

Rozważania o chacie GPT od miesięcy zajmują nie tylko ludzi związanych z rozwojem technologii, ale również dziennikarzy, literatów, etyków, i oczywiście nauczycieli. Chciałbym zaprezentować kilka przykładów wykorzystania sztucznej inteligencji na lekcjach informatyki w szkole ponadpodstawowej.

Jednym z ciekawszych działów informatyki jest kryptografia. Zaczynamy najczęściej od najprostszego szyfru Cezara, przy czym warto wspomnieć jaka jest jego historia. Szyfr ten powstał 100 lat przed naszą erą a dowiedzieliśmy się o tym z ChatGPT, korzystając ze strony OpenAI.

Nasze pytanie i odpowiedź

ST

Jak powstał szyfr Cezara



Szyfr Cezara, znany również jako przesunięcie Cezara, jest jednym z najprostszych i najstarszych znanych metod szyfrowania. Szyfr ten został nazwany na cześć Juliusza Cezara, rzymskiego wodza i polityka, który rzekomo go używał do komunikacji z sojusznikami.



Historia szyfru Cezara sięga około 100 lat p.n.e. Szyfr został opisany przez rzymskiego historyka Suetoniusza w jego dziele "Żywoty Cezarów". Według tej relacji Cezar stosował szyfr, w którym każda litera tekstu jawnego była przesuwana o trzy miejsca w prawo w alfabecie łacińskim.

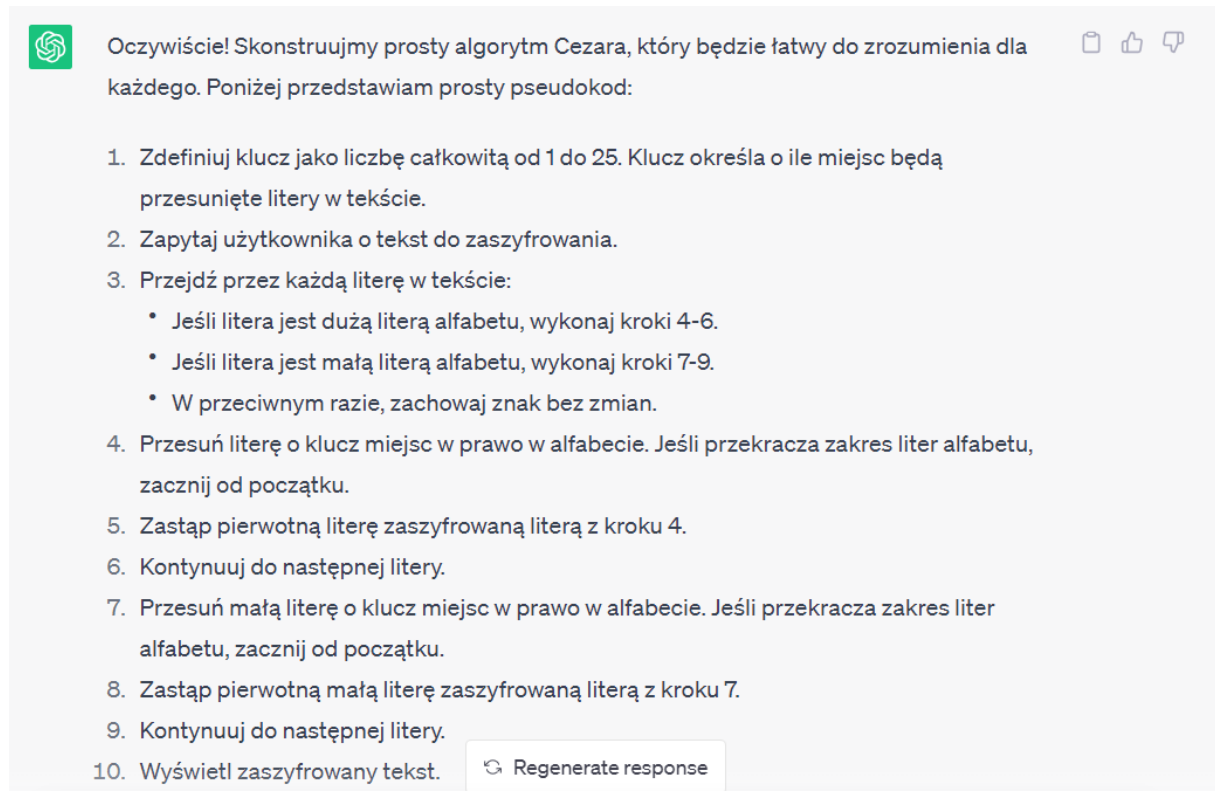
Przykładem zastosowania szyfru Cezara przez Cezara jest znane zdanie "HELLO" przekształcone w "KHOOR". Przesunięcie o trzy miejsca w prawo sprawia, że litera "H" staje się literą "K", "E" staje się "H", itd.

