# Cryptography

## Programming 3

**Ex 1** Consider $S$-box $S5$ for $DES$ (`http://www.itl.nist.gov/fipspubs/fip46-2.htm`), for all $x \in \{0,1\}^6$ and $y \in \{0,1\}^4$ and random $z \in \{0,1\}^6$ compute the probability:

$$S_5(z) \oplus S_5(z \oplus x) = y.$$

**Ex 2** Write an application that takes as an input several ciphertext that are known to be a result of "many-time-pad" encryption i.e., $c_i = m_i \oplus G(k)$ and outputs $m_i$. How many messages you need to perform such a computation? As $G$ take for example $RC4$.