Notes Cryptography

Brendon Mendicino

March 4, 2023

Contents

1 Introduction

Ho voglia di piangere

Definition 1.1 – Modulo Operator

$$\begin{aligned} &a = b \pmod{n} : b = n \cdot q + a \\ &a, b, q, n \in \mathbb{Z} \end{aligned}$$

Definition 1.2 – Congurnce Modulo n

$$\begin{aligned} &a \equiv b \pmod{n} \\ &a \pmod{n} = b \pmod{n} \end{aligned}$$

Example 1.1

Show that $a \equiv b \pmod{n}$ if and only if n divides $a - b$.

Proof.

$$r = a \pmod{n} \implies a = aq + r, \quad q \in \mathbb{Z}$$

$$a \pmod{n} = b \pmod{n} = x$$

$$b = nq_1 + x, a = nq_2 + x$$

$$\frac{b-a}{n} = \frac{nq_1 + x - (nq_2 + x)}{n} = q_1 - q_2$$

$$\boxed{q_1, q_2 \in \mathbb{Z} \implies \frac{b-a}{n} \in \mathbb{Z}}$$

□

1.1 Symmetric Cryptography

A symmetric cyryptosystem Π consist of three algorithms:

- Decryption
- Encryption
- Generation

Definition 1.3 – IND-secure

A system Π can be defined **IND-secure** if, given two plaintext as inputs (P_0, P_1) to Π and by randomly choosing one of them, there is no better chance of 0.5 to determine whether the ciphertext was generated from P_0 or P_1.

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.

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

3 IND-experiment

...

Frequency analysis is a technique that allows to attach to a letter a frequency (different for each language), ...

4 cpa-ind goal

the cpa is one the possible attacks