Тема: графічне кодування

Опис проблеми, вирішенню якої буде присвячено цикл домашніх завдань

В наш час доволі важко уявити мережу інтернет без шифрування. Паролі до акаунтів, банківських рахунків чи просто важливі дані для вузького кола - все це використовує методи шифрування. Зараз широке застосування отримала криптографія, яка дозволяє надійно передавати дані.

Шифрування ділиться на два типи за методами:

- Симетричне
- Асиметричне

Симетричне шифрування використовує один і той самий ключ, як для шифрування, так і для розшифрування.
Асиметричне шифрування використовує різні ключі на вході та виході, що робить його надійнішим.

Симетричне шифрування має багато недоліків, серед яких:

- часта заміна ключів
- складність тримати ключ в секреті, адже він є у двох осіб і може, як зашифрувати так і розшифрувати повідомлення.

Цей метод скоріше використовується в генерації псевдовипадкових чисел, або для шифрування, але в комбінації різних шифрів.

Асиметричне шифрування вирішує проблеми попереднього методу, адже воно використовує по одному закритому ключу, який не передається, для кожного учасника і один публічний, який і так відомий всім.
Звичайно і у цього метода є одна проблема:

- Він повільніший за симетричне шифрування в 4 рази, бо повідомлення передається між користувачами кілька разів.

Зараз для вирішення проблеми швидкості використовується комбінація обох методів, що робить шифрування більш надійним і швидким.

Я пропоную використати графічне шифрування, тобто перетворення utf символів в символи на зображенні. Цей спосіб шифрування радше належатиме симетричному методу, бо однакові ключі будуть мати обидва учасники. Це не так страшно, як в звичайних текстових шифрах таких, як шифр Віженера чи Цезаря, бо ключ даної програми - це два файли: з відповідністю кожного символа певній координаті в першому та файл з залежністю наступного символу від попереднього,

а не слово. Найцікавіше, що за такою методикою розшифрувати повідомлення буде неможливо без обох компонентів. Найменша помилка у крадія і він вже не отримує нічого. Закодований текст буде мати вигляд картини, схожої на карту сузір'їв, де кожен символ, це слово. Тоді, замість передавати текст, по-факту, користувачі передають один одному зображення, яке без повних даних розкодувати не вийде.

Вимога на систему

Спонсор проекту (Project Sponsor)

- Константиненко Ілля

Бізнес потреба (Business Need)

- Розробка надійної та естетичної системи шифрування, що може бути розкодована, лише якщо злодій має необхідне обладнання(програма) та секретні ключі.

Бізнес вимоги (Business Requirements)

- Можливість складно зашифрувати текст.
- Можливість представити текст у вигляді великого зображення.

Бізнес вигоди (користь) (Business Value)

- Два ключі забезпечують більшу надійність повідомлення.

Питання та обмеження (Special Issues or Constraints)

- Робота повинна бути виконана до 19 травня 2020 р.
- Термін виконання проекту не дозволяє опрацювати розкодування з зображення. Обов'язково треба встигнути шифровку і графічне зображення шифру.

Опис функціональних можливостей API

API для цього проекту відсутній.

Натомість буде використовуватись бібліотека вільного доступу OpenCV для Python

Дані будуть представлені двома способами:

- Png зображення

- Файл з набором точок вихідного зображення