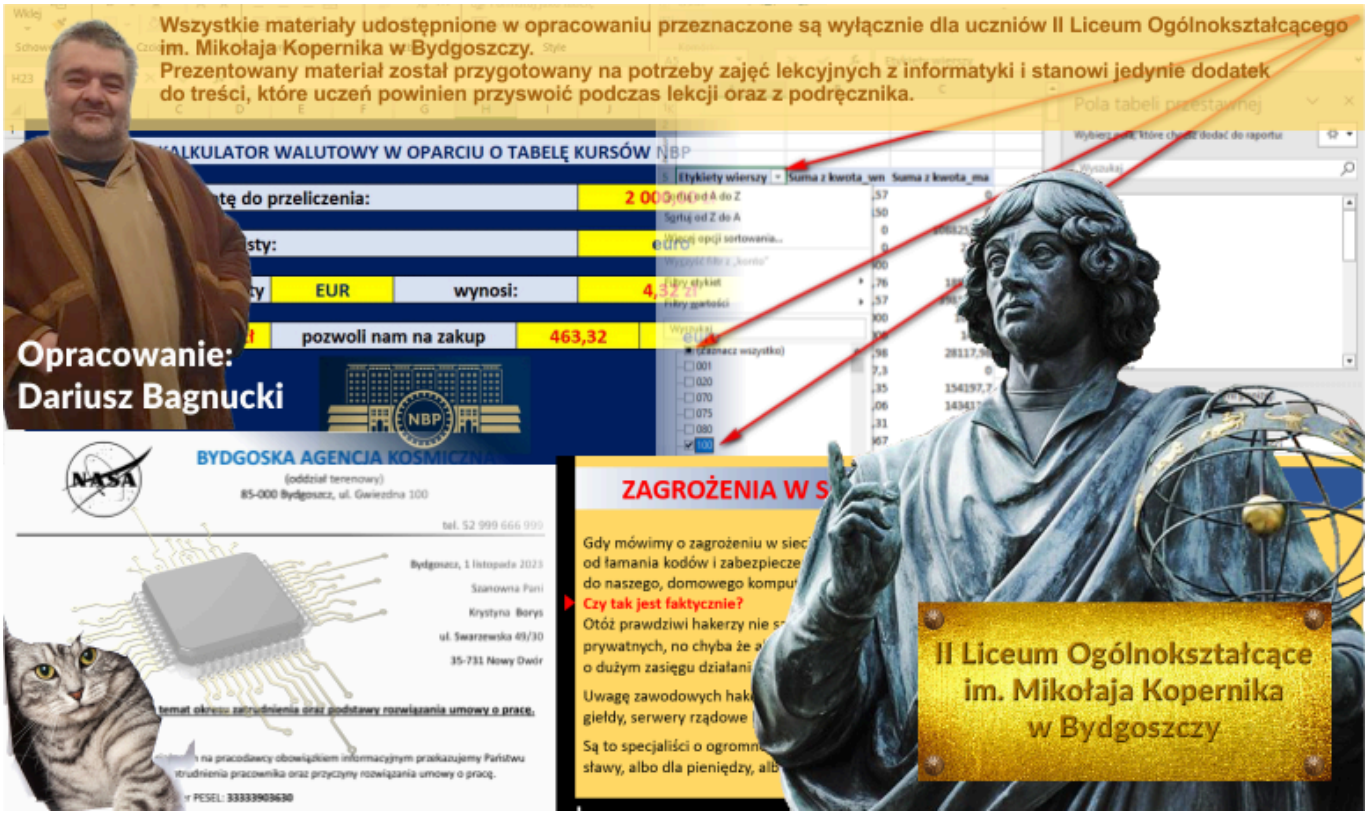


PROGRAMOWANIE – KRYPTOGRAFIA cz.1.

Cel lekcji:

Celem lekcji jest zapoznanie uczniów z pojęciem kryptografii.

Opowiemy sobie o tym, co kryje się pod pojęciem kryptografii, jakie korzyści można osiągnąć dzięki jej stosowaniu.

Podczas lekcji wykonamy prosty przyrząd do kodowania zwany maszynką Cezara.

Maszynka ta będzie wykorzystana na kolejnych zajęciach, na których przy jej pomocy będziemy rozkodowywać otrzymaną wiadomość.

Termin „kryptografia” wywodzi się ze starożytnej greki i składa się ze słów „cryptos” i „graphein”- co oznacza „tajemnica” i „pisać”.
Celem kryptografii jest szyfrowanie informacji w taki sposób, aby osoby nieuprawnione nie mogły ich odczytać.

Szyfrowanie wiadomości było stosowane od zawsze, a przynajmniej od czasu, gdy ludzie zaczęli powszechnie przekazywać sobie informacje przy pomocy pisma.

