Homework 2

- Questions from Lecture unit 2
- Please refer to the lecture slides for more information about the context in which the questions arise.
- Due date: September 18, 2019

Questions

1. Suppose the same key k is used to encrypt three messages m_1, m_2 and m_3.

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$
$$c_3 = m_3 \oplus k$$

   How much information about m_1, m_2 and m_3 can be obtained from the ciphertexts c_1, c_2 and c_3? If Alice happens to know m_1, can she determine what m_2 and m_3 are?

2. What are the last two digits of 4^{100}?

3. For positive integers $a < 2^n$ let $\langle a \rangle$ denote the n-bit binary representation of a (e.g. $\langle 5 \rangle = 101$ as a 3-bit number). Let N be an n-bit positive integer. Consider the function $f : \{0,1\}^n \to \{0,1\}^{2n}$ where $f(\langle a \rangle) = \langle a^2 \mod N \rangle || \langle a^3 \mod N \rangle$. The function f is not a pseudo-random generator. Do you see why?

4. Consider a small modification of G that we discussed. Again. we form an n-bit number $N = pq$ where p and q are primes. On input a pair of n-bit strings x and y:

   (a) View x as an integer in binary representation. For example $x = 1001$ is identified with 9.

   (b) Set $G(x, y) = (x^2 \mod N, y, b)$ where b is the $\oplus$ of the last bit of x and y. Hence b is 0 if x and y are both even or both odd. Otherwise, $b = 1$.

   (c) For example, $x = (1101)$,$y = (1011)$, $N = 15$, $x = 13$, $y = 11$, $x^2 \mod 15 = 4$, $G(x, y) = (0100, 1011, 0)$

With this construction, G is not a pseudorandom generator. Do you see why?

5. Is matrix cipher vulnerable to chosen plaintext attack?