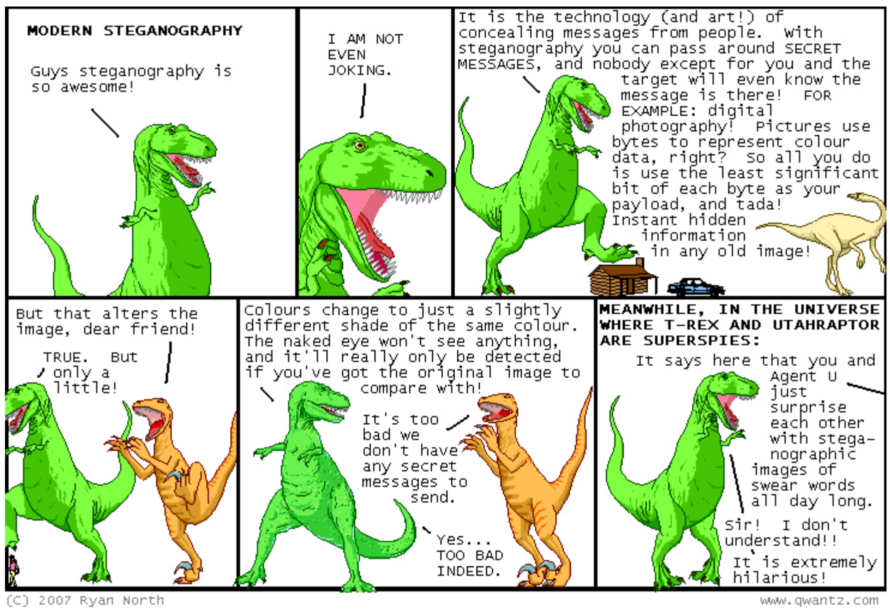
IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises XI.

1. Decrypt the following cryptotext.

2. Read carefully the following comics. The image can be downloaded here.



3. Consider the following generalized Dining Cryptographers protocol for n players $P_1, P_2, \ldots, P_n$ and messages of length n:

   Suppose that each pair of players (P_i, P_j) shares a set of keys $k_{i,j}(\omega)$ for $i, j, w \in \{1, 2, \ldots, n\}$, where $k_{i,j}(\omega) = k_{j,i}(\omega)$ and $k_{i,i}(\omega) = 0$. Each player P_i computes a vector of values:

$$W_i = \{W_i(1) = \oplus_{j=1}^{n} k_{i,j}(1), W_i(2) = \oplus_{j=1}^{n} k_{i,j}(2), \ldots, W_i(n) = \oplus_{j=1}^{n} k_{i,j}(n)\}.$$

   When broadcasting the messages, every player P_i chooses a random position c_i, applies XOR to her message m_i and $W_i(c_i)$ to obtain a new vector

$$V_i = \{W_i(1), W_i(2), \ldots, m_i \oplus W_i(c_i), \ldots, W_i(n)\}$$

   and makes this vector public.

   (a) Show that if every c_i is unique then the vector $V = \oplus_{i=1}^{n} V_i$ contains all the messages posted by all players.

   (b) What happens if two players choose the same position, *ie.* $c_j = c_i$ for two players P_i and P_j.

   (c) What happens when a dishonest player sets the vector V_i to a random vector.

4. Think hard, each exercise needs deliberation.