INFORMATYKA – MÓJ SPOSÓB NA POZNANIE I OPISANIE ŚWIATA

PROGRAM NAUCZANIA INFORMATYKI Z ELEMENTAMI PRZEDMIOTÓW MATEMATYCZNO-PRZYRODNICZYCH

Informatyka – poziom rozszerzony

Bezpieczeństwo WWW. O szyfrowaniu i podpisie elektronicznym

Paweł Perekietka

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Tytuł: ***Bezpieczeństwo WWW. O szyfrowaniu i podpisie elektronicznym***

Autor: ***Paweł Perekietka***

Redaktor merytoryczny: ***prof. dr hab. Maciej M. Sysło***

Materiał dydaktyczny opracowany w ramach projektu edukacyjnego
Informatyka – mój sposób na poznanie i opisanie świata.
Program nauczania informatyki z elementami przedmiotów matematyczno-przyrodniczych

www.info-plus.wwsi.edu.pl

infoplus@wwsi.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: *Marzena Kamasa*

Warszawa 2013

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

SCENARIUSZ TEMATYCZNY

BEZPIECZEŃSTWO WWW. O SZYFROWANIU I PODPISIE ELEKTRONICZNYM

INFORMATYKA – POZIOM ROZSZERZONY

OPRACOWANY W RAMACH PROJEKTU:

INFORMATYKA – MÓJ SPOSÓB NA POZNANIE I OPISANIE ŚWIATA.

PROGRAM NAUCZANIA INFORMATYKI

Z ELEMENTAMI PRZEDMIOTÓW MATEMATYCZNO-PRZYRODNICZYCH

Streszczenie

Kryptografia (szyfrowanie danych) rozwiązuje dwa zasadnicze problemy komunikacji internetowej – zapewnia poufność (tajność) i integralność (spójność) danych oraz pozwala na potwierdzenie autentyczności korespondencji. Zapoznanie uczniów z tymi zagadnieniami powinno być jednym z celów lekcji informatyki na poziomie rozszerzonym. Nie należy oczekiwać, by uczniowie poznawali wyczerpująco różne szczegóły techniczne (nawet jeśli są one przedstawiane podczas zajęć). Chodzi przede wszystkim o świadomość istnienia zagrożeń oraz zrozumienie logiki bezpieczeństwa połączenia internetowego, opartego na wykorzystaniu osiągnięć współczesnej kryptografii.

Czas realizacji

4 x 45 minut

Tematy lekcji

1. WWW i HTTP. O szyfrowaniu i podpisie elektronicznym (2 x 45 minut)
2. Kryptografia z kluczem jawnym (klucza publicznego). Algorytm RSA (2 x 45 minut)

LEKCJA NR 1-2

TEMAT: WWW i HTTP. O szyfrowaniu i podpisie elektronicznym

Streszczenie

Standardowa implementacja protokołu HTTP, który jest podstawą funkcjonowania usługi stron internetowych WWW, nie zawiera żadnych mechanizmów kryptograficznych. Oznacza to, że dane (w tym: hasła) przesyłane są przez sieć otwartym tekstem. Dlatego np. witryny internetowe instytucji finansowych wymuszają stosowanie szyfrowanej wersji HTTP.

W czasie lekcji omówione zostaną podstawy kryptografii pod kątem zastosowania w bezpieczeństwie usługi WWW. Nie chodzi przy tym o znajomość szczegółów technicznych, ale uświadomienie problemu oraz zrozumienie przez uczniów opisywanych mechanizmów.

Podstawa programowa

Etap edukacyjny: IV, przedmiot: informatyka (poziom rozszerzony)

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

III. Rozwiązywanie problemów i podejmowanie decyzji z wykorzystaniem komputera, z zastosowaniem podejścia algorytmicznego.

V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Treści nauczania – wymagania szczegółowe

1.3b. Uczeń prawidłowo posługuje się terminologią sieciową, korzysta z usług w sieci komputerowej, lokalnej i globalnej, związanych z dostępem do informacji, wymianą informacji i komunikacją;

2.5. Uczeń opisuje mechanizmy związane z bezpieczeństwem danych: szyfrowanie, klucz, certyfikat;

5.11e. Uczeń opisuje szyfr Cezara, szyfr przestawieniowy oraz szyfr z kluczem jawnym (RSA) oraz wykorzystanie algorytmów szyfrowania w podpisie elektronicznym;

7.3. Uczeń stosuje normy etyczne i prawne związane z rozpowszechnianiem programów komputerowych, bezpieczeństwem i ochroną danych oraz informacji w komputerze i w sieciach komputerowych;

7.4. 4) Uczeń omawia zagadnienia przestępczości komputerowej, w tym piractwo komputerowe, nielegalne transakcje w sieci.

Cele operacyjne

Uczeń:

- posługuje się klasycznymi przykładami szyfrów symetrycznych (podstawieniowych): szyfr Cezara i szyfr Vigenere'a;
- wyjaśnia, dlaczego współcześnie w kryptografii algorytmy są powszechnie znane, tajny zaś jest klucz (tzw. zasada Kerckhoffsa);
- dostrzega ograniczenia kryptografii symetrycznej, związane z dystrybucją (udostępnieniem) klucza;
- opisuje WWW jako usługę klient-serwer, działającą w oparciu o protokół HTTP;
- posługuje się pojęciami: poufność (tajność) danych, spójność (integralność) danych, uwierzytelnienie serwera;
- rozumie potrzebę stosowania narzędzi kryptograficznych dla zapewnienia bezpieczeństwa połączenia HTTP;

– opisuje mechanizm SSL i sposób realizacji usług poufności i uwierzytelnienia;
– opisuje mechanizm tworzenia podpisu elektronicznego i jego weryfikacji (na przykładzie certyfikatu serwera WWW);
– ma świadomość, że kryptografia i kryptoanaliza są ważnymi dziedzinami badań informatycznych.

