Help with the two-time pad

This web page has information about the two-time pad example.

To make things somewhat easier for you, we have created a worked example and a decryption program for the two-time pad. In this example, we are given two files, demo1.bin and demo2.bin. Both of these files were encrypted with the one-time pad demo.key.

We have provided a C++ program called one-time-pad-vrfy.cc. You may or may not find it useful in doing Problem 2-1 on the homework. This program can be compiled on a Unix computer with this command:

```
% g++ -o one-time-pad-vrfy one-time-pad-vrfy.cc
```

Once you have compiled it, you can run it on both examples:

demo1.bin

```
Output (128 bytes):
In some situations it is acceptable for the same identifier to be used
by different people; other applications require unique id


Output in hex:
49 6e 20 73 6f 6d 65 20 73 69 74 75 61 74 69 6f 6e 73 20 69
74 20 69 73 20 61 63 63 65 70 74 61 62 6c 65 20 66 6f 72 20
74 68 65 20 73 61 6d 65 20 69 64 65 6e 74 69 66 69 65 72 20
74 6f 20 62 65 20 75 73 65 64 20 62 79 20 64 69 66 66 65 72
65 6e 74 20 70 65 6f 70 6c 65 3b 20 6f 74 68 65 72 20 61 70
70 6c 69 63 61 74 69 6f 6e 73 20 72 65 71 75 69 72 65 20 75
6e 69 71 75 65 20 69 64


Many people find octal easier than hex.


Here is the output in octal:
111 156 040 163 157 155 145 040 163 151 164 165 141 164 151 157 156 163
040 151
164 040 151 163 040 141 143 143 145 160 164 141 142 154 145 040 146 157
162 040
164 150 145 040 163 141 155 145 040 151 144 145 156 164 151 146 151 145
162 040
164 157 040 142 145 040 165 163 145 144 040 142 171 040 144 151 146 146
145 162
145 156 164 040 160 145 157 160 154 145 073 040 157 164 150 145 162 040
141 160
160 154 151 143 141 164 151 157 156 163 040 162 145 161 165 151 162 145
040 165
```

