Cifras de Beale

De acordo com a lenda, no início do século XIX, um homem chamado Thomas J. Beale enterrou um tesouro no valor de milhões de dólares em algum lugar da Virgínia. Beale deixou três textos cifrados com um dono de hotel, Robert Morriss, antes de desaparecer, e instruiu Morriss a abrir o pacote contendo as cifras apenas se ele não retornasse dentro de 10 anos. O primeiro texto cifrado descreve o conteúdo do tesouro, enquanto os outros dois descrevem a localização exata do local de enterro. Apesar de muitas tentativas de decodificar as cifras, seu significado permanece um mistério até hoje. A Figura 1 abaixo mostra um dos textos cifrados.

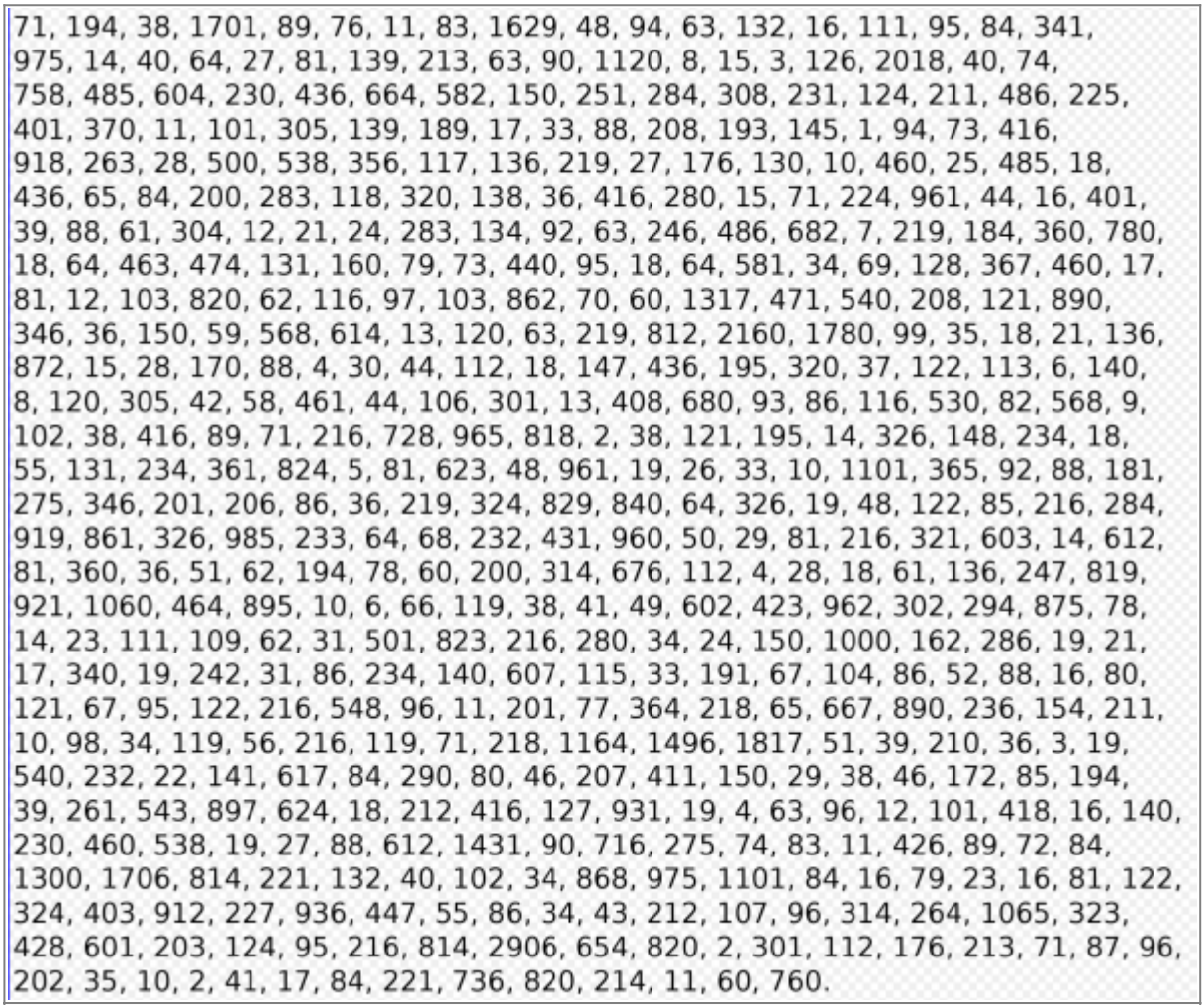


Figura 1: Texto cifrado de Beale

Acredita-se que os textos cifrados foram criados usando um **livro cifra**, que é um tipo de criptografia que usa um livro ou texto pré-acordado como chave. Em um livro cifra, a mensagem em texto simples é primeiro convertida em números, e então cada número é usado para referenciar uma palavra ou frase específica no livro. A sequência resultante de palavras ou frases se torna o texto cifrado, como o exemplo da Figura 1. (Para mais detalhes, https://en.wikipedia.org/wiki/Beale_ciphers)

Gerando as cifras

Beale usou uma variante de um livro cifra. Ele escolheu um texto longo como **texto cifra**, numerou cada uma das palavras do texto sequencialmente, começando em 0 (zero), e formou uma nova mensagem em que cada caracter desta mensagem é a primeira letra de alguma palavra do texto cifra. A mensagem codificada final consiste em uma lista dos números de sequência das palavras escolhidas.