Słowa kluczowe

szyfrowanie, klucz szyfrowania, kryptografia, kryptoanaliza, zasada Kerckhoffsa, dystrybucja klucza, poufność (tajność), spójność (integralność), skrót wiadomości, funkcja jednokierunkowa, podpis elektroniczny, certyfikat, uwierzytelnienie, protokół HTTP, serwer, klient, mechanizm SSL, atak kryptograficzny

Co przygotować



- Prezentacja 1 „Klasyczne_szyfry”
- Prezentacja 2 „Bezpieczeństwo HTTP”
- Skoroszyt Klasyczne_szyfry_Cezara_Vigenerea.xls oraz Klasyczne_szyfry_Cezara_Vigenerea.ods (materiały pomocnicze 1 i 2)
- Karta „Alfabet” (materiały pomocnicze 3)
- Schemat „Kryptografia Internetu” (materiały pomocnicze 4)
- Animacja „Podpis elektroniczny”

Przebieg zajęć

Wprowadzenie (5-10 minut)

Nauczyciel przedstawia uczniom problem: bezpieczeństwo połączenia internetowego ze szkolnym dziennikiem elektronicznym. Może posłużyć się narracją w rodzaju: *W szkole korzysta się z dziennika elektronicznego. Pewnego dnia nauczyciel, pracujący w jednej z sal, zauważa problem: w czasie sprawdzania obecności widzi na liście jednej z klas imię i nazwisko ucznia, którego tam być nie powinno. Okazuje się, że w bazie danych na serwerze wszystko jest w najlepszym porządku. Jak wyjaśnić to zdarzenie?*

Nauczyciel udziela głosu kilku uczniom. W razie potrzeby stawia pytania pomocnicze. Dostrzeżenie zasadniczych zagrożeń (zmiana danych w trakcie ich przesyłania lub przekierowanie do „klona” dziennika internetowego), powinno zakończyć się sformułowaniem dwóch wniosków dotyczących bezpiecznego połączenia przeglądarki internetowej z serwerem WWW: należy zapewnić poufność (tajność) oraz wiarygodność korespondencji, tj. możliwość potwierdzenia autentyczności serwera WWW.

Nauczyciel informuje uczniów, że w czasie kolejnych lekcji będą mieli możliwość poznać niektóre szczegółowe kwestie związane z osiągnięciami współczesnej kryptografii (m.in. kryptografia klucza publicznego, podpis elektroniczny), które zapewniają bezpieczeństwo połączenia z serwerami WWW (np. banku).

Zasadnicza część lekcji pierwszej (30-35 minut)

1. Aby przybliżyć uczniom wymaganie poufności danych, a przy tym pokazać znaczenie myślenia naukowego (komputacyjnego) dla realizacji tego wymagania, nauczyciel może posłużyć się następującym zadaniem: *Mamy grupę osób w różnym wieku. Jak wyznaczyć średnią arytmetyczną wieku, jeśli żadna osoba w grupie nie może poznać wieku żadnej innej osoby?* Nauczyciel prosi, aby każdy z uczniów pomyślał o pewnej liczbie dwucyfrowej (to będzie wiek jednej z osób z wcześniej sformułowanego zadania). Każdy z uczniów otrzymuje małą kartkę. Uczniowie w dyskusji, kierowanej przez nauczyciela, szukają rozwiązania zadania (w razie potrzeby najpierw pytają o właściwe rozumienie treści zadania). Nauczyciel może zapytać o to, czy uczniowie w ogóle wierzą w istnienie rozwiązania zadania...

Rozwiązanie wymaga współpracy w grupie i polega na zaszyfrowaniuinformacji: jedna osoba zapisuje na kartce liczbę większą od swojego wieku (np. o 150), zapamiętuje tajny klucz szyfrowania (czyli różnicę między 150 i swoim wiekiem) i przekazuje kartkę innej osobie, która na innej kartce zapisuje liczbę, która jest sumą 150 i jej wieku (np. 165) i podaje kartkę kolejnej osobie (wcześniej otrzymaną kartkę powinna zniszczyć). Procedura jest powtarzana tak długo, aż ostatnia osoba w grupie nie zapisze liczby na kartce – wówczas ta kartka trafia do osoby, która rozpoczynała i która, znając liczbę osób w grupie, jest w stanie obliczyć szukaną wartość średnią.

(Jeśli nauczyciel obawia się, że ktoś z uczniów może nie stosować się do reguł, to może wcześniej poprosić uczniów, aby nie niszczyli kartek, ale oddawali je kolejno nauczycielowi.)

W czasie obliczania średniej (lub później) nauczyciel może dopowiedzieć, że system podobny do przedstawionego mógłby zostać użyty w celu zrealizowania tajnego głosowania: głosujący na „tak" dodawaliby do otrzymanej liczby liczbę 1 (oczywiście wymagana byłaby wtedy uczciwość głosujących).

Podsumowując, nauczyciel powinien odnieść się do jeszcze jednego wątku. Mianowicie informacji, że choć utrata pełnej anonimowości jest dość powszechnie akceptowana, to warto wiedzieć, że istnieją protokoły komunikacyjne, które służą do utrzymania poufności transakcji elektronicznych.

Opisane wyżej zadanie powinno pomóc uczniom uwierzyć w to, że wykorzystując osiągnięcia kryptografii (teorii i praktyki szyfrowania) będzie można zapewnić wysoki stopień bezpieczeństwa danych przesyłanych między serwerem WWW a przeglądarką internetową (tj. uczynić dalsze rozważania bardziej wiarygodnymi).

W tym momencie nauczyciel może wspomnieć o: Shafi Goldwasser i Silvio Micalim, dwojgu naukowców, którzy w roku 2013 zostali laureatami prestiżowej Nagrody Turinga, przyznawanej corocznie przez amerykańską organizację naukową ACM za wybitne osiągnięcia w dziedzinie informatyki. Wspomniani naukowcy zasłużyli się stworzeniem matematycznych podstaw współczesnej kryptografii, stosowanej dla bezpieczeństwa Internetu.

2. Następnie nauczyciel powinien, chociażby w minimalnym zakresie, zapoznać, uczniów (lub przypomnieć, jeśli to było przedmiotem wcześniejszych lekcji) z historią kryptografii i przykładami prostych, klasycznych szyfrów podstawieniowych (np. starożytny szyfr Cezara, jedna z wersji nowożytnego szyfru Vigenere'a). Może zacząć o zapytania uczniów o znane im przykłady klasycznych szyfrów. Jedna z osób może przedstawić konkretny przykład (np. szyfr Cezara czy metoda płotu – znane często wśród uczestników ruchu harcerskiego przykłady szyfrów odpowiednio: podstawieniowego i przestawieniowego). Nauczyciel powinien podkreślić, że szyfr Cezara (przykład szyfru podstawieniowego) i pojęcie szyfru przedstawieniowego są wymienione w podstawie programowej poziomu rozszerzonego.

   Do prowadzenia dalszej części lekcji nauczyciel może wykorzystać prezentację „Klasyczne szyfry podstawieniowe" oraz kartę „Alfabety". Uczniowie powinni mieć możliwość praktycznego sprawdzenia działania algorytmów (oraz ich łamania), używając zasobu „Klasyczne szyfry podstawieniowe" w postaci skoroszytu programu MS Excel lub OO Calc. (Zaszyfrowane są frazy: „W marcu jak w garncu" oraz „Byle do wiosny").

