

Using A clever operation
in order to
have
The longest possible encryption key
for
a given message

Damiens ROBERT

01-08-2020

1 Demonstration

Let the message M be a matrix whose elements are either 1, either 0.

Let the encrypted message \dot{M} be a matrix whose elements are either 1, either 0.

Let's find the relation R that project M onto \dot{M} and the relation \dot{R} that projects \dot{M} onto M .

Let's first notice that we have every possible answer for a given element in M and \dot{M} is a set of couples which are the element in M and the element in \dot{M} .

$$((0,0) , (0,1) , (1,0) , (1,1))$$

Let's notice that if the element in M and \dot{M} , are either identical or different.

The relation R must build the possible couples in order to be able to construct \dot{M} is the XOR operator. We then obtain the set of element in E where E is the encryption key :

$$(0 , 1 , 1 , 0)$$

Let's notice that the relation to obtain M from \dot{M} and E is also a XOR.