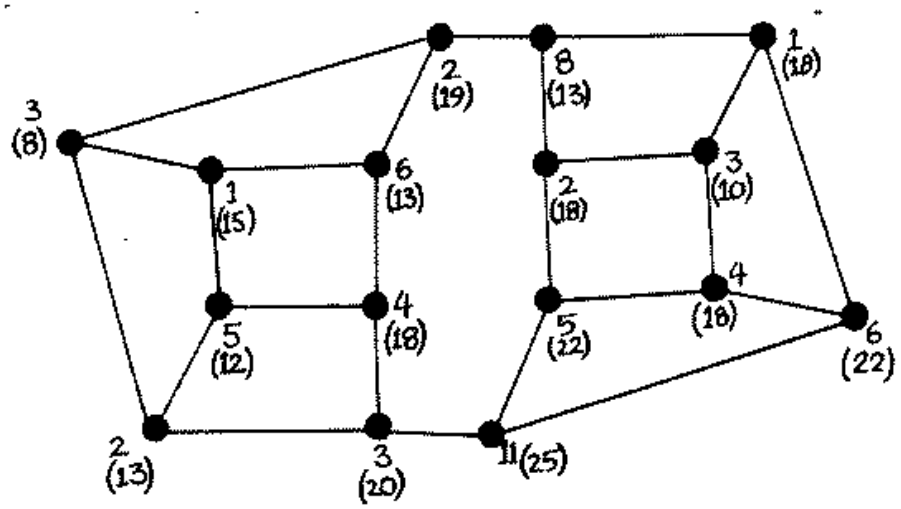
Na karcie pracy znajduje się wersja jawna (publiczna) mapy Wojtka. Chłopiec mógłby ją położyć na stole (czy zamieścić na stronie internetowej) tak, aby każdy mógł ją zobaczyć albo ograniczyć się tylko do wręczenia jej zainteresowanej osobie, która chce wysłać do niego wiadomość. Na poniższym rysunku pokazana jest natomiast wersja poufna (prywatna) mapy Wojtka. Różni się od wersji publicznej tym, że niektóre ze skrzyżowań są wyróżnione (pogrubione).



W czasie zajęć wszyscy uczniowie powinni być zaangażowani w pracę – jest jej sporo. Nie jest trudna, ale wymaga dużej dokładności. Pomyłka będzie mieć poważne konsekwencje. Ważne, by dzieci pojęły nieoczywistość możliwości takiego asymetrycznego sposobu szyfrowania informacji. Jeśli nie pojawią się u nich wątpliwości co do tego, że jest to w ogóle możliwe, nie będą mieć odpowiedniej motywacji do wysiłku, który będą musiały włożyć w pracę. Szczególnie cenne może być dla nich spostrzeżenie, że metoda ta pozwoli na przykład na ukrycie przed …nauczycielem znaczenia liścików przesyłanych podczas lekcji – nawet jeśli nauczyciel zna zasadę szyfrowania, nie będzie w stanie odtworzyć jawnego tekstu.



1. Narysuj na tablicy mapę (klucz) publiczny Wojtka (rysunek powyżej). Wybierz liczbę, którą Emilia będzie miała przesłać. W miejscach skrzyżowań umieść na mapie takie liczby, by ich suma była równa liczbie przesyłanej przez Emilię. Na rysunku (poniżej) są to liczby zapisane wyżej (te bez nawiasów). W tym przypadku Emilia wybrała liczbę 66, co oznacza, że suma liczb przy skrzyżowaniach musi być równa 66. Nic nie stoi na przeszkodzie, by wśród tych nich znajdowały się też liczby ujemne.