156 151 161 165 145 040 151 144

Here is how the results were obtained:

```
Bytes 0 .. 9
file demo1.bin     176 124 325 316 253 273 254 275 065 116  ~T......5N
file demo.key      067 072 365 275 304 326 311 235 106 047  7:......F'
================== ========================================
file1 XOR file2    111 156 040 163 157 155 145 040 163 151  In some si


Bytes 10 .. 19
file demo1.bin     316 166 054 323 055 165 226 134 104 133  .v,.-u.\D[
file demo.key      272 003 115 247 104 032 370 057 144 062  ..M.D../d2
================== ========================================
file1 XOR file2    164 165 141 164 151 157 156 163 040 151  tuations i


Bytes 20 .. 29
file demo1.bin     136 035 107 377 323 320 152 012 121 220  ^.G...j.Q.
file demo.key      052 075 056 214 363 261 011 151 064 340  *=.....i4.
================== ========================================
file1 XOR file2    164 040 151 163 040 141 143 143 145 160  t is accep


Bytes 30 .. 39
file demo1.bin     316 136 043 344 211 062 101 306 143 350  .^#..2A.c.
file demo.key      272 077 101 210 354 022 047 251 021 310  .?A...'...
================== ========================================
file1 XOR file2    164 141 142 154 145 040 146 157 162 040  table for


Bytes 40 .. 49
file demo1.bin     345 140 301 231 072 306 147 320 165 203  .`..:.g.u.
file demo.key      221 010 244 271 111 247 012 265 125 352  ....I...U.
================== ========================================
file1 XOR file2    164 150 145 040 163 141 155 145 040 151  the same i


Bytes 50 .. 59
file demo1.bin     135 114 227 000 010 126 376 226 273 362  ]L...V....
file demo.key      071 051 371 164 141 060 227 363 311 322  9).ta0....
================== ========================================
file1 XOR file2    144 145 156 164 151 146 151 145 162 040  dentifier


Bytes 60 .. 69
file demo1.bin     135 271 134 106 003 246 210 353 307 033  ].\F......
file demo.key      051 326 174 044 146 206 375 230 242 177  ).|$f....□
================== ========================================
file1 XOR file2    164 157 040 142 145 040 165 163 145 144  to be used


Bytes 70 .. 79
file demo1.bin     275 317 264 201 357 217 344 145 173 247  .......e{.
file demo.key      235 255 315 241 213 346 202 003 036 325  ..........
================== ========================================
```

```
file1 XOR file2    040 142 171 040 144 151 146 146 145 162   by differ


Bytes 80 .. 89
file demo1.bin     365 206 307 356 251 320 201 131 330 235  .......Y..
file demo.key      220 350 263 316 331 265 356 051 264 370  .......)..
================== ========================================
file1 XOR file2    145 156 164 040 160 145 157 160 154 145  ent people


Bytes 90 .. 99
file demo1.bin     110 121 272 336 343 240 314 356 042 204  HQ......".
file demo.key      163 161 325 252 213 305 276 316 103 364  sq......C.
================== ========================================
file1 XOR file2    073 040 157 164 150 145 162 040 141 160  ; other ap


Bytes 100 .. 109
file demo1.bin     246 302 305 012 241 371 236 274 176 054  ........~,
file demo.key      326 256 254 151 300 215 367 323 020 137  ...i......_
================== ========================================
file1 XOR file2    160 154 151 143 141 164 151 157 156 163  plications


Bytes 110 .. 119
file demo1.bin     006 260 312 126 143 134 332 041 175 057  ...Vc\.!}/
file demo.key      046 302 257 047 026 065 250 104 135 132  &..'.5.D]Z
================== ========================================
file1 XOR file2    040 162 145 161 165 151 162 145 040 165   require u


Bytes 120 .. 129
file demo1.bin     172 264 005 251 221 257 256 244 000 000  z.........
file demo.key      024 335 164 334 364 217 307 300 000 000  ..t.......
================== ========================================
file1 XOR file2    156 151 161 165 145 040 151 144 000 000  nique id..
```

demo2.bin

```
Output (128 bytes):
Client-side SSL certificates have been commercially available in the
United States since VeriSign started selling them in 1996.


Output in hex:
43 6c 69 65 6e 74 2d 73 69 64 65 20 53 53 4c 20 63 65 72 74
69 66 69 63 61 74 65 73 20 68 61 76 65 20 62 65 65 6e 20 63
6f 6d 6d 65 72 63 69 61 6c 6c 79 20 61 76 61 69 6c 61 62 6c
65 20 69 6e 20 74 68 65 20 55 6e 69 74 65 64 20 53 74 61 74
65 73 20 73 69 6e 63 65 20 56 65 72 69 53 69 67 6e 20 73 74
61 72 74 65 64 20 73 65 6c 6c 69 6e 67 20 74 68 65 6d 20 69
6e 20 31 39 39 36 2e 20
```

Many people find octal easier than hex.

Here is the output in octal:

```
103 154 151 145 156 164 055 163 151 144 145 040 123 123 114 040 143 145
162 164
151 146 151 143 141 164 145 163 040 150 141 166 145 040 142 145 145 156
040 143
157 155 155 145 162 143 151 141 154 154 171 040 141 166 141 151 154 141
142 154
145 040 151 156 040 164 150 145 040 125 156 151 164 145 144 040 123 164
141 164
145 163 040 163 151 156 143 145 040 126 145 162 151 123 151 147 156 040
163 164
141 162 164 145 144 040 163 145 154 154 151 156 147 040 164 150 145 155
040 151
156 040 061 071 071 066 056 040
```

