T-110.5210 Cryptosystems
December 16, 2010 / Exam

THIS EXAM IS FOR 4 CREDITS

Each problem is worth 6 points. This is a 24 point exam.

1. (a) Draw and describe a Feistel network. Explain its use in block cipher design. Name one block cipher that uses this construction.

   (b) Draw and describe a Substitution-Permutation network. Explain its use in block cipher design. Name one block cipher that uses this construction.

   (c) Draw and describe the Merkle-Damgård construction of a hash function. Name one hash function that uses this construction.

2. Let $f(x) = x^4 + x + 1$ be the feedback polynomial of an LFSR.

   (a) Draw a block diagram of the LFSR.

   (b) What are the cycles (periods) of the sequences generated by this LFSR?

3. Consider the RSA cryptosystem with modulus $n = 37 \cdot 47 = 1739$.

   (a) Compute the private decryption exponent d using public encryption exponent $e = 257$.

   (b) Encrypt the message $m = 38$.

4. Consider Diffie-Hellman key exchange in $\mathbf{F}_2[x]/(x^4+x+1)$ with generator $g = x+1$. Alice's secret exponent is $a = 7$ and Bob's secret exponent $b = 9$. Compute the shared key K.

Feedback from students plays a vital role in improving this course. Please submit any feedback by following the link through the course Noppa page.