Podsumowanie lekcji pierwszej (5 minut)

Nauczyciel powinien podkreślić, że współcześnie w kryptografii uznaje się, że sposoby (algorytmy) szyfrowania mogą być powszechnie znane, tajny zaś musi pozostać jedynie klucz – newralgiczny element algorytmu szyfrującego (tzw. zasada Kerckhoffsa). Stworzone metody szyfrowania, które gwarantują bezpieczeństwo szyfrów, tzn. moc komputerów, jest zbyt słaba, by sprawdzić bardzo dużą liczbę możliwych kluczy oraz prowadzić analizę metodą prób i błędów. To jednak nie koniec problemów. Pojawia się bowiem problem tzw. dystrybucji klucza (musi istnieć niepodważalnie bezpieczny kanał dostarczenia klucza odbiory...)

Nauczyciel stwierdza, że udało się znaleźć zaskakujące rozwiązanie – inny klucz (publiczny) jest używany do zaszyfrowania wiadomości, a inny klucz (prywatny, czyli tajny) do odszyfrowania. Dopowiada, że konsekwencją jest podział metod szyfrowania na: symetryczne (ten sam klucz do szyfrowania) i asymetryczne (różne klucze odpowiednio do szyfrowania i deszyfrowania).

Zasadnicza część lekcji (35-40 minut)

3. Nauczyciel posługuje się prezentacją multimedialną „Bezpieczeństwo protokołu HTTP". W notatkach do prezentacji zapisane zostały bardziej szczegółowe informacje, które mogą posłużyć nauczycielowi w przygotowaniu lekcji (np. przygotowania zapisu na tablicy, który ułatwi uczniom prowadzenie notatek z lekcji). Zakłada się, że uczniowie znają model warstwowy sieci komputerowych (w szczególności znają rolę protokołu TCP).

   Nauczyciel powinien na bieżąco odpowiadać na ewentualne pytania stawiane przez uczniów, lub zapisywać te pytania i odpowiedzieć na nie już po zakończeniu wyświetlania prezentacji.

Podsumowanie (5-10 minut)

Na zakończenie nauczyciel powinien przedstawić uczniom następujące zestawienie istotnych cech kryptosystemów symetrycznych i asymetrycznych i podkreślić, że ich komplementarność (uzupełnianie się) skłaniają do zastosowania w praktycznych realizacjach obu typów przekształceń kryptograficznych i to w taki sposób, aby najlepiej wykorzystać cechy każdego z nich.

aspekt	symetryczne	asymetryczne
poufność danych	duża szybkość szyfrowania i deszyfrowania	
spójność (integralność) danych	duża szybkość generowania i weryfikowania znacznika MAC	
uwierzytelnienie serwera i niezaprzeczalność		łatwość generowania podpisu cyfrowego
wymiana kluczy		łatwa w realizacji

Nauczyciel zapowiada, że w czasie kolejnych dwóch lekcji omówiona zostanie idea szyfrowania z kluczem jawnym oraz ukazane działanie jednego z algorytmów (tzn. RSA).

Zadanie domowe 1

1. Zadanie domowe polega na uzupełnieniu głównego tekstu, z użyciem akapitów zapisanych pod tekstem. Brakujące akapity należy wstawić w odpowiedniej (logicznej) kolejności.

   Celem zadania jest oczywiście utrwalenie wiedzy, ale również wskazanie uczniom stopnia szczegółowości wymaganej wiedzy. W treści zadania jest używany trochę inny język od tego na slajdach prezentacji (dotyczy to między innymi pewnych porównań i objaśnień, być może zbędnych dla niektórych uczniów) – ze względu na samodzielną pracę w domu. Należy zaznaczyć, że w tekście stosowane są pewne uproszczenia i pominięte są pewne kwestie szczegółowe.
2. W ramach przygotowania do kolejnych lekcji, dotyczących kryptografii z kluczem jawnym (w tym: algorytmu RSA), uczniowie powinni przypomnieć sobie
   - pojęcia: liczby pierwsze, rozkład na czynniki (dzielniki) pierwsze, dzielenie całkowite, reszta z dzielenia, największy wspólny dzielnik,
   - algorytmy: algorytm Euklidesa, algorytm rozkładu liczby na czynniki pierwsze oraz algorytm sprawdzania, czy liczba jest pierwsza (test pierwszości).

Ocenianie

Nauczyciel może oceniać osiągnięcia uczniów na podstawie obserwacji ich pracy i zaangażowania na lekcji.

Dostępne pliki

1. Prezentacja 1 i 2: „Klasyczne_szyfry" oraz „Bezpieczeństwo HTTP"
2. Skoroszyt Klasyczne_szyfry_Cezara_Vigenerea.xls oraz Klasyczne_szyfry_Cezara_Vigenerea.ods (materiały pomocnicze 1 i 2)
3. Karta „Alfabet" (materiały pomocnicze 3)
4. Animacja „Podpis elektroniczny"
5. Schemat „Kryptografia Internetu" (materiały pomocnicze 4)
6. Zadanie domowe

Informacja o materiałach źródłowych

Podstawowymi materiałem źródłowymi przy tworzeniu scenariusza były następujące książki:

V. Ahuja, *Bezpieczeństwo w sieciach*, Warszawa 1997,

K. Gaj, K. Górski, A. Zugaj, *Elementarz kryptologii*, Warszawa 1999,

Technologie informacyjne, podręcznik internetowy dla studentów Uniwersytetu Warszawskiego (http://www.mimuw.edu.pl/~ewama/TI/ti-student.pdf, s. 72-80.

Załącznik A

Uzupełnij tekst, wstawiając brakujące akapity w odpowiedniej (logicznej) kolejności.

Bezpieczeństwo połączenia WWW wynika najpierw z potwierdzenia autentyczności serwera WWW oraz z szyfrowania przesyłanych informacji (aby nikt niepowołany ich nie odczytał ani tym bardziej nie zmienił...).

Zacznijmy od końca...

Po potwierdzeniu autentyczności serwera przeglądarka internetowa ustala tzw. klucz sesji (czyli klucz szyfrowania) i od tej pory informacje przesyłane są w postaci zaszyfrowanej z zastosowaniem kryptografii symetrycznej.

W jaki sposób klucz sesji przesyłany jest do serwera WWW? Jako tekst jawny?

.....

Nie! W żadnym wypadku! Do przesłania klucza sesji między przeglądarką a serwerem też używa się szyfrowania – stosuje się kryptografię asymetryczną!

.....

Co to znaczy, że stosujemy kryptografię asymetryczną? Krótko mówiąc: Inny klucz używany jest do szyfrowania informacji, a inny odszyfrowania kryptogramu. Klucz służący do szyfrowania (nazywany publicznym) może być udostępniony publicznie, bo na jego podstawie nie da się w praktyce odtworzyć klucza prywatnego służącego do deszyfrowania.

.....

Serwer udostępnia przeglądarce swój klucz publiczny (stanowi on element tzw. certyfikatu) i dopiero wówczas ta może przekazać w sposób bezpieczny klucz sesji, szyfrując go kluczem publicznym serwera.

