深蓝学院
shenlanxueyuan.com

作业三：文件加密解密系统

主讲人 梁爽

纲要

- 第一部分：生成码本文件
- 第二部分：生成二进制文件
- 第三部分：加密二进制文件
- 第四部分：解密二进制文件
- 第五部分：测试正确性

生成码本文件

- 顺序生成[0,255]，然后随机打乱顺序，得到码本文件。
- 参考实现：左边为生成码本文件的代码，中间为生成的码本文件内容，右图为文件目录。

```cpp
#include <bits/stdc++.h>

std::vector<int> code;

int main () {
    // 生成随机码本
    for (int i = 0; i < 256; ++i) {
        code.push_back(i);
    }
    std::srand(unsigned(time(0)));
    std::random_shuffle(code.begin(), code.end());

    // 存储随机码本
    std::ofstream file("code_book.txt", std::ios::out);
    for (int i = 0; i < 256; ++i) {
        std::cout << code[i] << " ";
        file << code[i] << " ";
    }
    file << "\n";
    return 0;
}
```

build_codebook.cpp

```
36 235 122 7 38 218 201 135 161 5 202 170 35 167 176 230 137 46 37 132 56 136 103 88 145 8 127 12
 2 238 98 124 74 159 191 16 66 57 216 233 139 23 121 24 200 110 173 9 114 27 252 225 185 11 236 2
47 248 3 177 143 243 221 168 67 193 28 113 99 197 190 77 244 151 212 59 215 160 61 112 144 85 174
 203 44 227 4 14 78 106 76 183 163 29 162 80 199 234 125 154 72 239 242 198 83 17 0 25 223 229 17
5 180 49 54 63 47 245 195 118 93 211 115 140 208 10 1 21 206 187 102 31 48 194 237 117 126 133 21
9 130 204 250 128 30 70 40 13 43 58 255 60 64 20 65 192 109 22 131 231 222 157 189 240 62 246 50
179 51 254 107 87 32 52 95 158 186 91 141 15 196 73 150 101 155 81 171 92 18 89 34 94 79 172 232
53 33 184 181 209 166 19 90 228 153 45 120 210 207 26 41 224 108 116 104 149 39 217 169 111 69 18
8 226 147 182 119 68 142 156 100 148 42 164 178 220 152 105 249 97 96 214 82 129 86 134 251 146 1
23 253 138 84 165 6 241 71 205 213 55 75
```

码本文件

纲要

- 第一部分：生成码本文件
- **第二部分：生成二进制文件**
- 第三部分：加密二进制文件
- 第四部分：解密二进制文件
- 第五部分：测试正确性

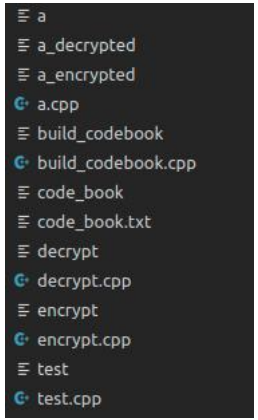
生成二进制文件

- 写一个C++程序a.cpp并编译，得到对应的二进制文件a。
- 参考实现：左图为a.cpp；生成二进制文件对应右图中的文件a。

```cpp
#include <bits/stdc++.h>

int main() {
    for (int i = 1; i <= 100; ++i) {
        printf("%d ", i);
    }
    printf("\n");
    return 0;
}
```

a.cpp



文件目录

纲要

- 第一部分：生成码本文件
- 第二部分：生成二进制文件
- **第三部分：加密二进制文件**
- 第四部分：解密二进制文件
- 第五部分：测试正确性

加密二进制文件

- 读入码本文件、待加密的文件、加密后文件名；输出加密后文件。
- 重点1：用合适的数据结构存储码本。
- 重点2：int/unsigned char/char转换。
- 参考实现：左图为参考代码，右图为代码输入

```cpp
#include <bits/stdc++.h>

std::string codebook, infile, outfile;

int main() {
  std::cin >> codebook >> infile >> outfile;

  // 读取输入文件：需要加密的文件
  std::ifstream in(infile, std::ios::in|std::ios::binary);
  if (!in) {
    std::cout << "The input file does not exist!" << std::endl;
    return 0;
  }

  // 读取码本文件
  std::ifstream code(codebook, std::ios::in);
  if (!code) {
    std::cout << "The codebook file does not exist!" << std::endl;
    return 0;
  }

  // 预处理码本文件
  std::vector<int> code_book;
  while (!code.eof()) {
    std::string s;
    std::getline(code, s);
    std::stringstream ss;
    ss << s;
    int num;
    while(ss >> num) {
      code_book.push_back(num);
    }
  }

  // 构建输出文件：加密后的文件
  std::ofstream out(outfile, std::ios::out|std::ios::binary);

  // 从输入文件计算得到输出文件
  char c;
  while (in.read((char*)&c, sizeof(c))) {
    unsigned char uc = c; // [-128, 127] -> [0, 255]
    int num = (int)uc;
    assert(num >= 0 && num < 256);
    int de_num = code_book[num];
    assert(de_num >= 0 && de_num < 256);
    out << char(de_num);
  }

  return 0;
}
```