Szyfr Cezara był stosunkowo prosty i stosowany głównie do celów militarnej komunikacji. Przesunięcie o trzy miejsca w alfabecie łacińskim było stosunkowo niewielkie, co sprawiało, że szyfr można było łatwo złamać przez brute force lub analizę częstotliwości występowania liter w tekście.

Mimo że szyfr Cezara jest łatwy do złamania, ma on wartość edukacyjną i historyczną jako przykład wczesnej kryptografii. Dzięki prostocie i intuicyjności szyfrowania, szyfr Cezara jest często używany jako pierwszy krok w naukowym wprowadzeniu do kryptografii i szyfrów.

Po otrzymaniu odpowiedzi zastanawialiśmy się wspólnie z uczniami czy sztuczna inteligencja przedstawia prawdę? Postanowiliśmy zweryfikować to, pozyskując informację z trzech różnych źródeł. Pierwsza grupa przeszukiwała źródła Wikipedii, druga wyszukiwarkę Google, trzecia tradycyjną encyklopedię. Po zebraniu materiałów i jej weryfikacji najbardziej zbieżne z podaną odpowiedzią okazały się zasoby z biblioteki szkolnej a najmniej cyfrowe. Wspólnie z uczniami dyskutowaliśmy, na podstawie jakich danych ChatGPT wygenerował nam wyżej cytowany przykład? Dało się wyczuć wśród młodzieży zdziwienie i pewną nieufność do treści przedstawionej przez chat.

Nasze kolejne pytanie: *Skonstruuj prosty algorytm Cezara, który będzie łatwy do zrozumienia dla każdego* i odpowiedź:



Oczywiście! Skonstruujemy prosty algorytm Cezara, który będzie łatwy do zrozumienia dla każdego. Poniżej przedstawiam prosty pseudokod:

1. Zdefiniuj klucz jako liczbę całkowitą od 1 do 25. Klucz określa o ile miejsc będą przesunięte litery w tekście.
2. Zapytaj użytkownika o tekst do zaszyfrowania.
3. Przejdź przez każdą literę w tekście:
 - Jeśli litera jest dużą literą alfabetu, wykonaj kroki 4-6.
 - Jeśli litera jest małą literą alfabetu, wykonaj kroki 7-9.
 - W przeciwnym razie, zachowaj znak bez zmian.
4. Przesuń literę o klucz miejsc w prawo w alfabecie. Jeśli przekracza zakres liter alfabetu, zacznij od początku.
5. Zastąp pierwotną literę zaszyfrowaną literą z kroku 4.
6. Kontynuuj do następnej litery.
7. Przesuń małą literę o klucz miejsc w prawo w alfabecie. Jeśli przekracza zakres liter alfabetu, zacznij od początku.
8. Zastąp pierwotną małą literę zaszyfrowaną literą z kroku 7.
9. Kontynuuj do następnej litery.
10. Wyświetl zaszyfrowany tekst.

Regenerate response

Uczniowie stwierdzili, że jest bardziej czytelny od tych poznawanych w dotychczasowy sposób. Wspólnie stworzyliśmy kod i zaimplementowaliśmy go w Pythonie. Po wykonaniu zadania i testach sprawdzających postanowiliśmy skonfrontować nasz najlepszy, według opinii grupy, program ze sztuczną inteligencją, aby określiła nam: czy istnieje możliwość stworzenia bardziej optymalnego kodu? CzatGPT stwierdził, że jest poprawny i nie podjął wyzwania udoskonalenia naszego kodu. Uczniowie sformułowali wniosek, że AI w niektórych sytuacjach daje opinię wymijającą, przynajmniej na tym etapie.

Takie stosowanie metod na lekcji z wykorzystaniem sztucznej inteligencji uświadamia uczniom, że to nowoczesne narzędzie nie jest doskonałe, ale bardzo przydatne w zdobywaniu wiedzy, jej analizowaniu i może wspierać rozwój projektów uczniowskich. Postanowiliśmy zmodyfikować algorytm szyfru Cezara poprzez wstawienie w umowne miejsca dodatkowych znaków i poprosiliśmy ChatGPT o deszyfrację tych kodów. Nie udało mu się w początkowej fazie odszyfrować zadania, o dziwo poprosił o dodatkowe informacje: jaki użyto klucz, jakie były modyfikacje w szyfrze? Po pełnym podaniu brakujących danych w dalszym ciągu nie dawał rady z deszyfracją. Uczniowie byli zaintrygowani...

Ucząc szyfrowania warto korzystać z ChatGPT, gdyż w sposób przejrzysty generuje kod programu, ale także sięga do metod, których nie mamy w podręcznikach lub zasobach edukacyjnych. Inspiruje to do poszukiwania informacji i poszerza wiedzę o języku programowania.

Stanisław Szulc
Doradca metodyczny w zakresie informatyki
MSCDN Wydział w Ciechanowie
Nauczyciel informatyki w I LO w Ciechanowie