Wracamy do początku...

Czy mamy jednak pewność, że serwer WWW, który przekazał swój klucz publiczny, był rzeczywiście tym, z którym miało być nawiązane połączenie? Odpowiedź brzmi: Nie! Użytkownik może stać się ofiarą tzw. ataku man-in-the-middle (problem tzw. *phishingu*).

.....

Istnieje więc konieczność potwierdzenia autentyczności klucza publicznego! W jaki sposób się to dokonuje?

Otóż kluczowi publicznemu serwera WWW (właściwie całemu otrzymanemu od niego certyfikatowi) powinien towarzyszyć podpis cyfrowy jednej z zaufanych organizacji autoryzujących.

.....

O podpisie cyfrowym...

Nadawca wiadomości tworzy tzw. skrót wiadomości, która ma być podpisana.

Skrót jest następnie szyfrowany kluczem... prywatnym twórcy wiadomości i jest załączany do oryginalnej wiadomości.

Odbiorca weryfikuje podpis postępując w następujący sposób: tworzy skrót odebranej wiadomości i porównuje go ze skrótem otrzymanym od nadawcy (oczywiście wcześniej musi go odszyfrować używając klucza... publicznego nadawcy).

.....

A	Jeśli właściciel serwera sam o to nie zadba (tzn. nie uiści odpowiedniej opłaty), to wówczas przeglądarka nie jest w stanie potwierdzić autentyczności serwera WWW i pojawia się informacja o potencjalnym zagrożeniu. Możemy kontynuować, ale nie będzie pewności, że informacje trafią do odbiory (a nie jego klona).	D	Dla przykładu: W jednej z metod szyfrowania klucz publiczny jest, nieco upraszczając, iloczynem dwóch wielocyfrowych liczb pierwszych, które stanowią klucz prywatny – problem faktoryzacji jest tak złożony obliczeniowo, że nie da się w nieodległej przyszłości na podstawie klucza publicznego odtworzyć prywatnego.
B	Wówczas serwer imitujący zbiera wszelkie treści (np. loginy i hasła) od niezorientowanych użytkowników, które później będą wykorzystane np. na prawdziwej stronie banku.	E	Warto w tym momencie przypomnieć sobie, czym był klucz szyfrowania w szyfrze Cezara czy metodzie płotu – na czym polegał problem konieczności przekazania klucza szyfrowania?
C	Ta metoda nie jest tak szybka do zrealizowania (tzn. jest złożona obliczeniowo), więc nie jest stosowana do szyfrowania całego połączenia, a tylko na użytek przekazania klucza sesji.	F	W przypadku podpisu cyfrowego certyfikatu mamy do czynienia odpowiednio z kluczem prywatnym i publicznym organizacji autoryzującej (przeglądarki internetowe posiadają klucze publiczne wielu zaufanych organizacji autoryzujących).

LEKCJA NR 3-4

TEMAT: Kryptografia klucza publicznego. Algorytm RSA

Streszczenie

Osiągnięciem współczesnej kryptografii jest to, że potrafimy zaszyfrować wiadomość jednym kluczem (publicznie dostępnym), ale do jej odczytania potrzebny jest inny klucz (prywatny) znajdujący się u odbiorcy wiadomości.

W czasie tych zajęć zostanie opisany sposób realizacji powyższego modelu szyfrowania.

W drugiej części lekcji przedstawiony zostanie poglądowy opis algorytmu RSA (opisany w roku 1978), który jako jeden z nielicznych kryptosystemów asymetrycznych oparł się próbom ataku i stał się de facto, na długie latam standardem.

Podstawa programowa

Etap edukacyjny: IV, przedmiot: informatyka (poziom rozszerzony)

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

III. Rozwiązywanie problemów i podejmowanie decyzji z wykorzystaniem komputera, z zastosowaniem podejścia algorytmicznego.

V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Treści nauczania – wymagania szczegółowe

1.3b. Uczeń prawidłowo posługuje się terminologią sieciową, korzysta z usług w sieci komputerowej, lokalnej i globalnej, związanych z dostępem do informacji, wymianą informacji i komunikacją;

2.5. Uczeń opisuje mechanizmy związane z bezpieczeństwem danych: szyfrowanie, klucz, certyfikat;

4.4. Uczeń wykorzystuje arkusz kalkulacyjny do zapisywania algorytmów;

5.11c. Uczeń opisuje i stosuje algorytmy na liczbach całkowitych:

- sprawdzanie, czy liczba jest liczbą pierwszą,
- rozkładanie liczby na czynniki pierwsze,
- iteracyjna realizacja algorytmu Euklidesa,
- szybkie podnoszenie do potęgi,

5.11e. Uczeń opisuje szyfr z kluczem jawnym (RSA) oraz wykorzystanie algorytmów szyfrowania w podpisie elektronicznym;

7.3. Uczeń stosuje normy etyczne i prawne związane z rozpowszechnianiem programów komputerowych, bezpieczeństwem i ochroną danych oraz informacji w komputerze i w sieciach komputerowych.

Cele operacyjne

Uczeń:

- wyjaśnia koncepcję kryptografii z kluczem jawnym (klucz publiczny a klucz prywatny), posługując się analogiami (np. kłódka zapadkowa, zbiór dominujący w grafie),
- rozumie, że bezpieczeństwo algorytmu szyfrowania z kluczem jawnym (asymetrycznego) opiera się na trudności obliczeniowej (np. problemu rozkładu liczby na czynniki pierwsze),
- wyjaśnia zastosowanie kryptografii asymetrycznej w celu zapewnienia bezpieczeństwa komunikacji w Internecie,

– opisuje etapy realizacji algorytmu RSA,
– dostrzega zastosowania algorytmów: Euklidesa oraz szybkiego podnoszenia do potęgi,
– posługuje się oprogramowaniem (np. arkuszem kalkulacyjnym), które służy do symulacji działania algorytmu RSA.

Słowa kluczowe

kryptografia z kluczem jawnym (asymetryczna), klucz publiczny, klucz prywatny, funkcja jednokierunkowa, liczba pierwsza, rozkład na czynniki pierwsze (faktoryzacja), algorytm Euklidesa

Co przygotować?


- Karta pracy „Klucz publiczny" (załącznik B , materiały pomocnicze 5)
- Film „Jak działa algorytm RSA?" (http://www.amara.org/pl/videos/cBmecV5lqtd7/info/rivest-shamir-adleman-the-rsa-algorithm-explained/)
- Skoroszyt „Jak działa RSA?" (materiały pomocnicze 6)

Przebieg zajęć

Wprowadzenie (5-10 minut)

Nauczyciel może posłużyć się następującą narracją: „Wyobraźmy sobie, że 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". Wskazane jest, aby nauczyciel przygotował kilka kłódek zatrzaskowych...

