Список використаних джерел:

1. Істер О.С. Математика 6 клас: підручник для закладів загальної середньої освіти Ч.2. Київ: Генеза, 2023. 208 с.
2. Козлова О. М. Упровадження сучасних освітніх технологій як шлях підвищення ефективності навчання математики. Черкаси, 2018. 254 с.
3. Падалко Н. Й. Методика навчання математики : метод. посіб. Луцьк: Волин. нац. ун-т ім. Лесі Українки, 2021. 143 с.
4. Паралелепіпед. GeoGebra. URL: https://www.geogebra.org/m/HBcEjwZy.

РОЗГЛЯД ПРОТОКОЛУ ДІФФІ-ГЕЛЛМАНА В КУРСІ КРИПТОГРАФІЇ ЧЕРЕЗ ПРИЗМУ ЙОГО ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

Головін М. Б., Головіна Н. А., Гузачов Д. М.
Волинський національний університет імені Лесі Українки

У сучасних умовах високої **актуальності** набуває якісна підготовка спеціалістів з кібербезпеки, що забезпечують конфіденційність інформаційного обігу. Метод обміну криптографічними ключами за протоколом Діффі-Геллмана є важливою темою курсу криптографії, яка має кілька аспектів: математичний базис протоколу, програмна реалізація та сам протокол взаємодії.

Метою цієї роботи є розгляд лаконічної програмної реалізації обміну криптографічними ключами мовою Python в якості методичного засобу для пояснення, як алгоритму обміну, так і процесу налагодження цього обміну.

Нижче представлений код програми обміну криптографічними ключами.

```
# функція генерування ключа за залишком від ділення
def GenerateZalishokKey(PublicKey1, PublicKey2, PrivateKey):
    ZalishokKey = PublicKey1**PrivateKey
    ZalishokKey = ZalishokKey%PublicKey2
    return ZalishokKey
# функція генерування повного_ключа
def GenerateFullKey( PublicKey2, PrivateKey, ZalishokKey):
    FullKey = ZalishokKey**PrivateKey
    FullKey = FullKey%PublicKey2
    return FullKey
# функція шифрування дешифрування повідомлення
def ShifrDeShifr(FullKey, text):
    ShifrText = ""; FullKeyStr = ""    # початові значення змінних
    while len(text)>len(FullKeyStr): # цикл видовження ключа до довжини тексту
        FullKeyStr+=str(FullKey)
    for N in range(len(text)):          # цикл шифрування або дешифрування
        ShifrText += chr(ord(text[N])^int(FullKeyStr[N]))
    return ShifrText
textIn=input('Текст для шифрування, інакше <┘ ')
```

```
Private=int(input('Вводить свій ПРИВАТНИЙ (секретний)ключ  [751, 999] '))
Public =int(input('Вводить свій ПУБЛІЧНИЙ (несекретний)ключ-1- [515, 979] '))
otrPublic =int(input('Ввести отриманий ПУБЛІЧНИЙ ключ-1- [979, 515]'))
if textIn !='': Zalishok=GenerateZalishokKey (otrPublic, Public, Private);
if textIn =='': Zalishok=GenerateZalishokKey (Public, otrPublic , Private)
print('ПУБЛІЧНИЙ(несекретний)ключ-2-', Zalishok)
otrZalishok=int(input('Ввести отриманий ПУБЛІЧНИЙ ключ-2- [484, 419] '))
if textIn !='': FullKey=GenerateFullKey(Public, Private, otrZalishok)
if textIn =='':
    textIn=input('Вводь текст для дешифрування ')
    FullKey=GenerateFullKey(otrPublic, Private, otrZalishok)
TextOut=ShifrDeShifr(FullKey,textIn);
print('Шифрований або деШифрований текст: ', TextOut)
```

З тексту програми видно, що основні події, які відбуваються, реалізовані трьома наступними функціями: генерування ключа за залишком від ділення, генерування повного ключа та функції симетричного шифрування.

Саме тіло програми починається з пропозиції завантаження тексту для шифрування. Якщо текст для шифрування введено, то далі програма буде працювати в режимі шифратора. Ящо ж текст не введено і натиснутий ввід, то вважається, що далі буде дешифрування. Мінімалістичний інтерфейс програми пов’язаний з бажанням авторів мінімізувати кількість рядків програми, щоб зосередити увагу на механізмі обміну ключами і протоколі обміну.

