Cryptography

Problem set 1

Definition 1. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every messsage $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $P[C = c] > 0$:

$$P[M = m|C = c] = P[M = m].$$

Definition 2. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$P[C = c|M = m] = P[C = c].$$

Definition 3. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$P[C = c|M = m_0] = P[C = c|M = m_1].$$

Definition 4. 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 $f(n) < \frac{1}{p(n)}$.

1. Prove or refute: definitions 1 and 2 are equivalent.
2. Prove or refute: definitions 2 and 3 are equivalent.
3. Prove or refute: definitions 1 and 3 are equivalent.
4. Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$P[M = m|C = c] = P[M = m'|C = c].$$

5. 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.
6. Let f, g be negligible functions. Show that:
   (a) The function $h(n) = f(n) + g(n)$ is negligible .
   (b) For any positive polynomial p, the function $h(n) = p(n) \cdot f(n)$ is negligible .
7. Find integer numbers X, Y such that $31X + 647Y = 1$.
8. Find 31^{-1} in Z^*_{647}.
9. Find a sequence $(a_i)_{i \geq 1}$ of natural numbers for which Euclidean algorithm needs exactly i iterations to find $\gcd(a_{i+1}, a_i)$.
10. Let $x = 130 \in Z^*_{899}$. Use Chinese Remainder Theorem to find a representation of x in $Z^*_{29} \times Z^*_{31}$.
11. Let $p = 29$, $q = 31$ and let $x = (22, 4) \in Z^*_p \times Z^*_q$. What is the value of x in Z^*_{899}?
12. Find $13^{3038} \bmod 3037$ and $139^{3035} \bmod 3037$.
13. Find $130^{839} \bmod 899$.