

Program 3: Stream Cipher RC4

CPSC370: Introduction to Computer Cryptology

Due Monday, October 17, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement the RC4 algorithm (size of vector $S = 256$).

1 Details of the program

1. Implement the RC4 algorithm in the following steps:
 - (a) Initialize the S vector and T vector for a given seed (or initial key);
 - (b) Permute the S vector;
 - (c) Generate key streams;
 - (d) Encrypt each byte stream of the plain text using the corresponding key byte (Hint: For byte XOR, see <http://www.cplusplus.com/forum/articles/38516/>);
 - (e) Decrypt each byte stream of the cipher text using the corresponding key byte;

When XORing two same bytes, you will generate 0. Just produce the byte itself if two bytes are same.

2. Experiment the correctness of your program by using the following plain text and seed:
 - (a) plain text: cryptology seed: 1 2 3 6
 - (b) plain text: RC4 seed: 5 7 8 9

For each test of your RC4 algorithm, you need to output the following information

- (a) Plain text
 - (b) Seed
 - (c) The vector S after initial permutation
 - (d) Key streams used for the input plain text
 - (e) Encrypted message
 - (f) Decrypted message
3. Your output should look like the screenshot output as shown in Figure 1.

```

C:\Users\dche\Dropbox\Course\CPSC370\Spring2016\Programs\prog3\RC4_Solution\RC4_V...
=====
TEST CASE 1
=====
Plaintext: cryptology
Seed used: 1236
After initial permutation of S:
100 3 231 14 19 26 44 48 159 101 83 164 81 120 123 144 161 196
31 153 179 230 24 200 74 110 67 146 140 130 237 136 208 86 0 135
172 4 238 244 82 34 58 132 96 225 186 155 192 28 209 80 46 212
9 87 38 127 60 72 188 121 133 202 247 151 147 246 255 11 165 242
125 77 33 99 118 134 199 207 214 221 177 160 107 119 218 50 27 61
253 71 239 141 175 236 106 205 92 194 1 174 7 84 114 137 22 95
193 163 16 191 204 185 49 116 20 62 216 189 47 162 54 250 18 90
124 79 56 198 112 166 217 206 167 154 122 170 203 143 173 156 240 152
171 138 15 13 248 41 5 97 226 234 150 142 117 35 108 57 91 103
235 158 64 75 42 145 29 70 190 243 109 17 25 126 201 43 169 232
32 115 184 59 183 63 102 69 168 233 223 36 6 66 52 157 213 55
139 93 210 182 228 254 40 78 176 129 2 131 53 76 30 215 219 241
104 113 222 148 111 249 245 128 37 23 51 229 88 195 12 187 197 94
211 251 65 149 252 8 227 180 178 98 45 224 220 85 89 73 10 39
21 181 105 68
Keys generated for plaintext: 196 102 226 189 141 131 159 206 142 103
Message encrypted: 240=05104
Message decrypted: cryptology
=====
TEST CASE 2
=====
Plaintext: RC4
Seed used: 5789
After initial permutation of S:
91 40 23 132 215 287 65 81 17 110 216 237 165 173 248 219 240 247
208 172 87 149 145 236 185 217 76 107 79 100 138 174 190 155 89 30
214 71 239 212 108 202 99 135 160 104 27 66 184 21 106 1 26 161
143 221 251 90 82 224 3 57 10 200 133 246 19 121 63 195 88 169
86 73 117 201 220 9 196 24 8 127 25 95 142 77 20 12 103 115
189 176 34 37 134 53 58 22 33 101 78 126 232 137 197 84 41 250
150 254 0 205 222 153 62 139 170 255 2 171 226 11 249 218 199 154
122 213 141 18 159 151 130 233 113 59 5 253 55 163 210 4 158 157
203 243 111 83 93 242 188 168 180 15 223 241 198 191 72 38 112 105
125 120 182 75 175 85 231 172 14 166 116 192 238 167 124 181 209 140
245 229 162 48 119 64 94 36 179 178 211 102 28 7 187 118 29 206
49 109 194 229 96 97 44 42 47 51 123 146 19 114 43 92 98 252
50 45 70 31 56 52 39 152 227 46 244 131 61 32 183 67 54 144
225 164 156 148 128 235 230 60 129 234 16 35 186 6 69 147 80 74
204 68 136 193
Keys generated for plaintext: 93 152 80
Message encrypted: 240
Message decrypted: RC4
Press any key to continue . . .

```

Figure 1: A screenshot of outputs

2 Submission

1. **Electronic submission** (Due by Monday, October 17, 2016 11:59PM)
 - (a) Make sure that your program is compilable
 - (b) Zip both the source codes and output screenshots into a file. The file format is as follows: `FirstNameLastName_Program3.zip` (e.g., `DongshengChe_Program3.zip`)
 - (c) Upload the zip file onto D2L Dropbox
2. **Hardcopy submission** (Due by Tuesday, October 18, 2016 in class)

Your hardcopy should include:

- Grading sheet (top)
- Source code (middle)
- Output screenshots (bottom)