3-Ciphers Report

计86 罗境佳 2018013469

代码文件位于 `src` 文件夹下。

AES-128-CBC

实现

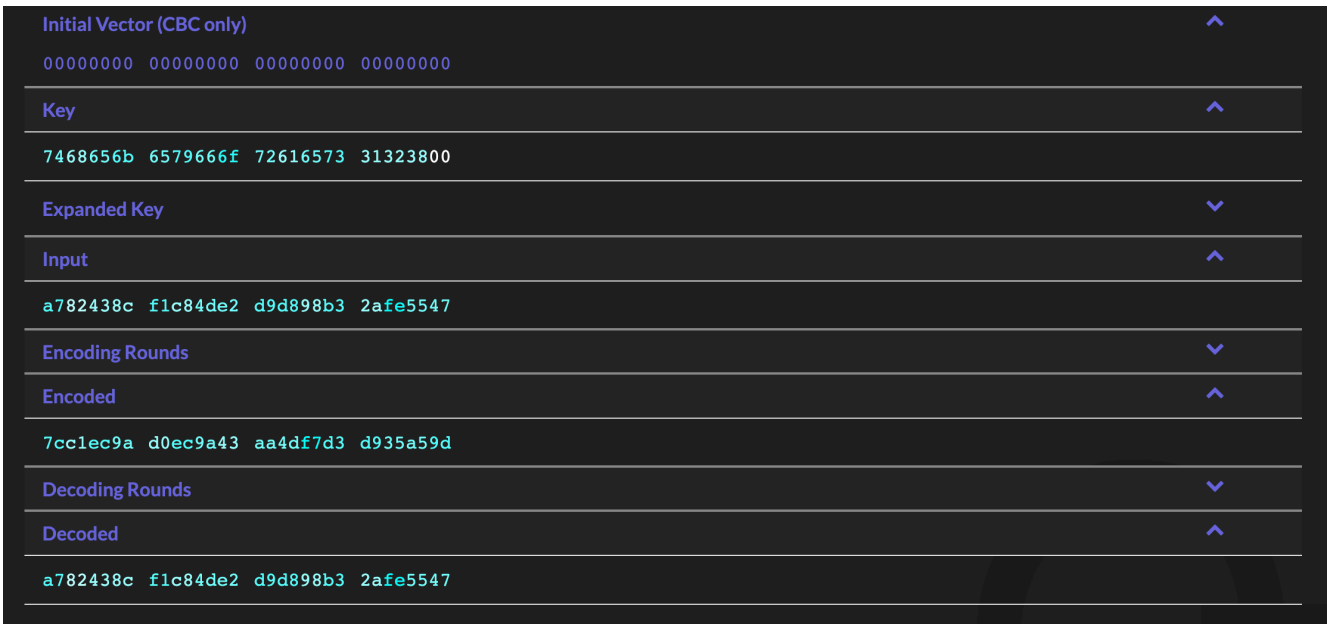
- 代码文件：`aes128.h` 、 `aes128.cpp`
- 使用一个 `__uint_128_t` 代表一个状态，按照课件和文献的说明实现了 `keyExpansion` 、 `subBytes` 、 `shiftRows` 、 `mixCols` 、 `addRoundKey` 等函数。
- S 盒、逆 S 盒以及 xtime 还有 Key Expansion 时的常数矩阵采用硬编码写死在代码中以节省时间。
- Key Expansion：采用文献中的方法实现，见 `aes128.h` 中的 `keyExpansion` 函数。
- Sub Bytes：利用 `s` 数组，将 state 的每个字节进行映射。
- Shift Rows：见 `shiftRows` 函数，state 按行存储，将其地址转换成 `u8*` 并进行轮换赋值。
- Mix Columns：矩阵乘法的实现见 `aes128.h` 的 `mixCols` 以及 `invMixCols` 函数，其中与 3、9、b、d、e 的乘法也基于 xtime 实现，见 `aes128.h` 中的一些宏定义。
- CBC：见 `main` 函数，具体做法是每个分组在 encode 之前与上一个分组的 encode 结果相异或，decode 后与上一个分组的 encode 结果相异或。

