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:
Було реалізовано підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. Також за допомогою програми обчислення частот біграм знайдено 5 найчастіших біграм (нижче представлено топ5) запропонованого шифртексту та виконано їх дешифрування.
Розпізнавач аналізує частоти найпоширеніших російських літер, частоту типових біграм, а коректність забезпечується тим, що критерії базуються на закономірностях мови:

```python
def find_key_and_decrypt(cipher_text, verbose=True):
    top5_plain = ["ст", "но", "то", "на", "ен"]
    top5_cipher, freq = count_bigrams(cipher_text)
    if verbose:
        print("Топ-5 біграм шифртексту:")
        for bg in top5_cipher:
            print(f"  {bg}: {freq[bg]}")
    mod = m * m
    results = []
    tested = 0
    for p1, p2 in permutations(top5_plain, 2):
        X1, X2 = bigram_to_number(p1), bigram_to_number(p2)

        for c1, c2 in permutations(top5_cipher, 2):
            Y1, Y2 = bigram_to_number(c1), bigram_to_number(c2)
            a_candidates = solve_linear_congruence((X1 - X2) % mod, (Y1 - Y2) % mod, mod)

            for a in a_candidates:
                if gcd(a, mod)[0] != 1:
                    continue
                b = (Y1 - a * X1) % mod
                tested += 1
                decrypted = decrypt_text(cipher_text, a, b)
                if decrypted is None:
                    continue
                if verbose and tested % 1000 == 0:
                    print(f"Протестовано {tested} ключів...")
                if is_russian_text(decrypted):
                    results.append((a, b, decrypted, (p1, p2, c1, c2)))
    if verbose:
        print(f"\nВсього протестовано {tested} ключів")
        print(f"Знайдено {len(results)} потенційних розшифрувань")
```

```python
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)

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

Знайдені п’ять найчастіших біграм шифртексту:

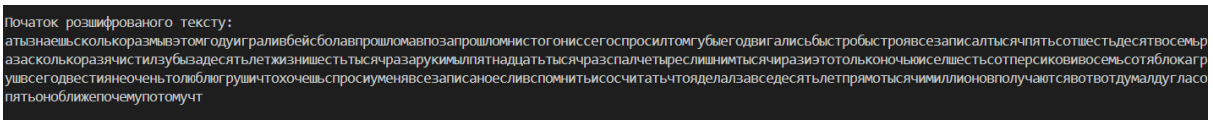
```
Топ-5 біграм шифртексту:
  цл: 51
  ял: 49
  ае: 43
  ле: 42
  чо: 39
```

Шифрований та відповідний розшифрований тексти (відповідно до варіанту завдання):

хетжщбеыжцллйшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеымюэвцфйжлцщвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошшйьтоюшцхоаимжоцллйшллебктяфлеьабуазгбшйьтошюййчажофщйленефцинебгбгугфязащ…….

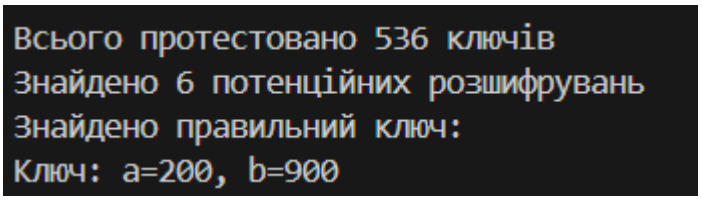
атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезаписал

тысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьле тжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишн имтысячиразиэтотольконочьюисел….



продовження у файлах 07.txt і decrypted.txt відповідно.

Знайдене значення ключа:
Ключ: a=200, b=900



Висновок:
було реалізовано криптоаналіз афінної біграмної підстановки: обробку шифртексту, розв’язання рівнянь для ключа (із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь) та саме дешифрування. Для автоматичного вибору правильного розшифрування було створено розпізнавач російської мови, що оцінює частоти літер і біграм.