Проведена успішна апробація цього програмного коду програми на лабораторному занятті з курсу «Криптографія і стеганографія».

На першому етапі заняття студентам була продемонстрована дія програми з відповідними поясненнями до коду і самого протоколу обміну.

На другому етапі, студентам пропонувалось скласти з перемішаних випадковим чином рядків програми текст діючої програми, відповідно відтворюючи всі її механізми, як правильною послідовністю рядків, так і відповідними програмними відступами, що утворюють систему підпорядкувань рядків. До перемішаних випадковим чином рядків були підмішані подібні але не правильні рядки [1]. Останнє, заставляло студентів при відтворенні програми концентрувати увагу і на сутності роботи окремих рядків. Зрозуміло, що такий підхід до курсу криптографії може мати успіх тільки за умови, якщо студенти пройшли попередньо курс практичного програмування на відповідній мові.

На третьому етапі заняття студентам ставилась задача перевірити роботу програми індивідуально користуючись підказками - числами в дужках, що знаходяться діалогових строкових константах, що пропонують ввод числових параметрів. Перше число, для шифрування, а друге для дешифрування.

На четвертому етапі заняття студенти розбиваються на пари і реалізують протокол обміну новими придуманими самотужки ключами. Кожен зі студентів працює на своїй машині, а ключі і шифрограму передають поштою. Успішна фіналізація кожним студентом роботи передбачає шифрування та відправку шифрограми, а потім отримання відповіді і дешифрування відповідного тексту.

Висновки. Представлений код оригінальної навчальної програми, що реалізує важливий для вивчення криптографії протокол обміну криптографічними ключами Діффі - Геллмана та симетричне шифрування і дешифрування.

Запропонована та апробована методика застосування цього програмного коду в процесі проведення відповідного лабораторного заняття.

Представлено пояснення сутності окремих етапів лабораторного заняття, а саме демонстрації роботи коду, відтворення коду в режимі конструювання, апробація протоколу обміну в ситуації наближеної до реальної.

Список використаних джерел:

1. Головін М.Б., Сомик О.І. Вивчення інформатики в контексті конструювання понятійних ієрархічних структур Вісник Харківського національного університету № 977, 2011. С.127-134 http://mia.univer.kharkov.ua/17/30205.pdf

ВИКОРИСТАННЯ ГЕЙМІФІКАЦІЇ НА УРОКАХ МАТЕМАТИКИ В НОВІЙ УКРАЇНСЬКІЙ ШКОЛІ

Горайчук О. П., Падалко Н. Й.

Волинський національний університет імені Лесі Українки

Актуальність теми. Створити умови для розвитку і самореалізації кожної особистості на уроках математики у 6 класі НУШ можливо із використанням нестандартних підходів. Зазначимо, що саме при навчанні математики в 6 класі, педагоги часто зустрічаємося з такою проблемою, як розсіяність дитячої уваги при вивченні нової теми.

Вирішення цієї проблеми можливе із застосуванням ігрових елементів у навчальному процесі. Зазначимо, що гейміфікація освітнього процесу створює стимул для активної пізнавальної діяльності при вивченні математики, перетворюючи навчання на захоплюючий ігровий процес. Використання ігрових елементів на уроках математики допомагає знизити страх перед математикою та збільшити зацікавленість учнів у предметі. Також, гейміфікація дозволяє індивідуалізувати процес навчання, пристосовуючи завдання та рівень складності до потреб кожного учня.

Розглянемо декілька ігор для 6 класу НУШ, які були апробовані на уроках математики в 6-х класах КЗ ЗСО «Вараський ліцей № 2» Вараської міської ради Рівненської області.

Мета. Показ доцільності використання гейміфікації на уроках математики в 6 класах НУШ.

Для вивчення та закріплення теми «Множення звичайних дробів» використовувалась цікава гра, під назвою «Дробова гонка».

Для її проведення слід до уроку підготувати картки з різними дробами на них. Кожна картка містить пару дробів для множення.