МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Компьютерний практикум №1

З дисципліни: «Криптографія»

Виконали:
Студенти гр. ФБ-03
Гузенков А.М.
Сірховець А.М
Перевірив:
Чорний О.М.

Київ – 2022

Тема
Криптоаналіз шифру Віженера
Мета роботи
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.
Постановка задачі
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).
Хід роботи
Завдання 1,2
Підібраний текст знаходиться у файлі text.txt.

Результат виконання:
Індекс відповідності відкритого тексту: 0.056354960811769106
Індекс відповідності для шифротексту з ключем довжиною 2: 0.04542042017666244
Індекс відповідності для шифротексту з ключем довжиною 3: 0.03723239593358849
Індекс відповідності для шифротексту з ключем довжиною 4: 0.03760274927478446
Індекс відповідності для шифротексту з ключем довжиною 5: 0.038801700892041234
Індекс відповідності для шифротексту з ключем довжиною 11: 0.03612094212100648

Ключ	Індекс відповідності
'зе'	0.04542042017666244
'всу'	0.03723239593358849
'воин'	0.03760274927478446
'казак'	0.038801700892041234
'живилюбикпи'	0.03612094212100648

Завдання 3
Шифротекст згідно з варіантом знаходиться у файлі variant.txt; результат дешифрування у файлі variant_decrypted.txt; результат з корекціями у файлі variant_decrypted_corrected.txt; процес корекції у файлі correction.
У зв’язку з неточністю частотного аналіза були взяті фракменти шифротексту та відкритого тексту. Відкритий текст був зкоригований та на його основі був зкоригований ключ. Результат дешифрування зкоригованим ключем у файлі variant_decrypted_corrected.txt

Результати виконання:
Значення ключа, обраховане алгоритмом: уланобсеребзяныепуля
Дораховане вручну значення: улановсеребряныепули