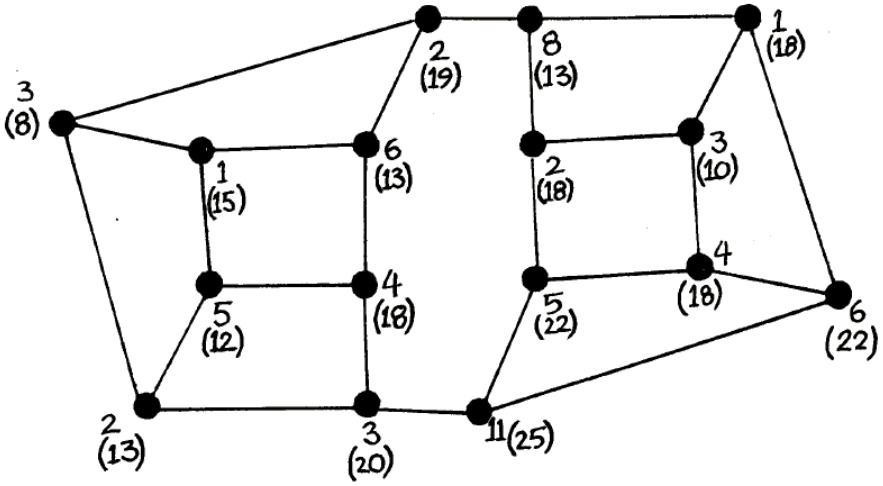
Następnie nauczyciel stwierdza, że w czasie pierwszej lekcji w sposób poglądowy wyjaśniona zostanie idea kryptografii asymetrycznej, a w czasie drugiej lekcji ukazany zostanie (na przykładzie) sposób realizacji powyższego modelu szyfrowania na przykładzie algorytmu RSA, stosowanego powszechnie w praktyce (m.in. do przekazania klucza sesji w połączeniu HTTPs).

Zasadnicza część lekcji pierwszej (30-35 minut)

1. Nauczyciel przedstawia uczniom problem, używając takich lub podobnych słów: „Emilia zamierza przekazać Wojtkowi poufną wiadomość. Cała wiadomość to tylko jedna tajemnicza liczba. Emilia, będzie stosować zasady określone publicznie przez Wojtka i w ten sposób zaszyfruje 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".
2. Nauczyciel wyjaśnia, że klucz publiczny (służący do szyfrowania) i klucz prywatny (służący od odszyfrowania) będą miały postać grafów, które można taktować jako mapę (plan) ulic i skrzyżowań pewnego miasta.

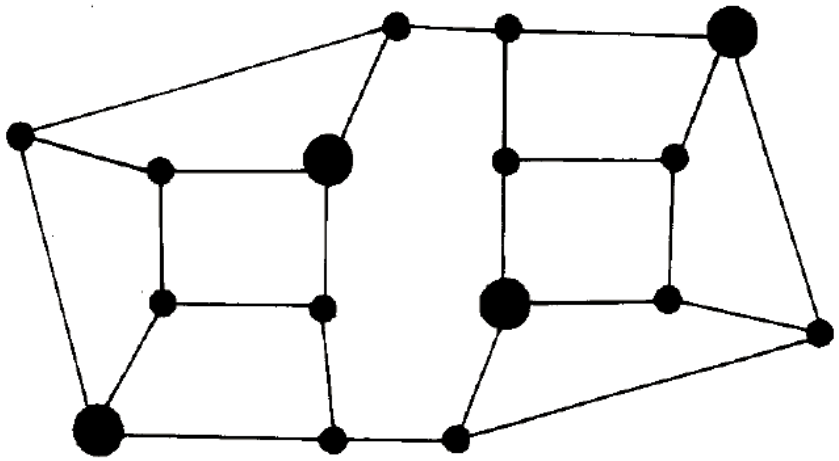
   W czasie zajęć wszyscy uczniowie powinni być zaangażowani w pracę – jest jej sporo. Nie jest trudna, ale wymaga dużej dokładności. Pomyłka będzie mieć negatywne konsekwencje. Ważne, by uczniowie dostrzegli brak oczywistości możliwości takiego asymetrycznego sposobu szyfrowania informacji. Jeśli nie pojawią się u nich wątpliwości co do tego, że jest to w ogóle możliwe, nie będą mieć odpowiedniej motywacji do wysiłku, który będą musieli włożyć w pracę.
3. Nauczyciel rysuje na tablicy mapę (klucz) publiczny Wojtka.

Wybiera liczbę, którą Emilia będzie miała przesłać. W miejscach skrzyżowań umieszcza 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 nich znajdowały się też liczby ujemne.)



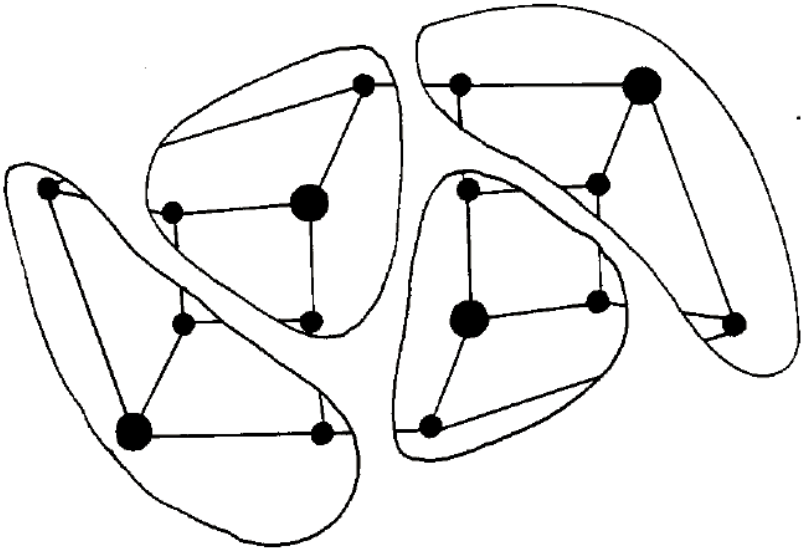
4. Nauczyciel podkreśla to, że Emilia nie może przesyłać do Wojtka w jawny sposób liczb, które wpisane zostały na publicznej mapie. Gdyby wpadły w niepowołane ręce, to ktokolwiek po ich zsumowaniu poznałby treść wiadomości. Dlatego Emilia powinna wykonać następujące obliczenia: przy każdym skrzyżowaniu 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). Nauczyciel powinien więc wymazać liczby napisane na początku (składniki) i zapisy obliczeń albo na nowym szablonie mapy zapisać tylko sumy. Można się łatwo przekonać, że uczniowie biorący udział w zajęciach nie będą w stanie odtworzyć liczb-składników (chyba że zapamiętali niektóre z nich).
4. Nauczyciel stwierdza, że tylko ktoś, kto jest w posiadaniu klucza prywatnego Wojtka może odtworzyć treść przesyłanej przez Emilię wiadomości. Informuje uczniów, że na prywatnej mapie wyróżnione są niektóre ze skrzyżowań – stanowią one klucz potrzebny do odszyfrowania.