Here is how the results were obtained:

```
Bytes 0 .. 9
file demo2.bin     164 126 234 330 252 242 344 356 057 103  tV....../C
file demo.key      067 072 365 275 304 326 311 235 106 047  7:......F'
================== ========================================
file1 XOR file2    103 154 151 145 156 164 055 163 151 144  Client-sid


Bytes 10 .. 19
file demo2.bin     337 043 036 364 010 072 233 112 026 106  .#...:.J.F
file demo.key      272 003 115 247 104 032 370 057 144 062  ..M.D../d2
================== ========================================
file1 XOR file2    145 040 123 123 114 040 143 145 162 164  e SSL cert


Bytes 20 .. 29
file demo2.bin     103 133 107 357 222 305 154 032 024 210  C[G...l...
file demo.key      052 075 056 214 363 261 011 151 064 340  *=.....i4.
================== ========================================
file1 XOR file2    151 146 151 143 141 164 145 163 040 150  ificates h


Bytes 30 .. 39
file demo2.bin     333 111 044 250 216 167 102 307 061 253  .I$..wB.1.
file demo.key      272 077 101 210 354 022 047 251 021 310  .?A...'...
================== ========================================
file1 XOR file2    141 166 145 040 142 145 145 156 040 143  ave been c


Bytes 40 .. 49
file demo2.bin     376 145 311 334 073 304 143 324 071 206  .e..;.c.9.
file demo.key      221 010 244 271 111 247 012 265 125 352  ....I...U.
================== ========================================
file1 XOR file2    157 155 155 145 162 143 151 141 154 154  ommerciall
```

```
Bytes 50 .. 59
file demo2.bin     100 011 230 002 000 131 373 222 253 276  @....Y....
file demo.key      071 051 371 164 141 060 227 363 311 322  9).ta0....
================== ========================================
file1 XOR file2    171 040 141 166 141 151 154 141 142 154  y availabl


Bytes 60 .. 69
file demo2.bin     114 366 025 112 106 362 225 375 202 052  L..JF....*
file demo.key      051 326 174 044 146 206 375 230 242 177  ).|$f....□
================== ========================================
file1 XOR file2    145 040 151 156 040 164 150 145 040 125  e in the U


Bytes 70 .. 79
file demo2.bin     363 304 271 304 357 306 321 167 177 241  .......w□.
file demo.key      235 255 315 241 213 346 202 003 036 325  ..........
================== ========================================
file1 XOR file2    156 151 164 145 144 040 123 164 141 164  nited Stat


Bytes 80 .. 89
file demo2.bin     365 233 223 275 260 333 215 114 224 256  .......L..
file demo.key      220 350 263 316 331 265 356 051 264 370  .......)..
================== ========================================
file1 XOR file2    145 163 040 163 151 156 143 145 040 126  es since V


Bytes 90 .. 99
file demo2.bin     026 003 274 371 342 242 320 356 060 200  ........0.
file demo.key      163 161 325 252 213 305 276 316 103 364  sq......C.
================== ========================================
file1 XOR file2    145 162 151 123 151 147 156 040 163 164  eriSign st


Bytes 100 .. 109
file demo2.bin     267 334 330 014 244 255 204 266 174 063  ........|3
file demo.key      326 256 254 151 300 215 367 323 020 137  ...i....._
================== ========================================
file1 XOR file2    141 162 164 145 144 040 163 145 154 154  arted sell


Bytes 110 .. 119
file demo2.bin     117 254 310 007 142 135 315 051 175 063  O...b].)}3
file demo.key      046 302 257 047 026 065 250 104 135 132  &..'.5.D]Z
================== ========================================
file1 XOR file2    151 156 147 040 164 150 145 155 040 151  ing them i


Bytes 120 .. 129
file demo2.bin     172 375 105 345 315 271 351 340 000 000  z.E.......
file demo.key      024 335 164 334 364 217 307 300 000 000  ..t.......
================== ========================================
file1 XOR file2    156 040 061 071 071 066 056 040 000 000  n 1996. ..
```