Z czasem szyfrowanie stawało się coraz bardziej powszechne. Od chwili, gdy w naszej rzeczywistości zagościł Internet, stało się ono wręcz konieczne.
Internet jest jawny i dostępny dla wszystkich. W sumie to dobrze, ale oznacza to również, że wszystko, co ludzie prześlą, może potencjalnie zostać przechwycone – jak pocztówka, którą może przeczytać każdy. Aby pokrzyżować szyki osobie nieuprawnionej, informacje muszą być przesyłane w postaci zaszyfrowanej.

Poziom szyfrowania jest wykładnikiem naszego bezpieczeństwa. Od niego zależy bezpieczeństwo naszych danych osobowych, kont bankowych, poczty elektronicznej oraz wielu bardzo ważnych informacji, które nie powinny być dostępne dla osób postronnych.

Metody kryptograficzne można podzielić na dwa rodzaje:

- szyfrowanie symetryczne

- szyfrowanie asymetryczne

Jak działa szyfrowanie symetryczne?

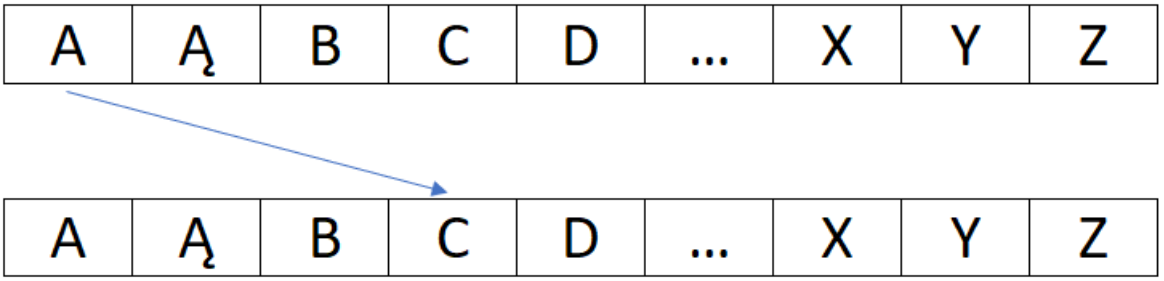
Wyobraźmy sobie następującą sytuację: Jacek chce wysłać Ani wiadomość przez Internet. Wiadomość ta zawiera poufne informacje, które nie powinny być czytane przez osoby postronne.
W sieci mamy jednak wiele ciekawskich osób, które bardzo chętnie poznałyby tajemnice Jacka i Ani.

Aby temu zapobiec Jacek poprzestawiał litery w swojej wiadomości przy użyciu specjalnego algorytmu kodującego.
Każdy, kto wszedł w posiadanie jego wiadomości widzi tylko i wyłącznie ciąg niezrozumiałych liter, który nie przedstawia dla niego żadnej wartości.

Niestety Ania otrzymała również ciąg liter, z których nic nie rozumie.
Z pomocą przychodzi jej jednak KLUCZ, który wcześniej przekazał jej Jacek.

Przy zastosowaniu tego klucza Ania może rozkodować otrzymaną wiadomość. Kluczem takim może być na przykład informacja, że każda litera w zakodowanej wiadomości jest przesunięta względem oryginalnego tekstu o trzy pozycje.

Oznacza to, że na miejsce litery A w oryginalnym tekście została wstawiona w tekście zakodowanym litera C.



Aby odkodować informację należy odwrócić działanie klucza, czyli w miejsce odczytanego z zakodowanego tekstu C należy wstawić literę A.

Podany powyżej przykład nazywany jest szyfrowaniem Cezara.

Nazwa pochodzi od imienia rzymskiego imperatora, który w ten sposób przekazywał rozkazy swoim wojskom, które w tamtych czasach podbiły prawie całą Europę oraz wiele krajów z poza niej. Dzięki temu trikowi rozkazy pozostawały niezrozumiałe dla jego przeciwników nawet w sytuacji gdy pojmano posłańca, a pisemny rozkaz wpadł w ręce wroga.