Uwaga: Na poniższym rysunku pokazana jest natomiast wersja poufna (prywatna) mapy Wojtka. Różni się od wersji publicznej tym, że niektóre ze skrzyżowań są wyróżnione (pogrubione).



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 sąsiednie zaznaczył obwodem, a następnie powtórzył tę procedurę dla kolejnych dbając o to, by cała mapa została podzielona na rozłączne kawałki (jak na rysunku).



Uczniowie powinni dostrzec to, że liczby pierwotnie zapisane przy 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.

6. 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.

7. Od tego momentu uczniowie powinni pracować w grupach czteroosobowych. Każda para w grupie powinna otrzymać mapę publiczną (załącznik B). Grupa 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.

Podsumowanie lekcji pierwszej (5-10 minut)

Nauczyciel powinien zwrócić uwagę na ograniczenia analogii, zastosowanej na początku lekcji – zauważa, że 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 kopii wiązałoby się z odkryciem tajemnicy pasującego do niej klucza. W świecie cyfrowym ten problem nie istnieje, tzn. że Wojtek mógłby zamieścić klucz publiczny na stronie internetowej tak, aby każdy mógł ją zobaczyć (albo ograniczyć się tylko do wręczenia jej zainteresowanej osobie, która chce wysłać do niego wiadomość).

Zasadnicza część drugiej lekcji (35-40 minut)

1. Nauczyciel powinien posłużyć się krótkim filmem „Jak działa algorytm RSA?". (W filmie wypowiadają się twórcy algorytmu RSA: Ronald L. Rivest, Adi Shamir i Leonard Adleman. Zaprojektowali go w 1977 roku. W lutym 1978 roku opublikowali opis w amerykańskim czasopiśmie „Communications of the ACM". Algorytm od razu spotkał się z dużym zainteresowaniem zarówno w środowiskach akademickich, jak i w gospodarce. Dzisiaj jest powszechnie stosowany m.in. w szyfrowanej wersji protokołu HTTP do wymiany kluczy sesji. Jest też stosowany do podpisów elektronicznych w narzędziach do szyfrowania poczty elektronicznej, np. PGP).

   Warto wyświetlić film po raz drugi, zatrzymując i zapisując na tablicy własności algorytmu RSA (dodając kilka słów wyjaśnienia, np. o równoważności stwierdzeń „e i φ są względnie pierwsze" i NWD(e, φ)=1).

   Efekt końcowy powinien wyglądać tak:

   I. Generowanie kluczy

   P i Q – duże liczby pierwsze

   (Nauczyciel może dopowiedzieć, że klucze stosowane dzisiaj w realizacjach RSA to zwykle liczby co najmniej 1024-bitowe. Określenie duża liczba pierwsza oznacza więc liczbę rzędu $2^{512} \approx 1000^{50} = 10^{150}$, czyli liczby nawet kilkusetcyfrowe w zapisie dziesiętnym).

   $n = P \cdot Q$

   (Nauczyciel może dopowiedzieć, że liczba, która ma dokładnie dwa czynniki pierwsze, jest nazywana półpierwszą.

   $\varphi = (P - 1)\,(Q - 1)$

   (Warto dodać, że tradycyjnie przez φ oznacza się w teorii liczb funkcję Eulera, przypisującą każdej liczbie naturalnej ilość liczb względnie z nią pierwszych nie większych od niej samej. Dla liczb pierwszych wartość funkcji jest dość oczywista).

   NWD(e, φ) = 1

   (Nauczyciel może zapytać uczniów o równoważne stwierdzenie, które pojawiło się na filmie – o liczbach względnie pierwszych. Może dopowiedzieć, że w praktyce jako e używa się małych liczb pierwszych, np. 17, 37 albo 65 537).

   $e \cdot d \equiv 1 \pmod{\varphi}$

   (Warto dodać, że działania wykonywane są w arytmetyce modularnej, a efekty zapisywane jako tzw. relacje przystawania. Powyższą można traktować jak informację o tym, że reszta z dzielenia $e \cdot d$ przez φ jest równa 1. W praktyce liczbę d można znaleźć korzystając z tzw. rozszerzonej wersji algorytmu

Euklidesa).

<*n*, *e*> – klucz publiczny

<*n*, *d*> – klucz prywatny

(Nauczyciel może dopowiedzieć, po wygenerowaniu kluczy należy w sposób nieodwracalny usunąć liczby *p* i *q*. Znając *e* oraz *p* i *q* stosunkowo łatwo obliczyć *d*).

II.Szyfrowanie

$C \equiv M^e \pmod{n}$

(Nauczyciel może dodać, że C to pierwsza litera angielskiego słowo Cryptogram, a M – Message, czyli wiadomość).

III.Deszyfrowanie

$M \equiv C^d \pmod{n}$

(Można dodać, że liczby e i d, wybrane w sposób przedstawiony wyżej, mają taką własność algebraiczną, że dla każdego M < n zachodzi równość $C^d = (M^e)^d = M^{e \cdot d} \equiv M \pmod{n}$).

W tym momencie nauczyciel powinien stwierdzić, że w czasie lekcji będzie przedstawiona realizacja algorytmu RSA w arkuszu kalkulacyjnym i wówczas uczniowie będą mieli okazję, prześledzić działanie algorytmu w praktyce.

2. Jeśli czas i kompetencje uczniów na to pozwalają, to nauczyciel może w tym momencie podjąć wątek trudności (dużej złożoności obliczeniowej) rozkładu dużych liczb na czynniki pierwsze, czyli tzw. faktoryzacji (o czym była mowa na filmie). Aby ukazać tę trudność faktoryzacji, posługuje się przykładem obliczeń, które mają ilustrować (w pewnym uproszczeniu) atak na algorytm RSA tzw. metodą siłową (ang. *brute force attack*). (Warto, aby uczniowie brali aktywny udział w tej części lekcji – powinni być przygotowani do wykonania niektórych obliczeń i sformułowania niektórych odpowiedzi). Oto szkic:

   2.1. Nauczyciel stwierdza: „Załóżmy, iż dysponujemy superszybkim komputerem, który w ciągu jednej sekundy jest w stanie wykonać nawet miliard operacji dzielenia. Niech liczba półpierwsza *n* jest liczbą 128-bitową. Będziemy testować podzielność kolejnych liczb nieparzystych poniżej pierwiastka kwadratowego z *n*. Ile czasu zajmie nam znalezienie dzielnika liczby *n*?"

