T-110.503 Basics of Cryptology
Exam
17.12.2002

1. (6 points) The length of the key of a cryptographic system is 100 bits. Key generation is performed using a pseudorandom number generator which generates the key in blocks of five bits. The generator is flawed in such a way that it only produces five bit blocks where the number of ones is less than the number of zeroes. Every such block occurs with equal probability. What is the actual strength of the key produced by this generator, that is, how many bits of entropy the key has?

2. (6 points) Consider an S-box with three input bits and three output bits defined using the function $\pi_S(z) = z^3$, for $z \in \mathbb{Z}_2[x]/(x^3 + x + 1)$. For example, $\pi_S(\mathtt{011}) = \pi_S(x + 1) = (x + 1)^3 = x^3 + x^2 + x + 1 = x^2 = (\mathtt{100})$. Compute the row of the *Difference Distribution Table* of π_S corresponding to the input difference $a' = \mathtt{100}$.

3. (6 points) Assume that AES block cipher is used in the CBC mode.

   a) Estimate the number of ciphertext blocks needed to have the probability of finding two equal ciphertext blocks to become larger than 0.5?

   b) Assume that two equal ciphertext blocks are detected, which have been produced using the same key (and the CBC mode). What can then be said about the corresponding plaintext blocks?

4. (6 points) Consider $p = 2003$, which is a prime. Find an element of order $q = 13$ in the multiplicative group $\mathbb{Z}^*_{2003}$.

5. (6 points) Suppose that $n = 84773093$ is the modulus and $b = 37869107$ is the public exponent in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine also the secret exponent a and $\phi(n)$.