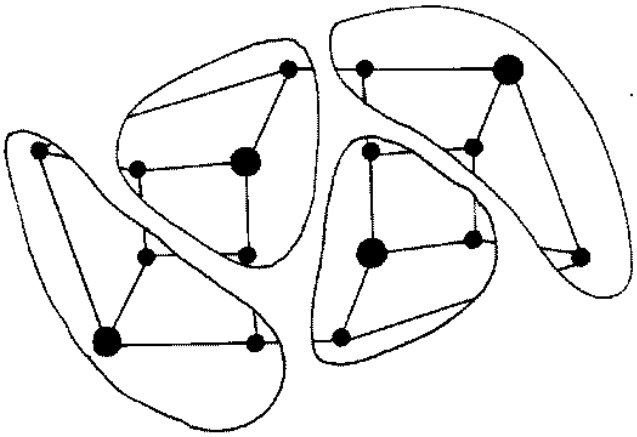


2. Emilia nie może przesyłać do Wojtka w jawny sposób liczb, które wpisane zostały na publiczną mapę. Gdyby wpadły w niepowołane ręce, to ktokolwiek po ich zsumowaniu poznałby treść wiadomości. Dlatego Emilia wykonuje następujące obliczenia: przy każdym skrzyżowaniu zapisuje w nawiasie sumę liczby wcześniej zapisanej oraz liczb z sąsiednich skrzyżowań. Dla przykładu: przy skrzyżowaniu najbardziej wysuniętym na prawo pojawi się liczba 22 jako suma liczb 6 oraz 1, 4, 11.

3. Emilia wyśle do Wojtka mapę, na której zapisane będą tylko sumy (liczby w nawiasach). Należy więc wymazać liczby napisane na początku (składniki) i zapisy obliczeń albo na nowym szablonie mapy zapisać tylko sumy. Można się łatwo przekonać, że dzieci biorące udział w zajęciach nie będą w stanie odtworzyć liczb-składników (chyba że zapamiętały niektóre z nich…).

4. Tylko ktoś, kto jest posiadaniu klucza prywatnego Wojtka może odtworzyć treść przesyłanej przez Emilię wiadomości. Na prywatnej mapie są wyróżnione niektóre ze skrzyżowań – stanowią one klucz potrzebny do odszyfrowania. Po zsumowaniu liczb zapisanych przy tych skrzyżowaniach (są to 13, 13, 22, 18) ujawniona zostanie wiadomość od Wojtka. Jest to liczba 66.

5. Dlaczego to działa? Mapa jest pod pewnym względem wyjątkowa. Wojtek przy tworzeniu wersji prywatnej (wyróżniania skrzyżowań) postępował następująco: wyróżnił jedno ze skrzyżowań i wszystkie najbliższe zaznaczył obwodem, a następnie powtórzył tę procedurę dla kolejnych dbając o to, by cała mapa została podzielona na rozłączne kawałki (jak na rysunku). Dzieci powinny dostrzec, że liczby pierwotnie zapisane przy niewyróżnionych skrzyżowaniach na danym kawałku mapy dają w sumie liczbę przy wyróżnionym skrzyżowaniu, która przesyłana jest do Wojtka. Oznacza to, że do odczytania wiadomości wystarczy, że Wojtek doda do siebie liczby przy wyróżnionych skrzyżowaniach: ich suma będzie równa sumie liczb zapisanych pierwotnie przy wszystkich skrzyżowaniach, co stanowiło właśnie treść przesyłanej wiadomości.



Wydaje się, że przesłanie jednej litery wymaga ogromnego nakładu pracy. Taka jest prawda – szyfrowanie informacji w przypadku kryptografii z kluczem publicznym nie jest sprawą prostą. Zysk jest jednak wielki: zainteresowane strony nie muszą spotykać się w celu przekazania klucza szyfrowania. Klucz szyfrowania nie jest bowiem tajny – może być umieszczony na tablicy ogłoszeń. Przesyłana wiadomość będzie bezpieczna dopóki klucz prywatny pozostaje tajemnicą adresata. Wszelkie obliczenia związane z utworzeniem szyfrogramu i później jego odkodowaniem wykonywane są z użyciem programów komputerowych, więc to komputer wykonuje tę ogromną pracę. Być może warto, by uczniowie dowiedzieli się, że należą do bardzo nielicznej grupy osób, które faktycznie bez użycia komputera będą mogły od początku do końca, dzięki odpowiedniemu przykładowi, przekonać się, jak działa kryptografia klucza publicznego. Wielu informatykom tzw. praktykom wydaje się, że nie jest możliwe zrozumienie przez dzieci tak trudnego (ich zdaniem) zagadnienia!

Co z podsłuchiwaniem? Mapa Wojtka jest identyczna z mapą Miejscowości Turystycznej (scenariusz 1), na której wyróżniona została najmniejsza liczba skrzyżowań takich, że rozmieszczone przy nich punkty sprzedaży pokrywają całe miasto (każdą ulicę dzieli co najwyżej jedno skrzyżowanie od punktu sprzedaży). W czasie tamtych zajęć pokazany został sposób stworzenia takiego planu miasta. Można powiedzieć, że punktem wyjścia są rozłączne kawałki mapy prywatnej Wojtka. Z rozważań zawartych w temacie 14 wiadomo, że jest praktycznie niemożliwe znaleźć rozwiązanie problemu lokalizacji inaczej niż metodą prostego przeszukiwania (najpierw konfiguracje z jednym pojazdem, później z dwoma itd. aż do skutku). Naukowcy do tej pory nie potrafią rozstrzygnąć, czy istnieje bardziej efektywna metoda!