   2.2. Nauczyciel zadaje kolejne pytania. Uczniowie powinni uzasadniać odpowiedzi.

   – Dlaczego wystarczy badań liczby do pierwiastka kwadratowego z *n*?

   – Ile bitów potrzeba na zapisanie pierwiastka z 2^{128}? Odp. 2^{64}.

   – Ile jest wśród nich liczb nieparzystych? Połowa, czyli 2^{63}.

   2.3. Nauczyciel stwierdza, że w przypadku liczb, stosowanych dla RSA, czynnik pierwszy jest zawsze liczbą z górnej połowy zakresu. Oznacza to, że wystarczy sprawdzić podzielność „tylko" dla 2^{62} liczb.

   2.4. Nauczyciel pyta: Jak długo będzie trwać sprawdzanie choćby połowy z 2^{62} liczb?

   Odpowiedź (przybliżona) w sekundach: $\frac{1}{2} \cdot 2^{62}/10^9 > 2 \cdot (10^3)^6/10^9 = 2 \cdot 10^9$

   Odpowiedź (przybliżona) w latach: ok. 73 lat.

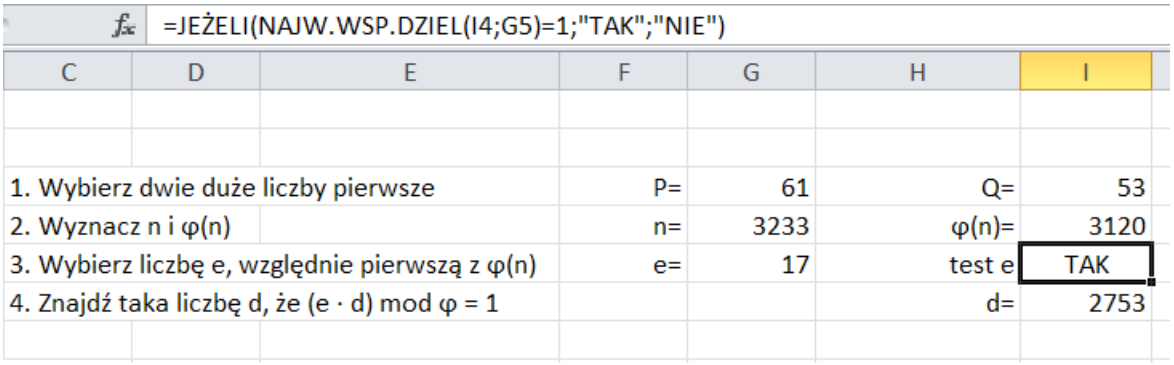
   2.5. Nauczyciel stwierdza, że istnieją szybsze metody faktoryzacji – wszystkie znane dzisiaj algorytmy działają jednak i tak w czasie wykładniczym względem długości rozkładanej liczby. I pyta uczniów o znaczenie ostatniego stwierdzenia: Ile razy wzrośnie czas przeszukiwania, jeśli liczbę zwiększyć o 10 bitów?

   Odpowiedź: Dla liczby o długości o 10 bitów większej, czas rośnie w przybliżeniu 2^{10} razy, czyli tysiąckrotnie.

   2.6. Nauczyciel podkreśla, że złamanie RSA jest równoważne obliczeniowo rozkładowi liczby *n* na czynniki pierwsze – mimo wielu lat badań nie udało się znaleźć ogólnej metody, przy pomocy której można odczytać tekst jawny z kryptogramu bez znajomości klucza prywatnego. Na tym fakcie opiera się bezpieczeństwo algorytmu RSA.

3. Następnie nauczyciel przedstawiona krok po kroku realizację algorytmu RSA w arkuszu kalkulacyjnym. Służy ona do zaszyfrowania liczby, a następnie jej zdeszyfrowania.

3.1. Nauczyciel omawia fragment arkusza, w której przedstawiony jest etap generowania kluczy:



Szczególnego komentarza wymaga na pewno zawartość komórek: I5 (zaznaczona na rysunku) oraz I6.

W pierwszym przypadku jest tam zapisana formuła, która służy do określenia trafności wyboru liczby *e* – powinna być ona względnie pierwsza z liczbą *φ*, czyli NWD(e, *φ*) musi być równy 1. W formule arkusza używana jest funkcja NAJW.WSP.DZIEL (szczegóły w pasku formuły). Może dopowiedzieć, że w praktyce jako e używa się małych liczb pierwszych, np. 17, 37 albo 65 537.

W drugim przypadku sprawa jest bardziej złożona – do wyznaczenia w sposób efektywny liczby *d*, która będzie stanowić element klucza prywatnego, można zastosować rozszerzoną wersję algorytmu Euklidesa dla liczb e i *φ*. Służy ona do znalezienia takich liczb całkowitych *s* i *t*, dla których $s \cdot \varphi + t \cdot e =$ NWD(*φ*, *e*) = 1. Realizacja algorytmu Euklidesa zapisana jest w drugim arkuszu (zakładce) skoroszytu RSA.xls. Nauczyciel może pominąć szczegóły (choć wówczas nie sposób zrozumieć działanie RSA i arkusz staje się dla ucznia „czarną skrzynką"). Ważne, aby uczniowie wiedzieli, że wartość t wyznaczona w ten sposób jest podstawiana za *d*.

3.2. Nauczyciel omawia fragment arkusza, w której przedstawiony jest proces szyfrowania.

Składa się on z dwóch kroków:

- zmiany reprezentacji liczby e na binarną (stosowana jest formuła z funkcją MOD, np. =MOD(B11;2) dla komórki D11)
- zastosowania algorytmu szybkiego potęgowania M^e (mod n), wykorzystującego binarną reprezentację wykładnika e (tzn. potęgowanie M^e jest realizowane jako ciąg mnożeń modulo n o czynnikach, które są odpowiednimi potęgami M o wykładnikach 1, 2, 4, 8 itd.).

Wiadomość (liczba mniejsza od n), która będzie szyfrowana zapisana jest w komórce C19. W kolejnych komórkach kolumny C wyznaczamy kolejne potęgi o wykładnikach 2, 4, 8 itd. wartości zapisanej w C19 (liczone modulo n). W komórce C20 mamy: =MOD(C19*C19;G4)

Postać zaszyfrowana jest tworzona iteracyjnie w kolumnie B:

- na początku w komórce B19 zapisujemy 1;
- w komórce B20 zapisujemy formułę =JEŻELI(D11=0;B19;MOD(B19*C19;G4)).