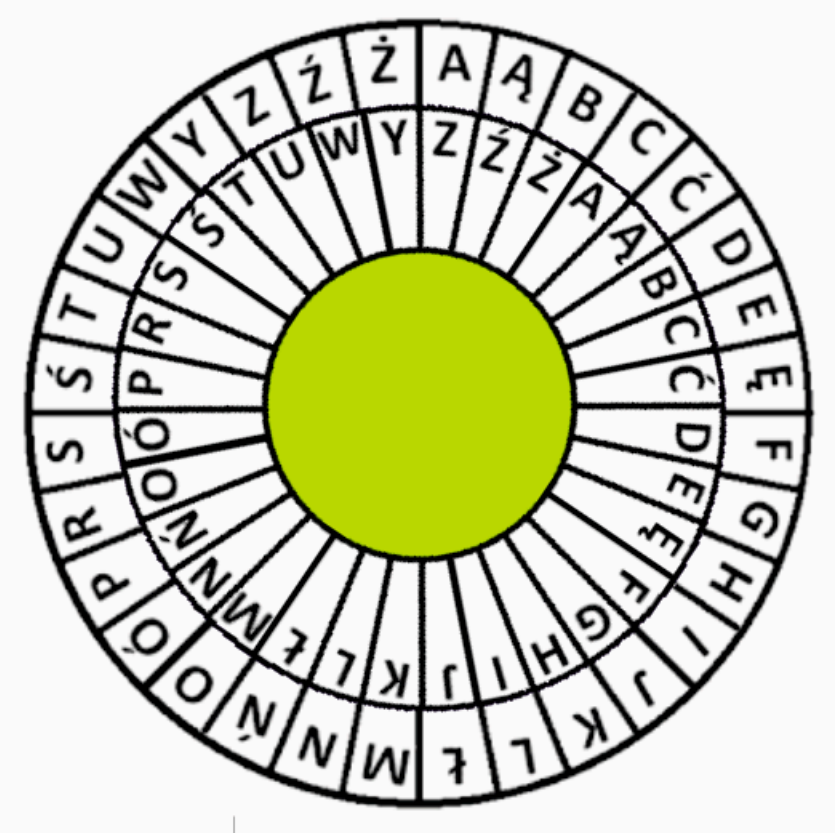
Nietrudno wyobrazić sobie co mogłoby się stać, gdyby obce wojska wiedziały o planach rzymskich legionów.
Banalnie prosty mechanizm przedstawiony na poniższej ilustracji pozwolił Cezarowi na sprawne dowodzenie legionami i zapewniał bezpieczeństwo przesyłanych informacji.

Maszynka Cezara składa się z dwóch współosiowo zamontowanych kół, które zostały podzielone na tyle części, ile liter znajduje się w alfabecie. W naszym przypadku koła podzielimy na 32 pola.

Do każdego pola wpisujemy kolejną literę alfabetu. Gdy koła są gotowe łączymy je współosiowo za pomocą pineski.

Ustawiamy oba koła w taki sposób, aby na kole większym i mniejszym litery się pokrywały, czyli pod A na dużym kole musi znajdować się A na kole mniejszym.

Następnie mniejsze koło obracamy o tyle znaków, ile wynosi przekazany nam wcześniej klucz.



Załóżmy, że nasz zakodowany tekst wygląda następująco:

Cduayżilmcóel

Na dużym kole szukamy litery C, odczytujemy znajdującą się poniżej literę na małym kole i zapisujemy ją na kartce.
W naszym przypadku odkodowaną literą będzie litera A.

Powtarzamy tą czynność tyle razy, ile mamy liter w zakodowanej wiadomości.
Po zakończeniu ujawni się nam pierwotny, czyli rozkodowany tekst.

W tym przypadku będzie to wyraz:

Absztyfikanci

Taką maszynę wykonamy na dzisiejszych zajęciach, aby przy jej pomocy rozkodować wiadomość, którą otrzymacie na kolejnej lekcji.

Wszystkie metody szyfrowania symetrycznego mają jedną wadę.

Cezar musiał wcześniej poinformować odbiorcę zaszyfrowanych listów za pośrednictwem posłańca, że alfabet zostanie przesunięty o 3 miejsca. Wiązało się to z koniecznością wysyłania dwóch posłańców, z których jeden niósł wiadomość, a drugi pasujący do jej odszyfrowania klucz. Rosło więc ryzyko, że jeden z nich nie dotrze do legionów i

powstanie ogromne zamieszanie, albo że pojmani zostaną obaj i wróg odczyta tajne informacje.

Kryptografowie starając się rozwiązać ten problem opracowali coś zupełnie nowego, bardziej zaawansowany system zwany szyfrowaniem asymetrycznym.

Jak działa szyfrowanie asymetryczne?

Rozważmy identyczną sytuację jak poprzednio.

Jacek chce przesłać wiadomość do Ani.

W tym przypadku Ania generuje dwa kody. Kod PUBLICZNY i kod PRYWATNY. Przesyła Jackowi kod PUBLICZNY, który może być przechwycony przez każdego bez narażenia wiadomości na odczytanie. Kod ten służy wyłącznie do kodowania wiadomości.

Aby ją rozkodować konieczne jest posiadanie obu kodów, PUBLICZNEGO oraz PRYWATNEGO. Przypominam, że kod PRYWATNY nigdy nie zobaczył światła dziennego i jest w wyłącznym posiadaniu Ani.

Ania mając oba kody rozszyfrowuje wiadomość od Jacka bez żadnego ryzyka ujawnienia jej treści.

Działanie obu metod zobrazowane jest w filmie, który został dołączony do lekcji, do obejrzenia którego serdecznie zapraszam.