Notes Cryptography

Brendon Mendicino

March 3, 2023

Contents

1 Introduction

Ho voglia di piangere

2 Openssl

Openssl has two versions 1.x and 3.x and 1.x will be dropped soon, but many applications still use it. The low level software implementations of the algorithm was a big mess, so a layer was created on top of it called *EVP Crypto API*, that just takes in the parameters and does a translation handling all the data.

Typical use of openssl:

1. include libraries
2. load facilities: load the functions required
3. create the context: select the tools, like a certain symmetric algorithm
4. initialize the context: assign IV, nonce, key...
5. operate on the context: provide the data on which the machine will work
6. finalize on the context: perform the concluding operations on the last output, like putting the padding, or the length of the digest
7. free the context: all the objects are *one time objects*, at the end of the operations the objects need to be freed;
8. free facilities

Usually the mode of use of the libraries is the incremental mode, which allow get small blocks a data encrypted.

To get an object the library is called which will return the function pointer to the implementation.

```
1 EVP_CHIPER *c = EVP_bf_cbc();
```