Załóżmy, że Wojtek przygotuje odpowiednio skomplikowaną mapę: z 50 czy nawet 100 skrzyżowaniami. Wydaje się, że wówczas nikt nie będzie w stanie odczytać treści przesyłanych wiadomości – nawet najmądrzejsi z matematyków nie poradzą sobie z tym. (Ściśle rzecz biorąc: nie poradzą sobie z odtworzeniem klucza prywatnego! Więcej na ten temat w części „O co w tym wszystkim chodzi?”)

6. Od tego momentu dzieci powinny pracować w grupach czteroosobowych. Każda para w grupie powinna otrzymać mapę publiczną (karta pracy). Powinna następnie wybrać wiadomość do przesłania (dowolną liczbę całkowitą) i zakodować jej treść z użyciem mapy (klucza publicznego). Po zakodowaniu należy przekazać szyfrogram innej parze. Próby odszyfrowania powinny zakończyć się brakiem sukcesu, chyba że uda się grupie odgadnąć klucz prywatny. Na końcu grupa powinna otrzymać prywatną wersję mapy, by móc odczytać treść wiadomości.

7. Następnie każda para może zaprojektować swoją własną mapę. Wersję publiczną przekazuje drugiej parze lub nawet „opublikować” na klasowej tablicy ogłoszeń. Zasada projektowania mapy jest identyczna z tą z zajęć „Miejscowość turystyczna”. Dzieci powinny dodać możliwie dużo ulic, by uniemożliwić „rozwiązanie” (odgadywanie) rozwiązania. Powinny jednak postępować ostrożnie, by przez przypadek nie dodać ulic do wyróżnionych skrzyżowań – wówczas kawałki mapy nie będą rozłączne, a to jest niezbędne do właściwego szyfrowania.

1.6. O co w tym wszystkim chodzi

Chcielibyśmy, aby możliwe było bezpieczne przesyłanie wiadomości siecią komputerową w taki sposób, by nikt poza adresatem nie mógł odczytać zaszyfrowanej wiadomości bez względu na posiadane umiejętności i determinację. Okazuje się, że zainteresowane strony nie muszą spotykać się w celu przekazania klucza do szyfrowania. Istnieje bowiem kryptografia klucza publicznego. Dzięki niej Emilia może bezpiecznie przesłać wiadomość do Wojtkaa przy pomocy jego klucza publicznego, który może być udostępniony np. na stronie internetowej.

Zapewnienie tajności (poufności) przesyłanej wiadomości to tylko jedno z wymagań stawianych kryptografii. Innym jest możliwość potwierdzenia tożsamości (uwierzytelnienia). Kiedy Emilia dostaje wiadomość od Wojtka powinna mieć pewność, że to rzeczywiście on jest nadawcą. Wyobraźmy sobie, że ktoś otrzymuje wiadomość: „Kochanie, zabrakło mi pieniędzy. Przelej, proszę, 100 dolarów na konto 0241-45-784329 – Wojtek." Skąd mieć pewność, że to naprawdę Wojtek wysłał wiadomość? Systemy kryptografii publicznej zapewniają i to. Pozwalają nie tylko na to, by Emilia wysłała Wojtkowi wiadomość szyfrując ją z użyciem jego klucza publicznego. Ale również na to, by Wojtek wysłał do Emilii wiadomość używając jego klucza prywatnego (tzw. podpis elektroniczny). Jeśli tę wiadomość można odszyfrować z użyciem klucza publicznego Wojtka, to nie ma wątpliwości, że to on jest jej nadawcą.

Trzeba przyznać, że choć schemat zaprezentowany w czasie zajęć daje dobre wyobrażenie o stosowanych w praktyce systemach kryptografii klucza publicznego, to nie jest tak naprawdę bezpieczny – nawet jeśli zastosujemy mapę dużych rozmiarów.

Dlaczego? Prawdą jest, że nikt nie zna efektywnej metody znajdowania zbioru dominującego w grafie (tzn. np. lokalizacji obwoźnych lodziarni przy jak najmniejszej liczbie skrzyżowań). I w tym sensie schemat jest bezpieczny – gdyż nikt nie jest wstanie odtworzyć mapy prywatnej. Okazuje się jednak, że istnieje inny sposób ataku, który pozwoli odczytać tekst jawny. Dzieci w szkole podstawowej nie będą w stanie go pojąć. Nauczyciel powinien mieć jednak świadomość ograniczeń analogii używanego w czasie zajęć schematu. Nauczyciel nie zainteresowany wyjaśnieniem tej kwestii nie musi czytać kolejnych akapitów!

Ponumerujmy skrzyżowania na mapie: 1, 2, 3, ... Liczby, które pierwotnie były przy nich zapisane oznaczmy jako: b_1, b_2, b_3, ..., a liczby tworzące szyfrogram, które są przesyłane jako: t_1, t_2, t_3, ... Jeśli np. skrzyżowanie nr 1 jest połączone ulicami ze skrzyżowaniami nr 2, 3 i 4, to zachodzi następujący związek: $t_1 = b_1 + b_2 + b_3 + b_4$.

Postępując w podobny sposób możemy zapisać równania dla każdego ze skrzyżowań. Liczba równań będzie równa liczbie niewiadomych b_1, b_2, b_3, ... Podsłuchujący jest w posiadaniu mapy publicznej i może bez problemu zapisać ten układ równań, a następnie rozwiązać z użyciem odpowiedniego programu komputerowego. Po wyznaczeniu wartości niewiadomych wystarczy je dodać do siebie, by poznać treść wiadomości. Nie ma potrzeby odtworzenia mapy prywatnej. Liczba obliczeń (złożoność obliczeniowa) wykonanych w czasie rozwiązywania układu równań metodą eliminacji Gaussa jest proporcjonalna do sześcianu liczby równań. W tym jednak przypadku, gdy większość współczynników przy niewiadomych jest równa 0, istnieją nawet bardziej efektywne metody rozwiązania układu równań. Jak wiadomo odtworzenie mapy prywatnej wymagałoby wykonania obliczeń o złożoności wykładniczej...

Nikt nie powinien czuć się oszukany! Schemat przedstawiony w czasie zajęć, choć był niedoskonała analogią, to jednak dał wyobrażenie o prawdziwych systemach kryptografii klucza publicznego. W rzeczywistości stosuje się inne techniki szyfrowania (tzn. oparte na innych problemach obliczeniowych niż problem zbioru dominującego) i trudno byłoby na lekcji z dziećmi wykonać potrzebne obliczenia bez używania komputera.

Dla przykładu: bezpieczeństwo jednej z metod kryptografii klucza publicznego stosowanej przez wiele lat opierało się na trudności rozkładu liczby na czynniki.

Czy da się rozłożyć na czynniki liczbę: 9 412 343 607 359 262 946 971 172 136 294 514 357 528 981 378 983 082 541 347 532 211 942 640 121 301 590 698 634 089 611 468 911 681? Tak! To iloczyn liczb: 86 759 222 313 428 390 812 218 077 095 850 708 048 977 i 108 488 104 853 637 470 612 961 399 842 972 948 409 834 611 525 790 577 216 753? Okazuje się, że w rozkładzie występują tylko dwie wielocyfrowe liczby pierwsze. Znalezienie rozkładu na czynniki tej 100-cyfrowej liczby mogłoby zająć nawet kilka miesięcy pracy komputera..

Wojtek mógłby użyć tej 100-cyfrowej liczby jako swojego klucza publicznego. Jej dwa czynniki pierwsze stanowiłyby klucz prywatny. Znalezienie dużych liczb pierwszych nie jest aż takim trudnym zadaniem dla komputera. Ich wymnożenie również. Dość szybko można więc przygotować klucz publiczny. Zupełnie inaczej ma się sprawa odtworzenia klucza prywatnego na podstawie znajomości klucza publicznego. Warto dodać, że w praktyce stosowano nawet klucze złożone 512-bitow (w zapisie dziesiętnym to ponad 150 cyfr) a nawet 1024 albo 2048 bitów!

Ściśle rzecz biorąc to nie same liczby pierwsze i ich iloczyn stanowiły wartości kluczy, ale liczby wygenerowane na ich podstawie. Efekt jest jednak ten sam: zasadnicza trudność złamania szyfru polegała na znalezieniu rozkładu liczby na czynniki. Nie będziemy tu jednak przedstawić szczegółów tej metody szyfrowania.