encrypt.cpp

```
code_book.txt a a_encrypted
```

代码输入

纲要

- 第一部分：生成码本文件
- 第二部分：生成二进制文件
- 第三部分：加密二进制文件
- **第四部分：解密二进制文件**
- 第五部分：测试正确性

解密二进制文件

- 读入码本文件、已加密的文件、解密后文件名；输出解密后文件。
- 重点：用合适的数据结构存储逆码本。
- 参考实现：如图所示。

```cpp
#include <bits/stdc++.h>

std::string codebook, infile, outfile;

int main() {
  std::cin >> codebook >> infile >> outfile;

  // 读取输入文件：需要解密的文件
  std::ifstream in(infile, std::ios::in|std::ios::binary);
  if (!in) {
    std::cout << "The input file does not exist!" << std::endl;
    return 0;
  }

  // 读取码本文件
  std::ifstream code(codebook, std::ios::in);
  if (!code) {
    std::cout << "The codebook file does not exist!" << std::endl;
    return 0;
  }

  // 预处理码本文件
  std::vector<int> inv_code_book(256, 0);
  int cnt = 0;
  while (!code.eof()) {
    std::string s;
    std::getline(code, s);
    std::stringstream ss;
    ss << s;
    int num;
    while(ss >> num) {
      inv_code_book[num] = cnt++;
    }
  }

  // 构建输出文件：解密后的文件
  std::ofstream out(outfile, std::ios::out|std::ios::binary);

  // 从输入文件计算得到输出文件
  char c;
  while (in.read((char*)&c, sizeof(c))) {
    unsigned char uc = c; // [-128, 127] -> [0, 255]
    int num = (int)uc;
    assert(num >= 0 && num < 256);
    int en_num = inv_code_book[num];
    assert(en_num >= 0 && en_num < 256);
    out << char(en_num);
  }

  return 0;
}
```

decrypt.cpp

```
code_book.txt a a_encrypted
```

代码输入

纲要

- 第一部分：生成码本文件
- 第二部分：生成二进制文件
- 第三部分：加密二进制文件
- 第四部分：解密二进制文件
- **第五部分：测试正确性**

测试正确性

深蓝学院 shenlanxueyuan.com

- 读入原始二进制文件和加密又解密的文件，判断两个文件是否相同。
- 参考实现：如图所示。

```cpp
#include <bits/stdc++.h>

std::string file, decrypted_file;

int main() {

  std::cin >> file >> decrypted_file;

  // 读取原文件
  std::ifstream f(file, std::ios::in|std::ios::binary);
  if (!f) {
    std::cout << "The input file does not exist!" << std::endl;
    return 0;
  }

  // 读取加密再解密后的文件
  std::ifstream df(decrypted_file, std::ios::in|std::ios::binary);
  if (!df) {
    std::cout << "The input file does not exist!" << std::endl;
    return 0;
  }

  char c, dc;
  int cnt = 0;
  while (f.read((char*)&c, sizeof(c)) && df.read((char*)&dc, sizeof(dc))) {
    if (c != dc) {
      std::cout << "Inorrect answer!" << std::endl;
      std::cout << "The " << cnt << "th character in original file is " << c << std::endl;
      std::cout << "The " << cnt << "th character in decrypted file is " << dc << std::endl;
      return 0;
    }
    ++cnt;
  }

  std::cout << "Correct answer!" << std::endl;
  return 0;
}
```

```
a a_decrypted
Correct answer!
```

test.cpp

代码输入输出

在线问答

深蓝学院
shenlanxueyuan.com

Q&A

深蓝学院
shenlanxueyuan.com

感谢各位聆听！

Thanks for Listening