Kryptografia i kryptoanaliza

Laboratorium 3

Michał Łaskawski

Zadanie 1

Zrealizować program implementujący podstawieniowy algorytm szyfrowania.

1. Wybrać fragment tekstu w języku angielskim.
2. Usunąć z niego wszystkie znaki nie będące literami (ograniczenie do 26 liter alfabetu łacińskiego).
3. Zaszyfrować tekst używając wybranego w sposób losowy klucza (tablicy podstawień): permutacji $\hat{\pi}$.

Zadanie 2

Mając do dyspozycji, otrzymany w ramach pierwszego zadania szyfrogram, dokonać ataku na zaimplementowany kryptosystem wykorzystując `Algorytm 1`:

Opis algorytmu - postać ogólna:

- Rozpocznij od początkowego przypuszczenia $\hat{\pi}$ dla permutacji dekodowania;
- Dla $\hat{\pi}$ oblicz wiarygodność: $\mathrm{Pl}(\hat{\pi})$ na zaszyfrowanym tekście;
- Powtórz następujące kroki dla wystarczającej liczby iteracji:
  - Zamień losowo $\hat{\pi}$ poprzez zamianę dwóch symboli z permutacji $\hat{\pi}$; nowa permutacja jest oznaczana jako $\hat{\pi}'$
  - Oblicz wiarygodność dla $\hat{\pi}'$: $\mathrm{Pl}(\hat{\pi}')$
    - Jeśli $\mathrm{Pl}(\hat{\pi}') > \mathrm{Pl}(\hat{\pi})$, to zachowaj $\hat{\pi}'$
    - W przeciwnym przypadku zachowaj $\hat{\pi}'$ z prawdopodobieństwem $\frac{\mathrm{Pl}(\hat{\pi}')}{\mathrm{Pl}(\hat{\pi})}$ oraz $\hat{\pi}$ z prawdopodobieństwem $1 - \frac{\mathrm{Pl}(\hat{\pi}')}{\mathrm{Pl}(\hat{\pi})}$

Uwagi:

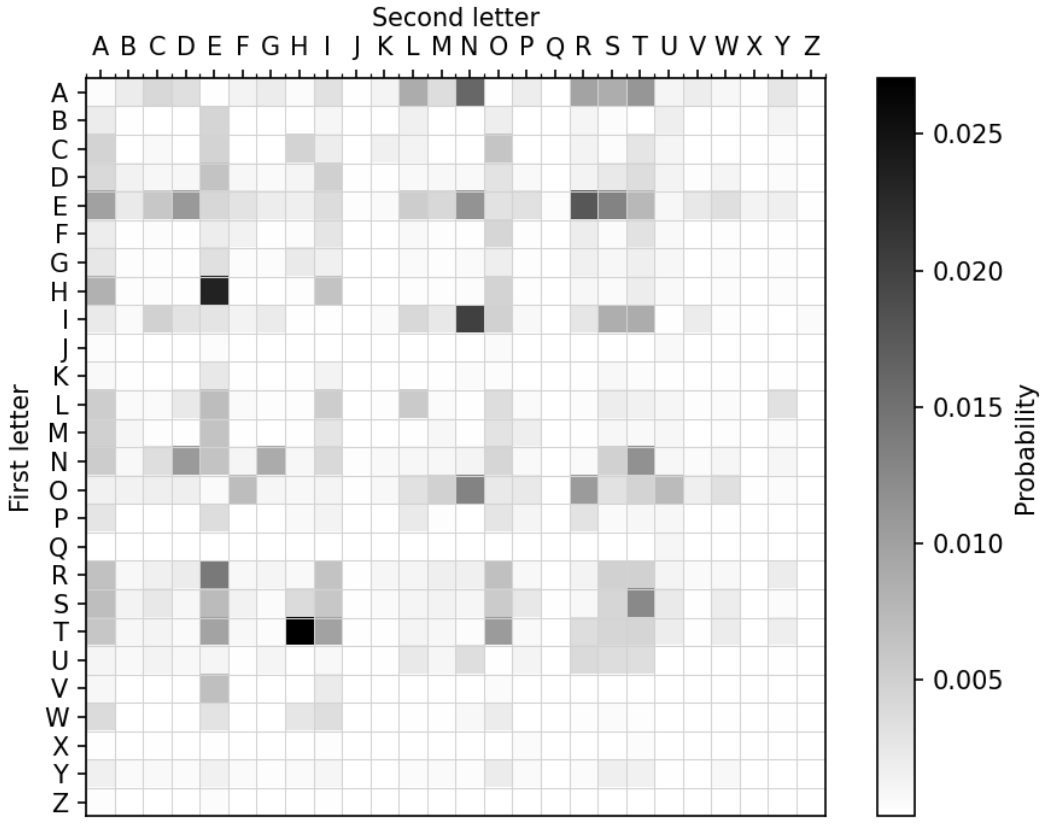
1. $\hat{\pi}$ - permutacja klucza (tablicy podstawień).
2. $\mathrm{Pl}(\hat{\pi})$ - funkcja wiarygodności zdefiniowana: $\mathrm{Pl}(\hat{\pi}) = \prod_{i,j} (M_{i,j})^{\hat{M}_{i,j}}$.
   - M - macierz bigramów utworzona na bazie tekstu referencyjnego, $M_{i,j}$ - liczba wystąpień pary (i, j) w tekście referencyjnym.
   - $\hat{M}$ - macierz bigramów utworzona na bazie szyfrogramu, $\hat{M}_{i,j}$ - liczba wystąpień pary (i, j) w szyfrogramie.
3. Dla danej permutacji $\hat{\pi}$, rozkład prawdopodobieństwa $q_{\hat{\pi}\hat{\pi}'} : \hat{\pi}' \in \chi$ jest zdefiniowany w następujący sposób:
   - $q_{\hat{\pi}\hat{\pi}'} = \frac{1}{26^2}$ jeśli przejście od $\hat{\pi}$ do $\hat{\pi}'$ może być dokonane przez losową zamianę dwóch wartości, oraz
   - $q_{\hat{\pi}\hat{\pi}'} = 0$ w przeciwnym przypadku.

   gdzie: χ to przestrzeń stanów wszystkich możliwych kluczy, które odpowiadają wszystkim możliwym permutacjom, w rozważanym przypadku wszystkich możliwych permutacji jest 26!.
4. Algorytm, na bazie funkcji wiarygodności, wygeneruje sekwencję kluczy deszyfrujących: $\{X_t : t = 0, \ldots, T\}$.
5. Jeśli $U(\{1, 2, \ldots, 26\})$ oznacza dyskretny rozkład jednostajny na liczbach całkowitych od 1 do 26, to ostatecznie implementacja algorytmu dla szyfru podstawieniowego przyjmuje postać:

Rysunek 1 przedstawia przykład macierzy bigramów dla tekstu referencyjnego:

Algorithm 1 MH

$t \leftarrow 0$
$X_0 \leftarrow \hat{\pi}_0$
for $t = 1, \ldots, T$ **do**
    dla $X_t \leftarrow \hat{\pi}$
    wygeneruj $i, j \sim U(\{1, 2, \ldots, 26\})$ ▷ $\sim$ znaczy ma rozkład
    wygeneruj $\hat{\pi}'$ ▷ zamieniając znaki na pozycjach i oraz j w kluczu $\hat{\pi}$
    $\rho(\hat{\pi}, \hat{\pi}') \leftarrow \frac{\mathrm{Pl}(\hat{\pi}')}{\mathrm{Pl}(\pi)}$ ▷ ρ - prawdopodobieństwo akceptacji
    wygeneruj $u \sim U([0, 1])$
    if $u \leq \rho(\hat{\pi}, \hat{\pi}')$ **then**
        $X_{t+1} \leftarrow \hat{\pi}'$
    else
        $X_{t+1} \leftarrow \hat{\pi}$
    end if
end for



Rysunek 1: Macierz bigramów