Considere por exemplo o seguinte texto como **livro cifra**:

```
"Em 1892 o intelectual paranaense José Francisco da Rocha Pombo colocaria, no Largo
Ouvidor Pardinho, a pedra fundamental da Universidade do Paraná. O projeto foi
frustrado pelo Movimento Federalista que impediu a
criação da universidade.Vinte anos depois, em 1912, o estado contava com um
reduzido número de intelectuais,
apenas nove médicos e quatro engenheiros, mas se desenvolvia muito devido a
produção da erva-mate. Além
disso, a Guerra do Contestado fez com que as vastas lideranças políticas se
empenhassem pela criação de
uma universidade, de modo a dar uma identidade ao povo paranaense."
```

Usando a ideia de Beale, (considerando que apenas **espaço** e **linefeed** (mudança de linha) são usados para separar palavras) teríamos **arquivo de chaves** abaixo, em que cada linha contém 2 campos separados por **':'** . O segundo campo contém uma lista da posição de palavras cuja primeiro caracter é o caracter indicado no primeiro campo.

```
1: 38 1
a: 89 85 72 65 63 59 48 35 31 15
c: 79 70 68 42 41 32 10
d: 86 83 80 67 64 61 58 56 46 36 33 20 18 7
e: 77 62 53 51 40 37 0
f: 69 28 25 24 17 6
g: 66
i: 88 47 30 3
j: 5
l: 74 12
m: 84 57 54 50 27
n: 49 45 11
o: 39 22 13 2
p: 91 90 78 75 60 26 23 21 16 14 9 4
q: 71 52 29
r: 44 8
s: 76 55
u: 87 82 81 43 34 19
v: 73
```

Usando os códigos acima, a frase **"casa de papel"** poderia ser codificada da seguinte maneira:

```
42 15 76 85 -1 46 51 -1 91 48 75 77 12
```

Ou ainda:

```
79 85 55 72 -1 64 62 -1 90 89 90 0 12
```

Note que no exemplo acima, algumas letras são representadas por vários códigos. Quanto maior o livro cifra, mais cchaves serão atribuídos para a mesma letra, aumentando assim o número de representações possíveis do texto cifrado. Ainda no exemplo acima, vale mencionar que o espaço entre as palavras foi representado pelo código -1.

Implementação do Trabalho

Escreva um programa em C que codifique e decodifique uma mensagem usando a cifra de Beale. O programa deverá ter as seguintes funcionalidades:

- Codificar uma mensagem qualquer contida em um arquivo ASCII usando um **livro cifra**. O programa deve ter uma opção de salvar em um arquivo texto as chaves geradas no formato descrito anteriormente. A linha de execução do programa dever ser a seguinte:

```
./beale  -e  -b LivroCifra -m MensagemOriginal -o MensagemCodificada -c
ArquivoDeChaves
```

- Decodificar uma mensagem, usando um arquivo de códigos

```
./beale  -d  -i MensagemCodificada  -c ArquivoDeChaves  -o MensagemDecodificada
```

- Decodificar uma mensagem usando o livro cifra

```
./beale -d -i MensagemCodificada -b LivroCifra -o MensagemDecodificada
```

- Um exemplo de livro cifra pode ser encontrado aqui

Requisitos

Tendo em vista que um caractere pode ter um número variável de chaves (dependendo do tamanho do livro cifra), você deve armazenar as chaves numa lista, a qual deve ser alocada dinamicamente. Para o mesmo livro cifra e mensagem, o programa deve fornecer mensagens codificadas a cada execução.

Estrutura do Código Fonte

O projeto deve ter, além do arquivo `beale.c` (que contém o código da função main), pelo menos três arquivos `.c` com as funções para gerar o arquivo de chaves, codificação e decodificação de uma mensagem. As estruturas de dados necessárias devem estar definidas em um arquivo `.h`

Produto a ser entregue

Deve ser entregue ao professor um arquivo *.tar* ou *.zip* contendo pelo menos:

- Arquivos `.c` e `.h`
- Arquivo `Makefile`. Este arquivo para o projeto deve ter pelo menos:
  - Os alvos `all` (default), `clean` e `purge`.
  - CFLAGS = `-std=c99 -Wall`
  - ATENÇÃO: Deve ser OBRIGATORIAMENTE usada a opção de compilação `-std=c99`
  - Compilar e ligar separadamente (gerar arquivos `.o` intermediários)
- Arquivo `LEIAME` contendo nome e GRR do aluno, texto explicando resumidamente os módulos criados, as estruturas de dados e os algoritmos usados.
- Estes arquivos devem estar em um diretório de nome **<login>**, onde **<login>** é o login do usuário nos sistemas linux do DINF.

- O nome do arquivo a ser entregue deve ser **<login>.tar** ou **<login>.zip**
- Os trabalhos devem ser entregues através do Moodle C3SL:
    - Turma BCC1 (Prof. Luiz Oliveira)
    - Turma BCC2 (Prof. Armando)
    - Turma BCC3 (Prof. Vinícius)

Avaliação

Os itens de avaliação do trabalho e respectivas pontuações são:

- Modularização e organização do código-fonte (15 pontos)
- Funcionamento: corretude das respostas nos testes executados (40 pontos)
- Eficiência: algoritmos e estruturas de dados utilizados para obter um melhor desempenho e uso eficiente de alocação dinâmica de memória (45 pontos)

ATENÇÃO: programas que tiverem erros de compilação ou terminarem a execução de forma abrupta sem que tenha havido processamento adequado receberão nota **ZERO**

From:
https://wiki.inf.ufpr.br/maziero/ - **Prof. Carlos Maziero**

Permanent link:
https://wiki.inf.ufpr.br/maziero/doku.php?id=prog2:cifras_de_baele

Last update: **2023/04/05 14:19**