Mid-term test in Cryptology I

September 30th, 2010

1. Find $H(\mathbf{K}|\mathbf{C}) - H(\mathbf{P}|\mathbf{C})$ for the shift cipher.

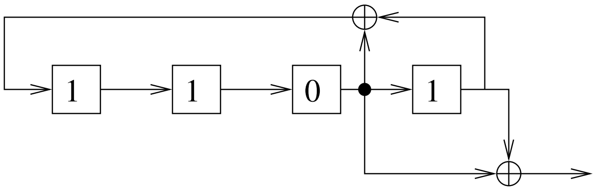
2. Consider an encryption scheme that has been obtained from the substitution cipher in the cipher block chaining mode. I.e. given an encryption function σ (a permutation of $\mathbb{Z}_{26}$), the encryption of some string $x_1 \cdots x_n \in \mathbb{Z}_{26}^n$ is the string $c_0 \cdots c_n$, where $c_0 \in \mathbb{Z}_{26}$ has been randomly generated and $c_i = \sigma(x_i + c_{i-1} \bmod 26)$.

   The following is a ciphertext produced by this encryption scheme:

   ```
   0      5      10     15     20     25     30     35
   irrqb  ayxca  hcaoz  gsnkn  gemvy  ntosx  hjhjg  xvxow
   ```

   It is known that $x_{13} = \texttt{a}$. What is x_{27}?

3. Consider the following keystream generating device made up of an LFSR, an extra output, and a combining XOR-operation. What is the linear complexity of the generated keystream, if the registers are initialized as shown?

4. Let the public key for the Merkle-Hellman singly iterated knapsack cryptosystem be

   $$(15, 1826, 458, 56, 111, 228, 3, 915, 6, 28, 2, 3658) \ .$$

   Decrypt the ciphertext 4326.

The test makes up a quarter of the final grade.
All exercises in the test have equal weight.
The solutions may be given in English or Estonian.