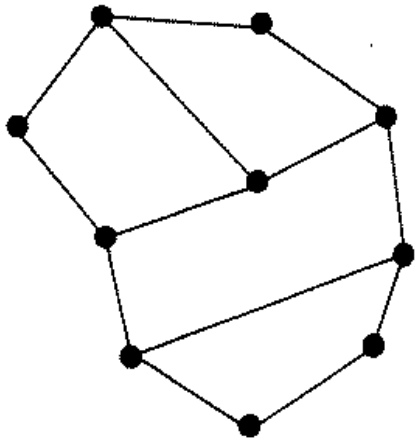
Jak bezpieczny jest system oparty o problem rozkładu liczby na czynniki pierwsze? Zagadnienie tzw. faktoryzacji przykuwało uwagę wielu matematyków przez wiele stuleci. Odkryte zostały metody znacząco bardziej efektywne od metody siłowej (przeszukiwania liczby po liczbie). Nikt jednak nie znalazł metody naprawdę szybkiej, a więc algorytmu wielomianowego. Co więcej, nie wiadomo, czy taki w ogóle istnieje. Wydaje się, że system oparty o trudność rozkładu liczby na czynniki, mimo że nie należy do grupy problemów NP.-zupełnych, jest bezpieczny (nie tylko w sensie matematyki szkolnej jak to było w przykładzie ukazanym wyżej). Pewności jednak nie ma. Choć do tej pory nikt jej nie znalazł, to być może istnieje jednak metoda złamania szyfru, która wcale nie wymaga rozłożenia liczby na czynniki. Podobnie jak złamanie szyfru Wojtka nie wymagało rozwiązania problemu lokalizacji dla Miejscowości turystycznej.

Można się zastanawiać, czy określona metoda szyfrowania jest bezpieczna również w przypadku, gdy wiadomo, że przesyłana będzie wiadomość o jednej z kilku ustalonych treści. Intruz mógłby postąpić następująco: zaszyfrowałby każdą z wersji i uzyskane w ten sposób szyfrogramy porównał z przechwyconym szyfrogramem. Metoda szyfrowania stosowana przez Emilię jest odporna na taki „atak”, gdyż tę samą wiadomość można zaszyfrować na wiele sposobów w zależności od tego, za pomocą jakiej sumy zapisana została szyfrowana liczba. W rzeczywistości systemy kryptograficzne są projektowane w taki sposób, by dla danego szyfrogramu liczba możliwych tekstów jawnych była bardzo duża. Zbyt duża aby mógł je wszystkie sprawdzić nawet szybki komputer.

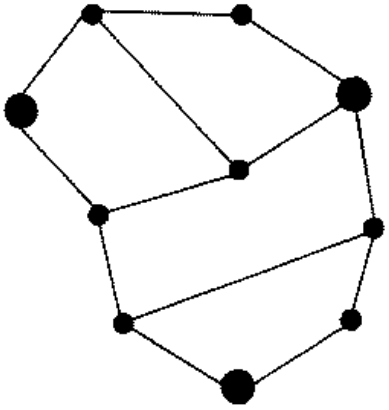
Nie wiadomo, czy istnieje szybki algorytm faktoryzacji. Nikt nie udowodnił, że jego znalezienie jest niemożliwe. Gdyby został odkryty wtedy wiele systemów kryptograficznych przestałoby być bezpiecznymi. W scenariuszu „Miejscowość turystyczna” poruszone zostało zagadnienie problemów NP-zupełnych, które wszystkie mają ze sobą ścisły związek: możliwość rozwiązania jakiegokolwiek z nich w sposób efektywny oznaczałoby możliwość rozwiązania pozostałych. Ponieważ daremny okazał się do tej pory ogromny wysiłek włożony w poszukiwanie szybkich algorytmów dla tych problemów, wydają się one wspaniałymi kandydatami do stosowania w projektowanych systemach kryptograficznych. Niestety napotkano na duże trudności w realizacji tego pomysłu. Do tej pory projektanci systemów kryptograficznych są zmuszeni ograniczać się do stosowania problemów (takich jak rozkład na czynniki pierwsze), których złożoność może okazać o wiele mniejsza niż problemów NP-zupełnych. Odpowiedzi na wyżej postawione pytania są warte wielu milionów dolarów. Są kluczowe dla działalności wielu przedsiębiorstw oraz dla bezpieczeństwa narodowego. Kryptografia jest dzisiaj bardzo istotnym obszarem badań w informatyce.

Karta pracy. Mały kryptograf

Zastosuj poniższe mapy do zaszyfrowania i odszyfrowania wybranej liczby:



mapa publiczna



mapa prywatna