Practicalwork

Instructor : Amina SOUYAH

Abstract.

This work proposes a sample cryptosystem based on Hill Cipher. The Hill Cipher algorithm is a poly-graphic block cipher relies on linear algebra, and belongs to the classical symmetric means of cryptography. The main objective of this contribution is to give a smooth introduction to the science of data encipherment/ decipherment, by practising such mechanism to hide the meaning of both messages and files. Firstly, implement the classical hill cipher (i.e., encipherment is applied to two plain-letters at a time), the mechanism must be realized over Z/Z_{256} . Secondly, an extra-additional work is to implement how to break the security of hill cipher by applying known plaintext attacks, exactly as we have done with tuto-sessions.

Remark:

This work is optional but properly credited, it helps for enhancing and increasing your continuous evaluation mark.

Architecture of the proposed Block Cipher Algorithm.