**Objective**

The aim of this project is to develop a chaos-based cryptography library for Arduino that can be used in a system to encrypt the information protecting it while travelling through unsafe channels. The methods of data encryption and decryption rely on the distinct properties of chaotic systems. Chaos-based encryption is easier to compute and use simple algorithms, allowing a more efficient implementation.

**Background**

**Encryption**

Information needs to be secured from attacks and to protect it we use a technique called cryptography. In this project we have implemented the functions using symmetric key stream encipherment.

**Chaos**

Chaotic systems are non-linear systems with complex dynamics with distinctive properties:
- Random-like behaviour
- High sensitivity to initial conditions and parameters

*Why are they useful in cryptography?*

Those properties make them a great option as pseudo-random number generator, needed in stream encryption.

**Methodology**

The library has been developed in different layers, making its usage easier for developers; they can use the upper layer (encryption and decryption functions).

Developers can choose to itemize the library accessing to the lower levels, where there is a wide range of chaotic maps. Different maps will give different cipher texts.

**Results & Applications**

- Crypto library for Arduino
- Implemented functions:
  - Chaotic maps
  - Pseudo-random number generator
  - Encryption-decryption functions

This library is a good option for high weighted applications, in which memory and computational resources have to be taken in account, for example: IoT applications.