Mid-term test in Cryptology I

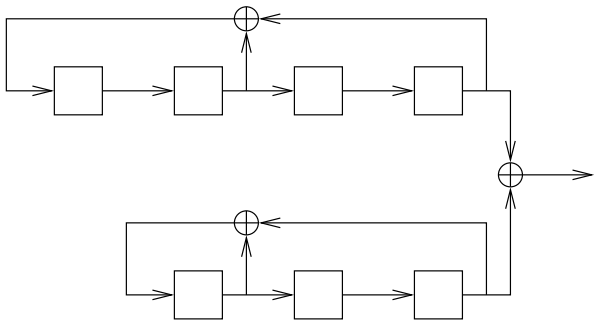
September 29th, 2009

1. Break the following ciphertext created from an English plaintext using the affine cipher:

   ```
   Wd iphkpu, X'qq fhbp h tijrg je ixf gihg qpgr fp!
   ```

2. Show that if a cryptosystem is unconditionally secure, then $H(\mathbf{K}|\mathbf{P},\mathbf{C}) = H(\mathbf{K}|\mathbf{C})$.

3. Consider the following keystream generating device made up of two LFSR-s and a combining XOR-operation. Is it possible to initialize the registers in such a way that the resulting stream has linear complexity 6?



4. Let e be the encryption function of a block cipher where the length of plaintexts, ciphertexts and keys is n. Consider the function $E : \{0,1\}^{2n} \to \{0,1\}^n$ defined by $E(x\|y) = e_{x\oplus y}(y)$, where $x, y \in \{0,1\}^n$. Can E be a one-way function?

The test makes up a quarter of the final grade.
All exercises in the test have equal weight.