Krok 2:	Szyfrowanie		
1	Zmiana reprezentacji		
	e		
	17	8	1
	8	4	0
	4	2	0
	2	1	0
	1	0	1
2	Szybkie potęgowanie		
	C	M	
	1	**1500**	
	1500	3065	
	1500	2360	
	1500	2374	
	1500	757	
	717	808	

W przypadku e = 17 sprawa jest dość prosta, gdyż 17 = 16 + 1. To znaczy, że szyfrogram 717 powstaje w wyniku mnożenia $M \cdot M^{16}$ (mod n), tj. $1500 \cdot 757$ (mod 3233).

3.3. Nauczyciel informuję, że proces deszyfrowania jest realizowany podobnie.

Jeśli algorytm szybkiego potęgowania nie jest uczniom jeszcze znany, nauczyciel powinien zapisać przykład:

$717^{2753} = 717^{2048+512+128+64+1} = 717^{2048} \cdot 717^{512} \cdot 717^{128} \cdot 717^{64} \cdot 717^{1}$

7^1

$7^2 = (7^1)^2$

$7^4 = (7^2)^2$

$7^8 = (7^4)^2$

...

$7^{1024} = (7^{512})^2$

$7^{2048} = (7^{1024})^2$

Do wyliczenia potęgi bierzemy tylko te reszty, które występują w wyżej zapisanej sumie potęg 2. Nauczyciel zaznacza, że wszystkie operacje mogą być wykonywane modulo 3233 – wynika to ze wzoru ab mod n = (a mod n) · (b mod n) mod n).

3.4. Nauczyciel prezentuje działanie algorytmu dla innej wartości M (należy wybrać taką liczbę, która nie będzie wymagać zbyt wielu czynności dostosowania stosowanego wcześniej skoroszytu).

4. Uczniowie sprawdzają działanie algorytmu dla wybranych przykładów.

Powinni poświęcić sprawdzeniu działania algorytmu RSA odpowiednią ilość czasu również w domu. W razie potrzeby poprosić nauczyciela o konsultacje. W przeciwnym przypadku postrzegać będą algorytm RSA jako przykład poza ich zasięgiem (tzw. czarna skrzynka). W większości przypadków to nie jest prawda – algorytm nieprzypadkowo znajduje się wśród wymagań maturalnych.

Zadanie domowe 2

1. Każda para (wg podziału z pierwszej lekcji) ma zaprojektować swoją własną „mapę Wojtka". Wersję publiczną powinna „opublikować" na klasowej tablicy ogłoszeń. Uczniowie powinni 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. Każda para powinna też „opublikować" przykład szyfrogramu, który powstał po zastosowaniu „klucza publicznego".

2. *Dla zainteresowanych*

   Mimo wielu lat badań nie udało się znaleźć ogólnej metody łamania szyfru RSA, przy pomocy której można odczytać tekst jawny z kryptogramu bez znajomości klucza prywatnego. Istnieje taka metoda dla algorytmu „map Wojtka" – wystarczy zapisać odpowiedni układ równań kilku zmiennych. Zadanie uczniów polega na złamaniu kilku „szyfrogramów" z zadania domowego 1.

   Wskazówka: Należy zapisać odpowiedni układ kilku równań liniowych i go rozwiązać.

3. Zadanie polega na przygotowaniu opisu zagadnienia ataku kryptologicznego „Man in the middle" (pol. człowiek pośrodku). Uczniowie powinni zacząć od obejrzenia krótkiego filmu „Kryptografia klucza publicznego" (http://www.youtube.com/watch?v=jJrICB_HvuI), pochodzącego z zasobów projektu Computer Science Unplugged.

4. *Dla zainteresowanych*

   Zadanie polega na zaprogramowaniu algorytmu RSA. Uczniowie powinni pracować w grupach i podzielić się pracą nad implementacją różnych części składowych (np. poszczególnych algorytmów). Fazę tworzenia kodu musi oczywiście poprzedzić faza opracowania szczegółowej specyfikacji.

Ocenianie

Nauczyciel może oceniać osiągnięcia uczniów na podstawie obserwacji ich pracy i zaangażowania na lekcji oraz na podstawie prac przygotowanych w ramach zadania domowego.

Dostępne pliki

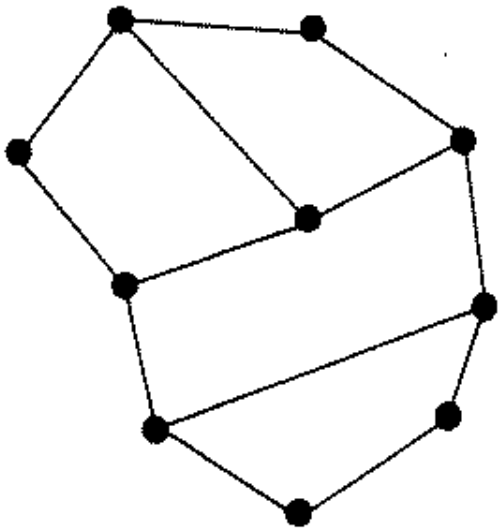
1. Materiały pomocnicze 5 i 6
2. Test

Informacja o materiałach źródłowych

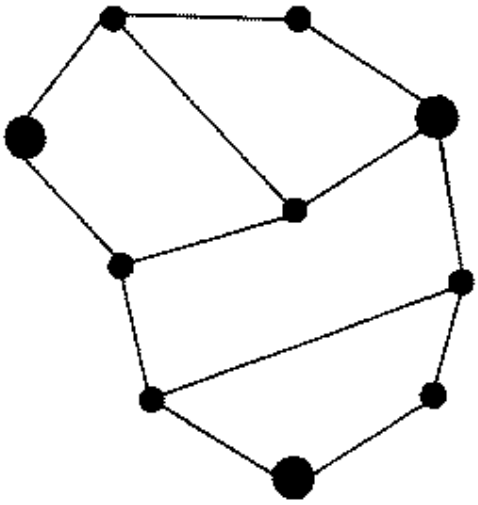
Nauczyciel może wykorzystać publikacje, które stanowiły inspirację do opracowania scenariusza: książkę M. Wrona, *Niebezpieczeństwo komputerowe*, Warszawa 2000, scenariusz „Młody kryptograf", pochodzący z zasobów projektu CSUnplugged (tłumaczenie na język polski jest dostępne na stronach projektu csunplugged.org) oraz publikację pokonferencyjną H. Zeng, *Teaching the RSA algorithm using spreadsheets*, dostępną w zasobach acm.org. Elementarny opis rozszerzonej wersji algorytmu Euklidesa można znaleźć np. w popularnonaukowej książce *Piramidy, szyszki i inne konstrukcje algorytmiczne*, napisanej przez prof. Macieja M. Sysłę.

Załącznik B

Zastosuj poniższe mapy do zaszyfrowania i odszyfrowania wybranej liczby:



mapa publiczna



mapa prywatna

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska
Wyższa Szkoła
Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego