



Szyfrowanie i deszyfrowanie – projekt

- [Wprowadzenie](#)
- [Przeczytaj](#)
- [Prezentacja multimedialna](#)
- [Sprawdź się](#)
- [Dla nauczyciela](#)



Z e-materiału [Wstęp do kryptografii](#) wiemy, do czego służą szyfry. Poznaliśmy też kilka algorytmów szyfrujących. Rozumiemy, jak działają, i potrafimy dokonać ich implementacji w różnych językach programowania.

Zdobytą wiedzę wykorzystamy do praktycznego opracowania projektu. W tym e-materiale zajmiemy się przygotowaniem do stworzenia własnego programu szyfrującego i deszyfrującego informacje. Skupimy się przede wszystkim na sformułowaniu stojących przed nami zadań – w ten sposób łatwiej nam będzie rozpocząć praktyczną realizację programu.

Z implementacją programu możesz zapoznać się w pozostałych e-materiałach z serii:

- [Szyfrowanie i deszyfrowanie w języku C++](#),
- [Szyfrowanie i deszyfrowanie w języku Java](#),
- [Szyfrowanie i deszyfrowanie w języku Python](#).

Więcej zadań? Sięgnij do: [Szyfrowanie i deszyfrowanie – zadania maturalne](#).

Twoje cele

- Przeanalizujesz proces wyboru algorytmu kryptograficznego przy założeniu konkretnych potrzeb i wymagań użytkownika.

- Zdecydujesz, w którym języku programowania wykonasz projekt.
- Wyjaśnisz, jak efektywnie organizować swoją pracę podczas tworzenia projektu oraz na jakie etapy można ją podzielić.
- Uzasadnisz, które podstawowe funkcje są niezbędne w projektowanym programie.
- Objąśnisz, jak powinien wyglądać przykładowy interfejs użytkownika.
- Przygotujesz się do implementacji wybranego algorytmu.

Przeczytaj

Wybór algorytmu szyfrowania i deszyfrowania

Przed przystąpieniem do analizy zadań projektowych, musimy najpierw zdecydować, jakie funkcje ma spełniać nasz program. W tym przypadku są to: szyfrowanie i deszyfrowanie informacji. Należy więc zadać sobie pytanie, w jaki sposób miałyby się odbywać cały proces. I spróbować rozwiązać kolejne kwestie, związane z tematem: czy zamierzamy korzystać z gotowych przetestowanych rozwiązań, czy może nasz program ma realizować innowatorskie, opracowane przez nas metody? Czy zależy nam na szyfrowaniu kluczowych informacji, ważnych dla bezpieczeństwa danych? Czy też priorytetem jest szybkość wykonywanych operacji? Czy szyfrować będziemy zdania, czy może ciągi liczb?

Podobnych pytań i wątpliwości może być wiele. Na potrzeby omawianego projektu pozostaniemy przy poznanych dotychczas algorytmach szyfrowania oraz deszyfrowania informacji. Możemy na przykład założyć, że zrealizujemy projekt programu, w którym wykorzystamy szyfr Cezara.

Analiza zadań projektowych

Gdy podjęliśmy już decyzję, jaki algorytm szyfrowania wykorzystamy, możemy przejść do analizy poszczególnych zadań projektowych. Jej przeprowadzenie przed przystąpieniem do praktycznej realizacji kodu programu może się wydawać zbędne, jednakże wbrew pozorom zaoszczędzi nam to wielu późniejszych poprawek projektu, a także uporządkuje harmonogram pracy. Ustalenie konkretnych zadań oraz ich kolejności podczas tworzenia projektu pomoże nam skupić się na aktualnych priorytetach. Wiemy na przykład, że obecna faza projektu to funkcja deszyfrująca informacje – i w tym momencie jest to jedyne, czym musimy się zająć. Łatwiej będzie nam wyobrazić sobie założone rezultaty na każdym z mniejszych etapów pracy niż ukończony program, a skupiając się jedynie na ostatecznym rezultacie, możemy pominąć wiele istotnych szczegółów.

Ostatecznie zrezygnowanie z analizy zadań projektowych pozornie zaoszczędzi nam trochę czasu, jednakże taka decyzja może skutkować dodatkowymi godzinami naprawiania możliwych do uniknięcia błędów. Spróbujemy więc przemyśleć, czym musimy się zająć podczas pisania programu kryptograficznego. Aplikacja powinna realizować szyfrowanie i deszyfrowanie z zastosowaniem algorytmu Cezara.

Najpierw należy podjąć decyzję, w jakim języku programowania napiszemy kod. Wybór ten może być determinowany wieloma czynnikami, jednak w naszym wypadku wybierzemy języki C++, Java oraz Python (praktycznej realizacji projektu w tych językach poświęcimy kolejne e-materiały).

W następnym kroku należy zastanowić się nad ogólną konstrukcją docelowego programu. Aby potencjalni użytkownicy mogli bez problemu odnajdywać potrzebne funkcje, program powinien być zaopatrzony w odpowiednie menu i interfejs. Obecność tych elementów to standard w dzisiejszych czasach i warto pomyśleć o nich również w przypadku naszego projektu. W menu znajdą się takie opcje jak **szyfrowanie**, **deszyfrowanie** oraz **wyjście**. Jest to podstawowy zbiór funkcji, który na potrzeby naszego programu będzie wystarczający. Musimy więc skonstruować odpowiednie menu, a następnie napisać poszczególne fragmenty kodu odpowiedzialne za trzy wspomniane opcje.

Najprostszą listę zadań możemy przedstawić następująco:

1. Wybór języka programowania.
2. Stworzenie menu zawierającego opcje **szyfrowanie**, **deszyfrowanie** oraz **wyjście**.
3. Stworzenie funkcji odpowiedzialnej za szyfrowanie.
4. Stworzenie funkcji odpowiedzialnej za deszyfrowanie.
5. Stworzenie funkcji odpowiedzialnej za wyłączanie programu.

Jest to bardzo ogólna lista zadań projektowych, jednak daje nam już wstępne informacje na temat realizowanego projektu.

Ważne!

Warto praktykować działania projektowe i analizować zadania różnego typu. Nawet w przypadku prostych, szkolnych projektów odpowiednie przygotowanie i zaplanowanie kolejnych kroków może zmienić, przyspieszyć przebieg całej pracy. [Zarządzanie projektami](#) to obecnie potężna dziedzina, którą zajmują się całe zespoły wykwalifikowanych w tym kierunku ludzi. Zdobyte teraz umiejętności, przydadzą ci się w pracy projektowej na studiach, a także podczas wykonywania obowiązków zawodowych.

Słownik

projekt

zbiór działań mający na celu stworzenie unikalnego produktu lub usługi w określonym czasie

zarządzanie projektami

działania, które obejmują planowanie projektu oraz kontrolę nad jego przebiegiem i zakończeniem

Prezentacja multimedialna

Polecenie 1

Przeanalizuj prezentację, w której krok po kroku przedstawiono poszczególne zadania w realizacji projektu programu szyfrującego oraz deszyfrującego tekst metodą szyfru Cezara.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Wybór języka programowania

W pierwszej kolejności należy wybrać język programowania, w którym będziemy realizować nasz program.

1

2

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Stworzenie menu z opcjami **szyfrowanie**, **deszyfrowanie** oraz **wyjście**.

Zanim przejdziemy do realizacji konkretnych funkcji, najpierw stworzymy menu. Gdy użytkownik wybierze konkretną opcję w programie, zostanie wywołana konkretna funkcja (na tę chwilę realizacji projektu jest ona jeszcze niegotowa).

3



Przykładowy wygląd menu

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

4

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Stworzenie funkcji realizującej opcję szyfrowania

Pierwszą realizowaną przez nas funkcją będzie ta odpowiedzialna za szyfrowanie podanej informacji. Wybrany przez nas szyfr to klasyczna metoda Cezara (przesunięcie z kluczem).

5

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Realizacja szyfrowania będzie wymagała od nas w zasadzie trzech elementów: pobrania tekstu

jawnego od użytkownika, zaszyfrowania podanej informacji oraz wypisania użytkownikowi szyfrogramu na ekranie. Zakładamy, że dane są wprowadzane przez użytkownika z poziomu klawiatury. Jest to proste i praktyczne rozwiązanie będące standardem w dzisiejszych programach. Po wykonaniu szyfrowania oraz wciśnięciu wybranego przycisku przez użytkownika nastąpi powrót do menu. Nie będziemy się zagłębiać w techniczne wykonanie poszczególnych elementów, ponieważ będzie ono zależało od wybranego języka programowania oraz sposobu realizacji konkretnych działań w szyfrowaniu Cezara.

