Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Тема: “Криптоаналіз афінної біграмної підстановки”
Варіант: 7

Виконали: студенти Оласюк Олександр
групи ФБ-32 та Гарбар Дар’я
групи ФБ-33

Київ 2025

Мета роботи:
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Хід роботи:

Опис роботи запропонованого вами автоматичного розпізнавача російської мови (із обґрунтуванням коректності):
Скрипт реалізує автоматичний розпізнавач російської мови, який використовується під час дешифрування біграмного афінного шифру. Основною метою є перевірка, чи є розшифрований текст справжнім російським текстом, і таким чином визначити ключ.
Функція is_russian_text визначає, чи є текст російської мови на основі закономірностей частот літер та біграм:

```
def is_russian_text(text: str, verbose=False):
    if len(text) < 50:
        return False

    letters = Counter(text)
    total = len(text)

    common_letters = "оеаинтср"
    rare_letters = "фщъэ"

    common_freq = sum(letters.get(c, 0) for c in common_letters) / total
    rare_freq = sum(letters.get(c, 0) for c in rare_letters) / total
    typical_bigrams = ["ст", "но", "то", "на", "ен", "ов", "ра", "ко", "ор", "ер"]
    bigram_count = 0
    for i in range(len(text)-1):
        if text[i:i+2] in typical_bigrams:
            bigram_count += 1
    bigram_freq = bigram_count / (len(text) - 1) if len(text) > 1 else 0

    bad_bigrams = ["йй", "ыы", "ьь", "ъъ", "щщ", "жй", "фщ"]
    bad_count = sum(text.count(bg) for bg in bad_bigrams)

    if verbose:
        print(f"  Частота поширених літер: {common_freq:.3f}")
        print(f"  Частота рідкісних літер: {rare_freq:.3f}")
        print(f"  Частота типових біграм: {bigram_freq:.3f}")
        print(f"  Погані біграми: {bad_count}")

    return (common_freq > 0.35 and
            rare_freq < 0.08 and
            bigram_freq > 0.05 and
            bad_count < len(text) * 0.01)
```

Класифікація базується розподілі частот літер, частот біграм.

Знайдені п’ять найчастіших біграм шифртексту:

Шифрований та відповідний розшифрований тексти (відповідно до варіанту завдання):
*хетжщбеыжцллйшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеымюэвцфйжлцщвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошшйьтоюшцхоаимжоцллйшллебктяфлеьабуазгбшйьтошюййчажофщйленефцинебгбгугфязащ…….

атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишнимтысячиразиэтотольконочьюисел….

продовження у файлах . і . відповідно.

Знайдене значення ключа:

Висновок: