Cifras de Transposição e Substituição

Lucas Gabriel de Oliveira Lima - 231003406

16 de abril de 2025

Resumo

Neste trabalho, será apresentado conceitos de algoritmos de cifras de substituição e transposição. Com substituição, será trabalhado a criptografia e decriptograia por Ceasar Cipher, e também ataques ao Shift Cipher de modo cipher-text only, tanto por força bruta quanto por distribuição de frequência. Com transposição, será trabalhado a criptografia e decriptograia por Rail Fence Cipher, e também ataques a essa cifra de modo cipher-text only, tanto por força bruta quanto por distribuição de frequência. Além disso, será mostrado as partes principais do código-fonte da implementação desses algoritmos, utilizando a linguagem **C++**.

1 Introdução

Criptografia é uma forma de proteger dados, tentando modificar esses dados de forma que apenas o emissor e o receptor consigam saber o que ele de fato significa.

Nesse sentido, uma das formas de criptografia é a criptografia simétirica. Nela, as chaves de criptografia são privadas, ou seja, a chave que o emissor utiliza para criptografar o texto é a mesma para que no processo de decriptação o texto cifrado seja revertido para o texto original. Um ponto positivo dessa estratégia, se comparado à criptografia assimétrica, é que o algoritmo de criptografia tende a ser mais rápido. No entanto, caso alguma das parte deixe escapar a chave, a entidade que a obter teria mais facilidade para realizar a decriptação do dado.

Com isso, será trabalharemos estratégias de cifrar dados com criptografia simétrica, dando foco a duas formas de cifras principais: por **substituição** e por **transposição**.

Além disso, para cada um desse tipo de cifras, será realizado ataques simulando o papel de alguém que estária no meio do caminho entre emissor e receptor, tentando quebrar essas cifras contendo apenas o texto cifrado, ou seja, o atacante não tem conhecimento da chave privada.

Diante disso, utilizaremos duas abordagens principais de ataque para cada uma das diferentes formas de cifra: por **força bruta** e por **distribuição de frequência**. Por força bruta, tentamos todas as possíveis chaves e passamos por todas as diferentes combinações possíveis para o texto cifrado. Já por distribuição de frequência, partimos tendo em nosso conhecimento a frequência esperada de cada letra e cada digrama (duas letras juntas) no idioma que estamos trabalhando, e com isso calculamos uma pontuação com base na frequêcia das letras do texto que momentaneamente decriptamos, e com base nisso assumimos que o texto com melhor pontuação é o de maior probabilidade de corresponder ao texto original.

Para a quebra das cifras, foi-se utilizado os valores de frequência de letras e digramas no dicionário inglês. Como base, utilizamos o artigo *English Letter Frequency Counts: Mayzner Revisited or ETAOIN SRHLDCU* [May12]. No código-fonte, é possível encontrar esses valores no arquivo "Utils.hpp".

1.1 Instruções

O código-fonte do projeto pode ser encontrado no seguinte GitHub https://github.com/lucasdbr05 (link clicável direto para o repositório). Nele, há um arquivo README.md, no qual se encontra os comandos de compilação e execução do programa. A implementação dos requisitos pedidos no trabalho fei feito utilizando C++.

2 Cifra por substituição

Consiste em um método de encriptação onde cada caractere do texto original é substituido por um caractere diferente seguindo um padrão pré estabelecido, e de acordo com uma chave k. De inicio, cada letra do nosso alfabeto é mapeado a um respectivo número seguindo a ordem alfabética (A=0, B=1, C=2, ...).

Nesse processo utilizamos conceitos de aritmética modular. Algoritmos de **Shift Cipher** (cifra por substituição), dada uma chave k predefinada, texto original S, e texto resultante da encriptação C, cada caractere de C será dado pela seguinte fórmula:

$$C[i] = (S[i] + k) \mod 26$$

Tendo o texto cifrado C encripitado, para decriptografá-lo, basta aplicar a seguinte fórmula para cada caractere de C para obter o respectivo de S—:

$$S[i] = (C[i] - k + 26) \mod 26$$

Nessas fórmulas, (mod 26) corresponde ao resto positivo de um número inteiro na divisão por 26.