6

**Program kryptograficzny
Szyfr Cezara**

Tekst jawny:

Szyfrogram:

Powrót

Przykładowy wygląd okna szyfrowania
Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

7

Stworzenie funkcji realizującej opcję deszyfrowania

W tym wypadku będziemy postępować analogicznie jak w poprzednim kroku. Deszyfrowanie metodą Cezara jest bardzo proste i polega jedynie na zmianie wartości klucza szyfrującego na przeciwną, a następnie ponownym wykonaniu szyfrowania. W efekcie otrzymamy tekst jawny.

8

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Ponownie podzielimy zadanie na trzy osobne czynności: pobranie szyfrogramu od użytkownika, wykonanie procesu deszyfrowania oraz wypisanie tekstu jawnego na ekranie. Po wykonaniu deszyfrowania oraz wciśnięciu wybranego przycisku przez użytkownika nastąpi powrót do menu.

9



Program kryptograficzny
Szyfr Cezara

Szyfrogram:

Tekst jawny:

Powrót

Przykładowy wygląd okna deszyfrowania

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/PZgSFijHk>

Stworzenie funkcji realizującej opcję wyłączenia programu

Ostatnim krokiem będzie już tylko stworzenie prostej funkcji kończącej działanie naszego programu.

Problem 1

Opracuj pseudokod algorytmu dla zaprezentowanego programu.

1

Sprawdź się

Pokaż ćwiczenia:   

Ćwiczenie 1



Dokończ zdanie.

Zagadnienie zarządzania projektami...

- ☐ jest przydatne jedynie dla menadżerów projektów w wielkich korporacjach.
- ☐ jest przestarzałe i nieprzydatne w XXI wieku.
- ☐ jest tożsame z zagadnieniem realizacji projektu.
- ☐ może się przydać nawet podczas prostych szkolnych projektów.

Ćwiczenie 2



Wskaż, jaką wartość przyjmuje klucz w klasycznym szyfrze Cezara.

- ☐ 13
- ☐ 5
- ☐ 2
- ☐ 3

Ćwiczenie 3



Wskaż, które z poniższych czynników mogą wpłynąć na wybór metody szyfrowania w projekcie programu kryptograficznego.

- ☐ Wymagania, by program realizował szyfrowanie w jak najkrótszym czasie.
- ☐ Przeznaczenie programu do szyfrowania wiadomości tekstowych.
- ☐ Odgórne wytyczne określone przez zlecniodawcę.
- ☐ Przeznaczenie programu do szyfrowania istotnych informacji bankowych.

Ćwiczenie 4



Wskaż, w jaki sposób odbywa się deszyfrowanie metodą Cezara.

- ☐ Na szyfrogramie ponownie zostaje przeprowadzona operacja szyfrowania, tym razem z odwrotną wartością klucza.
- ☐ Wszystkie litery szyfrogramu zostają przesunięte w tekście o trzy pozycje w lewo.
- ☐ Na szyfrogramie ponownie zostaje przeprowadzona operacja szyfrowania, tym razem z przeciwną wartością klucza.
- ☐ Deszyfrowanie w metodzie Cezara jest niemożliwe.

Ćwiczenie 5



Wskaż, jakie warunki muszą spełniać działania, by można było uznać je za projekt.

- ☐ Przyczyniają się do utworzenia unikalnego produktu lub usługi.
- ☐ Realizowane są przez co najmniej pięcioosobowy zespół.
- ☐ Przeprowadzane są w pewnym, określonym czasie.
- ☐ Przyczyniają się do masowego utworzenia wielu identycznych przedmiotów.

Ćwiczenie 6



Przyporządkuj odpowiednie czynności do poniższych grup.

Realizacja projektu

stworzenie interfejsu graficznego dla przygotowywanego projektu

sprawdzanie postępów poczynionych w pracach nad projektem

Zarządzanie projektem

wybór zespołu projektowego

napisanie funkcji realizującej szyfrowanie podanego tekstu

przeanalizowanie zadań projektowych

stworzenie menu dla przygotowywanego projektu

Ćwiczenie 7



Wskaż właściwy fragment, by poprawnie dokończyć każde ze zdań.

