KASUMI

Project Cryptography

Trento, 7 December 2018

- Group **CANTOR**: Piasenti, Tizianel, Pellegrino.
- Group **DIRICHLET**: Pavone, Schicchi, Fidao.

Write a MAGMA code which implements the KASUMI cipher supporting keys of length 128 bit.
Your code has to contain two functions:

- Kasumi(P,K) for encrypting,
- KasumiDecryption(C,K) for decrypting,

with the following specifications:

```
NAME:   Kasumi(P,K)
INPUTS: P a string of bytes in hexadecimal notation of length 8
        K a string of bytes in hexadecimal notation of length 16
OUTPUT: C a string of bytes in hexadecimal notation of length 8

NAME:   KasumiDecryption(C,K)
INPUTS: C a string of bytes in hexadecimal notation of length 8
        K a string of bytes in hexadecimal notation of length 16
OUTPUT: P a string of bytes in hexadecimal notation of length 8
```

NOTE:
In the hexadecimal notation:

$$0x01 = 00000001$$
$$0x02 = 00000010$$
$$0x03 = 00000011$$
$$\vdots$$
$$0xA2 = 10100010.$$

Moreover:

$$0x0102 = 0000000100000010.$$

You will find the specifications for the Code attached, as well as a list of Test Vectors.
The implementation must be **completely written in MAGMA language**, without calling any external program.

The project will be tested and evaluated during the lecture on **21/12/2018**. If the program fails to work correctly, even on one test vector (or if it does not load, or if it is composed by more than one file), and this problem is not fixed before the end of the 21/12/2018 lecture, then all the team members will fail and they will have to attend again the whole lab session in Autumn 2019. During the lecture, the speed of your algorithm will be evaluated as well.

Participants of the team that presents the faster algorithm will receive one extra point that contribute to the final mark of the exam.