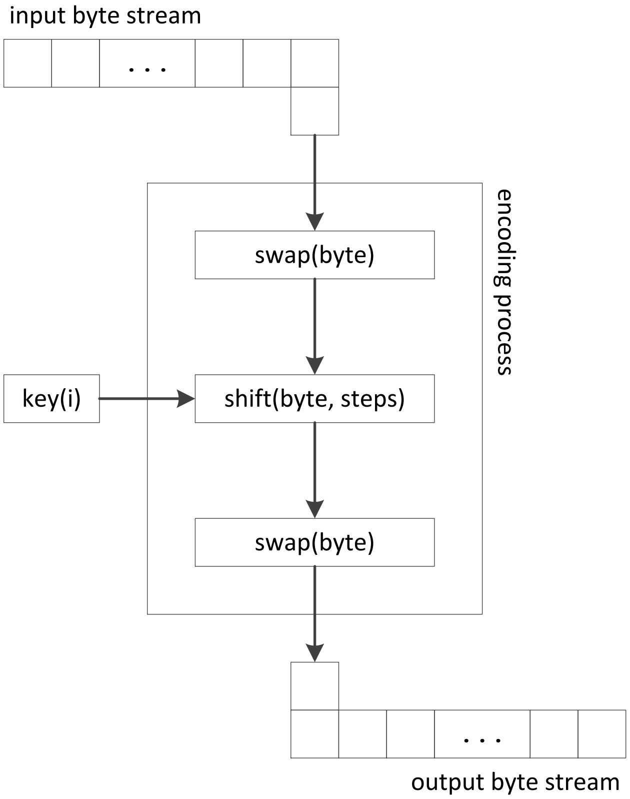
Cryptography (Shift Cipher)

The given file was encrypted using the encryption scheme below with a given key

1. Decrypt the given encrypted file and save the output to a file
2. The output file is supposed to be an image, follow the instructions on the image for the next step
3. Submit the secret key as an MD5 hash

Encryption scheme



Each byte of the input file is fed into an encoding process where

1. its high-order and low-order byte is swapped
2. it is then shifted by x steps (or the key(i) value)
3. its high-order and low-order byte is then swapped again

using a given key: {key(0), key(1), ..., key(n)}, key size: n where key(i) is [0, 255]

Example 1

assuming an input byte is 0x01, a key(i) is 3

1. swap(0x01) output 0x10
2. shift(0x10, 3) outputs 0x13
3. swap(0x13) outputs 0x31

Example 2

- **inputs**
  - byte array: {0x01, 0x02, 0x03, 0x04, 0x05}
  - key: {1, 6, 9}, key size: 3
- **encoding process**
  - encode(0x01, 1) outputs 0x11
  - encode(0x02, 6) outputs 0x62
  - encode(0x03, 9) outputs 0x93
  - encode(0x04, 1) outputs 0x14
  - encode(0x05, 6) outputs 0x65
- **output**
  - byte array: {0x11, 0x62, 0x93, 0x14, 0x65}

References

[1] Khan Academy - Shift Cipher
https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/shift-cipher

[2] Cornell University - Shift Ciphers (lecture)
http://www.math.cornell.edu/~mec/Summer2008/lundell/lecture1.html

[3] ASCII Table
http://www.asciitable.com/