Cryptography

Problem set 2 - 13-14 III 2013

Definition A function f is negligible if for every polynomial $p(\cdot)$ there exists an N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.

Problem 1 The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^{cn^{\frac{1}{3}}(\log n)^{\frac{2}{3}}}$. Assuming $4GHz$ computers and $c = 1$ (and that the units of the given expression are clock cycles), estimate the size of numbers that cannot be factored for the next 100 years.

Problem 2 Let f, g be negligible functions. Show that:

1. The function $h(n) = f(n) + g(n)$ is negligible .
2. For any positive polynomial p, the function $h(n) = p(n) \cdot f(n)$ is negligible .

Problem 3 Solving SUDOKU is an NP-complete problem. Design a secret-key encryption scheme that bases on the hardness of solving SUDOKU. Prove that an adversary who breaks secrecy of your scheme can be used as an oracle to solve SUDOKU problem.

Problem 4 Use Hamiltonian cycle problem to design an encryption scheme (or authentication scheme) which security is reducible to the NP-hardness of the underlying problem.

Problem 5 Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme $\langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m_0, m_1 \in \mathcal{M}$, and all $c_0, c_1 \in \mathcal{C}$ with $P(C_0 = c_0 \wedge C_1 = c_1) > 0$:

$$P(M_0 = m_0 \wedge M_1 = m_1 | C_0 = c_0 \wedge C_1 = c_1) = P(M_0 = m_0 \wedge M_1 = m_1),$$

where m_0 and m_1 are sampled independently from the same distribution over $\mathcal{M}$.

Prove that no encryption scheme satisfies this definition (hint: take $m_0 \neq m_1 but c_0 = c_1$).