Institut for Matematik og Datalogi
Syddansk Universitet

September 21, 2016
JFB

Cryptology – F16 – Assignment 1

Assignment due Monday, October 3, 12:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in January, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become an assignment you redo). You may work in groups of two (or three). Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

1. We noted that for all groups $\mathbb{Z}_n^*$, where $n \geq 3$, the set of quadratic residues modulo n (those elements of $\mathbb{Z}_n^*$ which are squares modulo n) is a proper subgroup of $\mathbb{Z}_n^*$. Define the set of cubic residues modulo $n \geq 3$ to be:

$$C_n = \{x \in \mathbb{Z}_n^* \mid \exists y \in \mathbb{Z}_n^* \text{ s.t. } x \equiv y^3 \pmod{n}\}$$

   (a) Show that, for every $n \geq 3$, C_n is a subgroup of $\mathbb{Z}_n^*$.

   (b) Find an $n \geq 3$ where C_n is a proper subgroup of $\mathbb{Z}_n^*$. Show that it is.

   (c) Find an $n \geq 3$ where C_n is a not proper subgroup of $\mathbb{Z}_n^*$. Show that it is not.

2. 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	1	2
k_4	2	4	1	3

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

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.

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

   Suppose k and n are restricted to being between 0 and $\ell - 1$. For which k is this function a permutation of the set $\mathbb{Z}_\ell$?

4. 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 ultimately periodic, but not purely period. What is the period with your initial values?

5. Give an example of where the linear complexity of two bit strings, s and t, both of length $n > 5$ are such that their linear complexities are not additive, meaning $L(s \oplus t) < L(s) + L(t)$.

6. Suppose you had two examples of ciphertext, both enciphered using Vigenère ciphers. How would you make an intelligent guess as to whether or not the same sequence of substitution alphabets was used, without directly attempting to decipher? Is the assumption that the key stream is periodic (as in the Vigenère cipher) necessary?