A seguir está a minha implementação da **Shift Cipher**:

```
#pragma once
#include <string>
using namespace std;

class ShiftCipher {
    private:
        int k;

        bool is_upper_case(char c) { return ('A' <= c && c <= 'Z'); }
        bool is_lower_case(char c) { return ('a' <= c && c <= 'z'); }

        char encrypt_char(char c) {
            if(is_upper_case(c)) {
                c = 'A' + (c - 'A' + k)%26;
            } else if(is_lower_case(c)) {
                c = 'a' + (c - 'a' + k)%26;
            }

            return c;
        }

        char decrypt_char(char c) {
            if(is_upper_case(c)) {
                c = 'A' + (c - 'A' - k + 26)%26;
            } else if(is_lower_case(c)) {
                c = 'a' + (c - 'a' - k + 26)%26;
            }
            return c;
        }


    public:
        ShiftCipher() {}

        ShiftCipher(int k) {
            this->k = k;
        }
        string encrypt(string message) {
            for(char &c: message) {
                c = encrypt_char(c);
            }
            return message;
```

```
        }

        string decrypt(string message) {
            for(char &c: message) {
                c =  decrypt_char(c);
            }
            return message;
        }

};
```

Um caso especial da cifra de substituição se trata da **Ceasar Cipher**, que segue as mesmas especifições descritas acima, com a chave $k = 3$.

2.1 Análise de Complexidade

Nos métodos de encriptar (encrypt) e decriptar (decrypt) do código acima, podemos ver, que em ambos, se itera pelo texto, que é uma operação *O(n)*, e que nessas iterações é aplicada uma operação no caractere, que tem custo *O(1)*. Com isso, vemos que a complexidade de encriptar e decriptar por Shift Cipher tem complexidade *O(n)*.

2.2 Quebra por força bruta

Para uma cifra de substituição, temos 26 diferentes chaves possíveis, pois todas elas pertencem a Z_{26}.

Com isso, basta iterarmos por todas as chaves e aplicar a função de decriptar utilizando k no texto cifrado para obter um novo texto cifrado. Com isso, realizariamos 26 vezes uma operação de decriptar, o que já discutimos ser *O(n)*, o que resultaria em uma complexidade de *O(26*n)*. A implementação da quebra por força bruta pode ser encontrada a seguir.

```

        vector<string> brute_force(string cipher_text) {
            vector<string> res;
            for(int k=0; k<26; k++) {
                shift_cipher = ShiftCipher(k);
                res.push_back(
                    shift_cipher.decrypt(cipher_text)
                );
            }
            return res;
        }
```

2.3 Quebra por distribuição de frequência

Para trabalharmos com distribuição de frequência, inicialmente verificamos a frequência das letras no texto cifrado, e então analisamos isso comparado à frequencia de letras esperada no nosso idioma.

Nessa analise, comparamos a letra mais frequente em nosso texto e, vamos comparando com as letras mais frequentes do idioma para, calcular o valor de k que seria esperado caso a letra mais frequente no texto cifrado correspondesse ao i-ésimo mais frequente no idioma. Então fazemos essa decripatação e calculamos o score do texto momentaneamente decifrado. Então, calculamos a pontuação para esses textos e consideramos o texto de melhor pontuação como o de maior probabilidade de corresponder ao texto original.

Esse processo é realizado comparando às 5 letras mais frequentes, que corresponde $\lfloor\sqrt{26}\rfloor$, que foi o que retornou resultados mais satisfatórios nos testes realizados. Com isso, temos uma complexidade de *O(5*n)*.

```
        string frequency_distribution(string cipher_text) {
            double best_score = utils.INF;
            int best_k = -1;
            string plain_text;
```

```
5
6               map<char, double> frequency = get_letters_frequency_in_text(
                    cipher_text);
7               vector<pair<double, char>> sorted_frequency =
                    get_letters_frequency_in_descending_order(frequency);
8
9               for(int i=0; i*i<26; i++) {
10                  int k = calculate_key(sorted_frequency[0].second, i);
11                  shift_cipher = ShiftCipher(k);
12                  string current_plain_text = shift_cipher.decrypt(cipher_text);
13                  double current_score = calculate_score(current_plain_text);
14                  if(current_score < best_score) {
15                      best_score = current_score;
16                      plain_text = current_plain_text;
17                      best_k = k;
18                  }
19              }
20              return plain_text;
21          }
```

Para realizar o cálculo da pontuação utilizamos a seguinte fórmula: FE = Frequência esperada de uma letra no idioma (percentual) FP = Frequência percebida de uma letra no texto (percentual) L = Conjunto com as 26 letras do alfabeto

$$score = \sum_{l \in L} |FE[l] - FP[l]|$$

E consideramos um score melhor quanto menor o seu valor. A seguir está a implementação da função de cálculo de score:

```
1           double calculate_score(string& text) {
2               map<char, double> letters_frequency =
                    get_letters_frequency_in_text(text);
3               double score = 0;
4
5               for(int i=0; i<26; i++) {
6                   score += abs(letters_frequency['A'+i] - utils.
                        letter_percent_occurrence[i]);
7               }
8               return score;
9           }
```

2.4 Conclusões

A cifra por substituição se apresenta como um estratégia muito simples de criptografia, se aplicada isoladamente. Ela apresenta algumas fraquezas, como ser fácilmente quebrável pelo método de força bruta.

Além disso, observa-se que em textos grandes, geralmente compensa mais aplicar a análise por distribuição de frequência, pois por ser probabilistico, quanto maior o espaço-amostral (tamanho do texto) ele tende a ter mais chances de acertar. Enquanto para textos menores, a força bruta tende a valer mais a pena, pois o tempo para executar o algoritmo tende a ser razoávelmente bom e combre os casos de erro utilizando distribuição de frequência.

3 Cifra de Tranposição

Consiste é um método de encriptação que permuta as posições dos caracteres sem modificar os valores dos caracteres. Um exemplo de cifra por transposição, é a Rail Fence Cipher. A cifra consiste em escrever o texto original, de tamanho n, em uma tabela de k linhas por n colunas, sendo este k a chave de criptografia desse algoritmo. Por fim, iteramos por cada linha dessa tabela, adicionando no

texto encriptado os caracteres que estão naquela linha. Por exemplo, para o texto "TRANSPOSITION CIPHER", seria gerado a seguinte tabela:
T***S***I***N***P***
*R*N*P*S*T*O* *I*H*R
A*O***I***C***E*

E então, após passar pelas linhas para montar o texto cifrado, obteremos o seguinte resultado: "TSINPRNPSTO IHRAOICE".

Para decriptografar, iteramos pelo texto cifrado, remontando a tabela, e fazemos o "zig-zag"para reconstruir o texto original.

A seguir está a minha implementação da **Rail Fence Cipher**:

```cpp
#pragma once
#include <string>
#include <vector>
using namespace std;

class RailFenceCipher {
    private:
        int k;
        vector<vector<char>> rails;

        int update_direction(int rail, int direction) {
            if (rail + direction == k) {
                direction =  -1; // change to go up
            }
            if(rail + direction < 0) {
                direction =  1; // change go down
            }
            return direction; // keep the direction
        }

        string recover_rails_text(bool encrypt) {
            string text = "";

            if(encrypt) { // for encypt text
                for(int i=0; i< k; i++){
                    for(auto c: rails[i]) {
                        if(c != '*') {
                            text += c;
                        }
                    }
                }
            } else { // for decrypt
                int direction = 1, rail = 0;
                int n = rails[0].size();
                for(int i=0; i<n; i++){
                    text += rails[rail][i];
                    direction = update_direction(rail, direction);
                    rail += direction;
                }
            }
            return text;
        }

    public:
        RailFenceCipher(){}

        RailFenceCipher(int n_rails) {
            this->k = n_rails;
        }
```

```
50
51          string encrypt(string message) {
52              int n = message.size();
53              rails = vector(k, vector<char>(n, '*'));
54
55              int rail = 0;
56              int direction = 1;
57
58              for(int i=0; i<n; i++){
59                  rails[rail][i] = message[i];
60                  direction = update_direction(rail, direction);
61                  rail += direction;
62              }
63
64              return recover_rails_text(true);
65          }
66
67          string decrypt(string cipher_text) {
68              int n = cipher_text.size();
69
70              rails = vector(k, vector<char>(n, '*'));
71              vector<int> rails_len = vector<int>(k, 0);
72
73              int direction = 1, rail = 0;
74              for(int i=0; i<n; i++){
75                  rails_len[rail]++;
76                  direction = update_direction(rail, direction);
77                  rail += direction;
78              }
79
80
81              int diff = 2*(k-1), i = 0;
82              for(int rail=0; rail<k; rail++) {
83                  for(int j = rail; j<n;) {
84                      rails[rail][j] = cipher_text[i];
85                      j+= diff; i+= (diff != 0);
86                      if(2*rail-1>0) {
87                          if(j>=n) continue;
88                          rails[rail][j] = cipher_text[i];
89                          j+= 2*rail;i++;
90                      }
91                  }
92                  diff = (diff-2<0 ? 0 : diff-2);
93              }
94
95              return recover_rails_text(false);
96          }
97  };
```

Nesse projeto, para as etapas de encriptação e decriptação, utilizamos uma chave $k = 3$.