正确性

- 与 AES Step-by-Step 中的结果进行了对比，运行方式为 `make t-aes` 。
- 我的运行结果：

```
Luode-MacBook-Pro:src gloriallluo$ make t-aes
7468656b 6579666f 72616573 31323800
before round:
a782438c f1c84de2 d9d898b3 2afe5547
plain:
a782438c f1c84de2 d9d898b3 2afe5547
encode:
7cc1ec9a d0ec9a43 aa4df7d3 d935a59d
decode:
a782438c f1c84de2 d9d898b3 2afe5547
```

- AES Step-by-Step 的结果：



效率

- 运行方式为 `make aes`。
- 结果为 106.3896 Mbps。

RC4

实现

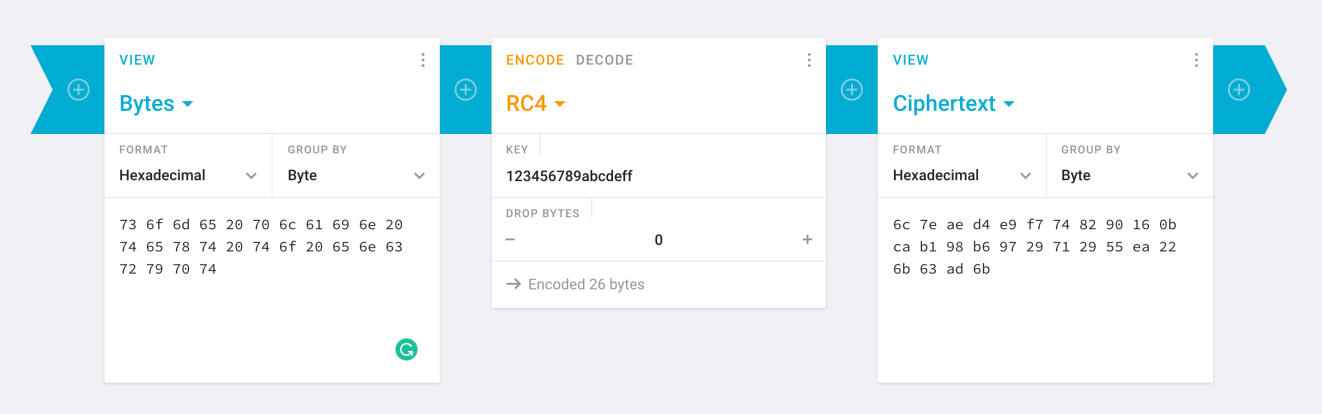
- 代码文件：`rc4.cpp`。
- KSA 过程：依据 key 对 S 盒进行充分交换，见 `KSA` 函数。
- PRGA 过程：生成与明文等长的密文，见 `PGRA` 函数。

正确性

- 与 Cryptii 中的结果进行了对比，运行方式为 `make t-rc4`。
- 我的运行结果：

```
Luode-MacBook-Pro:src gloriallluo$ make t-rc4
73 6f 6d 65 20 70 6c 61 69 6e 20 74 65 78 74 20 74 6f 20 65 6e 63 72 79 70 74
6c 7e ae d4 e9 f7 74 82 90 16 0b ca b1 98 b6 97 29 71 29 55 ea 22 6b 63 ad 6b
73 6f 6d 65 20 70 6c 61 69 6e 20 74 65 78 74 20 74 6f 20 65 6e 63 72 79 70 74
```

- Cryptii 中的结果：



效率

- 运行方式为 `make rc4`。
- 结果为 862.3158 Mbps。

SHA-3-256

实现

- 采用一个 5 * 5 的 u64 数组来存放状态。
- 轮函数：进行 24 轮循环，每轮循环将 state 分别经过 thet、rho_n_pi、chi、iota 等变换。见 `sha256.cpp` 中的 `keccak` 函数。
- sponge 函数：对原消息进行 padding 以及分组，之后经过 `keccak` 函数，最后取 256 位得到 `digest` 数组。