Analiza zadań projektowych...

może korzystnie wpłynąć na czas i efektywność realizacji projektu. ☐

nie gwarantuje żadnych korzyści i przyczynia się do mniejszej efektywności. ☐ **Zarządzanie**

projektami to...

zbiór działań mających na celu rozplanowywanie i kontrolę przebiegania projektu. ☐

zbiór działań mających na celu wytworzenie unikalnego produktu. ☐

Ćwiczenie 8



Uporządkuj czynności związane z pracą projektową.

Dobór metody, którą chcemy zrealizować nasz cel.



Realizacja projektu.



Uwzględnienie ograniczeń czasowych i zasobów ludzkich.



Pytanie o cel projektu. Co chcemy osiągnąć?



Podsumowanie: czy udało się osiągnąć cel? Jaki etap należy usprawnić?



Dla nauczyciela

Autor: Maurycy Gast

Przedmiot: Informatyka

Temat: Szyfrowanie i deszyfrowanie – projekt

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

I. Rozumienie, analizowanie i rozwiązywanie problemów na bazie logicznego i abstrakcyjnego myślenia, myślenia algorytmicznego i sposobów reprezentowania informacji.

II. Programowanie i rozwiązywanie problemów z wykorzystaniem komputera oraz innych urządzeń cyfrowych: układanie i programowanie algorytmów, organizowanie, wyszukiwanie i udostępnianie informacji, posługiwanie się aplikacjami komputerowymi.

IV. Rozwijanie kompetencji społecznych, takich jak: komunikacja i współpraca w grupie, w tym w środowiskach wirtualnych, udział w projektach zespołowych oraz zarządzanie projektami.

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

I. Rozumienie, analizowanie i rozwiązywanie problemów.

Zakres podstawowy. Uczeń:

2) stosuje przy rozwiązywaniu problemów z różnych dziedzin algorytmy poznane w szkole podstawowej oraz algorytmy:

b) na tekstach: porównywanie tekstów, wyszukiwania wzorca w tekście metodą naiwną, szyfrowania tekstu metodą Cezara i przestawieniową,

II. Programowanie i rozwiązywanie problemów z wykorzystaniem komputera i innych urządzeń cyfrowych.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

3) sprawnie posługuje się zintegrowanym środowiskiem programistycznym przy pisaniu, uruchamianiu i testowaniu programów;

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Przeanalizujesz proces wyboru algorytmu kryptograficznego przy założeniu konkretnych potrzeb i wymagań użytkownika.
- Zdecydujesz, w którym języku programowania wykonasz projekt.
- Wyjaśnisz, jak efektywnie organizować swoją pracę podczas tworzenia projektu oraz na jakie etapy można ją podzielić.
- Uzasadnisz, które podstawowe funkcje są niezbędne w projektowanym programie.
- Objaśnisz, jak powinien wyglądać przykładowy interfejs użytkownika.
- Przygotujesz się do implementacji wybranego algorytmu.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimediu i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. Chętni lub wybrani uczniowie przygotowują prezentacje na temat różnych szyfrów.
2. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Szyfrowanie i deszyfrowanie – projekt”. Uczniowie zapoznają się z treściami w sekcji „Przeczytaj”.

Faza wstępna:

1. Przedstawienie tematu i celów zajęć.
2. Prowadzący prosi uczniów, aby zgłaszali swoje propozycje pytań do tematu. Jedna osoba może zapisywać je na tablicy. Gdy uczniowie wyczerpią swoje pomysły, a pozostały jakieś ważne kwestie do poruszenia, nauczyciel je dopowiada.

Faza realizacyjna:

1. Uczniowie prezentują przygotowane przez siebie wystąpienia.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Prezentacja multimedialna”. Uczniowie wspólnie analizują prezentację, w której krok po kroku przedstawiono poszczególne zadania w realizacji projektu programu szyfrującego oraz deszyfrującego tekst metodą szyfru Cezara.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-8 z sekcji „Sprawdź się”. Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel ponownie wyświetla na tablicy temat i cele lekcji zawarte w sekcji „Wprowadzenie”. W kontekście ich realizacji następuje omówienie ewentualnych problemów z rozwiązaniem ćwiczeń z sekcji „Sprawdź się”.

Praca domowa:

1. Uczniowie proponują 3 tematy projektów, możliwych do realizacji w zespołach klasowych. Muszą sformułować cele, określić metodę działania i podać planowany czas wykonania zadań.

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj” można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.