3.1 Análise de Complexidade

Para encriptar, fazemos uma iteração do tamanho do texto, o que tem complexidade *O(n)*, e para cada iteração, inserimos a i-ésima letra na i-ésima coluna do da matriz e na linha correspondente, e autalizamos a próxima linha, em complexidade *O(1)*. Com isso, vemos que a complexidade da encriptação tem complexidade *O(n)*.

Para decriptar, primeiramente, calculamos quantas vezes vamos passar em cada linha da matriz montá-la, em *O(n)*. Posteriormente, para cada linha, realizamos um cálculo para passar apenas nos caracteres adequados para inserir naquela linha, fazendo que essa operação também tenha custo *O(n)*. No final, o processo de decriptografar também tem complexidade *O(n)*.

3.2 Quebra por força bruta

Para a cifra de transposição escolhida, partindo de um texto cifrado de tamanho n, temos que a chave pode variar de 2 a n, o seja podemos ter de 2 a n para realizar a criptografia.

Com isso, temos que passar por todas as chaves e aplicar a função de decriptar utilizando k no texto cifrado para obter um novo texto cifrado. Com isso, realizariamos n vezes uma operação de decriptar, que já também já discutimos ser uma operação de complexidade *O(n)*, o que resultaria em uma complexidade de $O(n^2)$. A implementação da quebra por força bruta pode ser encontrada a seguir.

```
vector<string> brute_force(string cipher_text) {
    vector<string> res;
    int n = cipher_text.size();
    for(int k=2; k<=n; k++) {

        rails_fence = RailFenceCipher(k);
        res.push_back(
            rails_fence.decrypt(cipher_text)
        );
    }
    return res;
}
```

3.3 Quebra por distribuição de frequência

Para trabalharmos com distribuição de frequência, inicialmente verificamos a frequência das digramas no texto cifrado, e então analisamos isso comparado à frequencia de digramas esperada no nosso idioma. Para essa cifra, foi escolhido trabalhar com os digramas do idioma, pois eles traziam um resultado mais satisfatório que trabalhando com as letras apenas.

Com isso, também foi necessário passar por todas as chaves possíveis para uma string de tamanho n, mas a distribuição de frequência foi util para obter a saída que mais provavelmente corresponde ao texto original após realizar o cálculo da pontuação. Com isso, a quebra por distribuição de frequência também tem complexidade $O(n^2)$.

```
string frequency_distribution(string cipher_text) {
    double best_score = utils.INF;
    int best_k = -1;
    string plain_text;

    int n = cipher_text.size();

    for(int k=2; k<=n; k++) {
        rails_fence = RailFenceCipher(k);
        string current_plain_text = rails_fence.decrypt(cipher_text);
        double current_score = calculate_score(current_plain_text);

        if(current_score < best_score) {
            best_score = current_score;
            plain_text = current_plain_text;
            best_k = k;
        }
    }
    return plain_text;
}
```

Para realizar o cálculo da pontuação utilizamos a seguinte fórmula:
FE = Frequência esperada de um digrama no idioma (percentual)
FP = Frequência percebida de um digrama no texto (percentual)

B = Conjunto com os 676 digramas no alfabeto

$$score = \sum_{bi \in B} |FE[bi] - FP[bi]|$$

E consideramos um score melhor quanto menor o seu valor. A seguir está a implementação dessa função de cálculo de score:

```
        string frequency_distribution(string cipher_text) {
            double best_score = utils.INF;
            int best_k = -1;
            string plain_text;

            int n = cipher_text.size();

            for(int k=2; k<=n; k++) {
                rails_fence = RailFenceCipher(k);
                string current_plain_text = rails_fence.decrypt(cipher_text);
                double current_score = calculate_score(current_plain_text);

                if(current_score < best_score) {
                    best_score = current_score;
                    plain_text = current_plain_text;
                    best_k = k;
                }
            }
            return plain_text;
        }
```

3.4 Conclusões

A cifra por transposição se apresenta como um estratégia ainda simples se aplicada isoladamente, mas que tende a ser mais segura que um algoritmo de substituição. Isso, principalmente, porque uma tentativa de quebra, tanto por força bruta, quanto por distribuição de frequência, tem complexidade computacional maior que a de cifra por substituição.

Ademais, vale também para a cifra por transposição que em textos grandes, geralmente compensa mais aplicar a análise por distribuição de frequência, pois da mesma forma é probabilistico. Enquanto para textos menores geralmente vale mais a pena utilizar a quebra por força bruta.

Referências

[May12] Mark Mayzner. English letter frequency counts: Mayzner revisited or etaoin srhldcu. 2012.