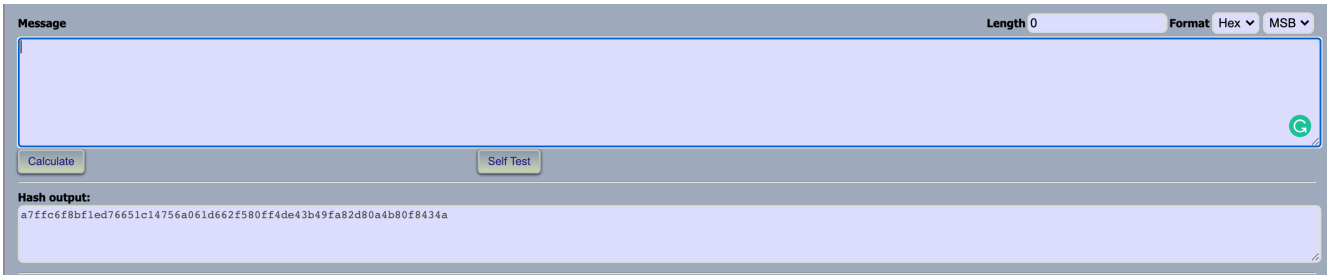
正确性

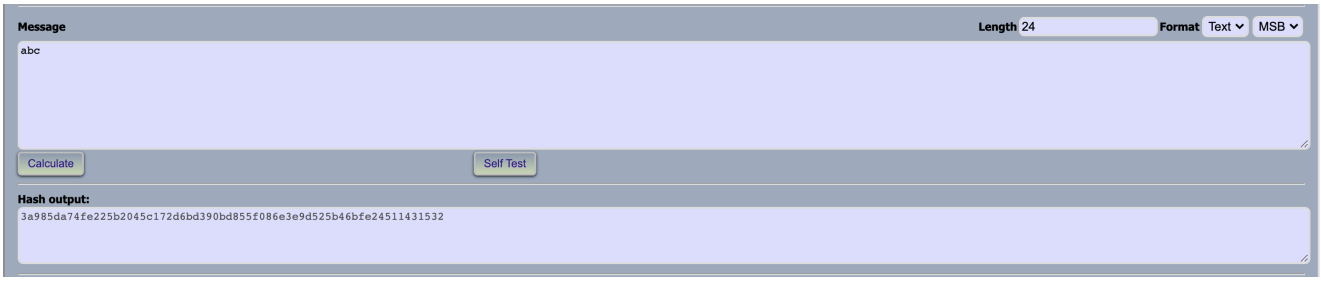
- 与 ONLINE SHA-3 Keccak CALCULATOR 中的结果对比，运行了几个测例，运行方式为 `make t-sha3`。
- 我的运行结果：

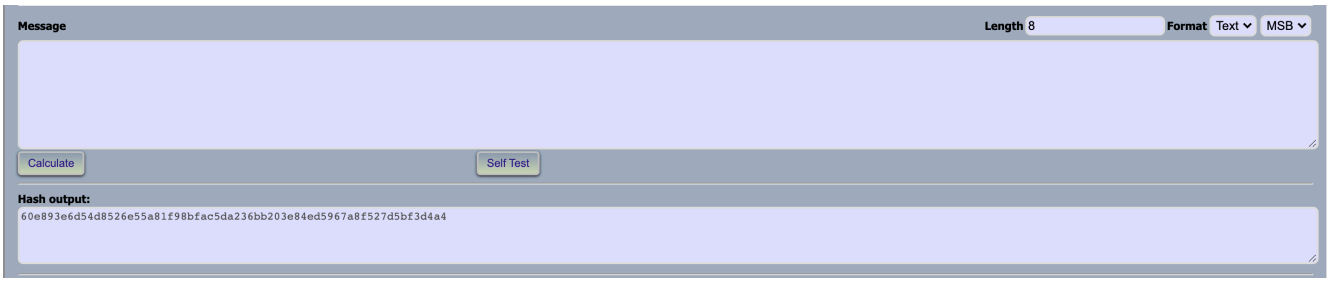
  分别为 ""、“abc“、" "、"hello world" 的哈希值

```
Luode-MacBook-Pro:src gloriallluo$ make t-sha3
a7ffc6f8 bf1ed766 51c14756 a061d662 f580ff4d e43b49fa 82d80a4b 80f8434a
3a985da7 4fe225b2 045c172d 6bd390bd 855f086e 3e9d525b 46bfe245 11431532
60e893e6 d54d8526 e55a81f9 8bfac5da 236bb203 e84ed596 7a8f527d 5bf3d4a4
644bcc7e 56437304 0999aac8 9e7622f3 ca71fba1 d972fd94 a31c3bfb f24e3938
```

- ONLINE SHA-3 的结果：







效率

- 运行方式为 `make sha3`。
- 结果为 186.3636 Mbps。

注：算法效率通过运行10次并取平均所得，采用了 -O1 优化。