Institut for Matematik og Datalogi
Syddansk Universitet

September 20, 2019
JFB

Cryptology – 2019 – Assignment 1

Assignment due Friday, October 11, 12:00

Groups of up to three students are allowed (and encouraged) on this assignment. Note that this is part of your exam project, and it will count some towards the grade in the course, so you may not work with others not in your group. If it is late, it will not be accepted. Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

You may write your answers in either English or Danish. If you do it by hand, write very neatly and legibly.

1. Consider multiple round Vigenère encryption, both in the case where all periods are the same length and in the case where they might have different lengths. Multiple round encryption is encryption more than once, using a different key for each encryption. (The ciphertext from round i is the plaintext input to round $i+1$).

   (a) Is there any security advantage to multiple round encryption in the two cases? Explain your answer for the two cases separately.

   (b) How could such a system be cryptanalyzed?

2. Consider the group $\mathbb{Z}_{25}^*$?

   (a) What are the elements of the group?

   (b) What is the order of the group?

   (c) Find a generator g of the group.

   (d) Which other elements are generators? Explain how you know that the others are not, referring to the power g is raised to in order to get that element in your explanation.

(e) Find a subgroup of order 4. How many subgroups are there of this order? Why?

3. Suppose a cryptosystem has $P = \{a, b, c, d\}$, $C = \{1, 2, 3, 4\}$ and $K = \{k_1, k_2, k_3, k_4\}$. The encryption rules are as follows:

	a	b	c	d
k_1	1	2	3	4
k_2	4	3	2	1
k_3	3	4	2	1
k_4	2	4	1	3

Suppose the relevant probabilities are: $p(K = k_i) = 1/4$ for $1 \leq i \leq 4$, $p(P = a) = 1/4$, $p(P = b) = 1/4$, $p(P = c) = 1/6$, and $p(P = d) = 1/3$.

(a) Compute the probabilities $p(C = y)$ for all $y \in \{1, 2, 3, 4\}$.

(b) Does this cryptosystem achieve perfect secrecy? Explain your answer.

4. Consider the following family of pseudorandom function generators: $F_k(n) = n \oplus k$ (the operation $\oplus$ considers the binary representations of n and k, padded so they both have the length of the longer one, and does a bitwise XOR).

(a) Design an adversary (Eve) which efficiently (using q calls to the oracle, where $q \geq 2$ is not large) obtains the result $\mathrm{Adv}^{\mathrm{PRF}}_{\{F_k\}_K}(A; q) \geq 1 - (1/|C|)^{q-1}$.

(b) Explain why your adversary has the stated advantage.

(c) Suppose k and n are restricted to being between 0 and $2^\ell - 1$ for some positive integer ℓ. For which k is this function a permutation of the set $\mathbb{Z}_{2^\ell}$? Explain.

5. Find a linear feedback shift register of length 5, along with initial values for the register, which show that the the linear feedback shift register is eventually periodic, but not purely periodic. What is the period with your initial values? Make the period be at least 3.

6. Suppose that a keystream S is produced by a linear feedback shift register of length L (by a linear recurrence relation of degree L). Suppose the period is $2^L - 1$. Consider any positive integer i and the following pairs of positions in S:

$$(S_i, S_{i+1}), (S_{i+1}, S_{i+2}), ..., (S_{i+2^L-3}, S_{i+2^L-2})), (S_{i+2^L-2}, S_{i+2^L-1})).$$

How many of these pairs are such that $(S_j, S_{j+1}) = (0, 1)$? (In other words, how many times within one period does the pattern 01 appear?) Prove that your answer is correct.

7. Consider creating a stream cipher by using two LFSRs and using the bitwise AND (multiplication modulo 2) of the two key streams produced as the key stream for the cipher. Why is this a bad idea?

   (a) Specify an adversary for the PRF security game which shows why this is a bad idea.

   (b) Compute the advantage the adversary has for the PRF security game?