Cryptography

Problem set 2

Definition A generator $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is predictable if there exists an efficient (probabilistic polynomial time) algorithm $\mathcal{A}$ and such an $i : 1 < i < l(n)$ that:

$$P\left[\mathcal{A}(G(x)_{1\dots i}) = G(x)_{i+1}\right] > \frac{1}{2} + \varepsilon(n)$$

for a non-negligible function $\varepsilon(n)$.

Problem 1 Show that if G is a pseudorandom generator then G is unpredictable.

Problem 2 Let $\mathsf{G} : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator. Design a computationally unbounded distinguisher $\mathcal{D}$ which predicts next bits of G's output with non-negligible advantage.

Problem 3 Let G be a pseudorandom generator where $|G(s)| > 2|s|$.

1. Define $G'(s) = G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?
2. Define $G'(s) = G(s_1 \dots s_{n/2})$, where $s = s_1 \dots s_n$. Is G' necessarily a pseudorandom generator?

Problem 4 Let G be a pseudorandom generator and define $G'(s)$ to be the output of G truncated to n bits (where $|s| = n$). Prove that the function $F_k(x) = G'(k) \oplus x$ is not pseudorandom.

Problem 5 Let $G : \{0,1\}^s \to \{0,1\}^n$ be a pseudorandom generator. Which of the following generators are also pseudorandom?

1. $G'(x) = G(0)$
2. $G'(x) = G(x)||G(x)$
3. $G'(x) = G(x)||0$.
4. $G'(x) = G(x)_{0,\dots,n-2}$ ($G'(x)$ takes as its output first $n-1$ bits of $G(x)$)
5. $G'(x) = G(k) \oplus 1^n$.

For each case: prove or refute pseudorandomnes of G'.

Problem 6 Let G be a pseudorandom generator and define $G'(s) = G(s)_{1\dots n}$ (output truncated to the first n bits) for $|s| = n$. Prove that the function $F_k(x) = G'(k) \oplus x$ is not pseudorandom.

Problem 7 Let F be a pseudorandom function, and G a pseudorandom generator with expansion factor $l(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. In each case, the shared key is a random $k \in \{0,1\}^n$.

1. To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$ and send $\langle G(k) \oplus m_1, G(k+1) \oplus m_2 \rangle$.
2. To encrypt $m \in \{0,1\}^{n+1}$, choose a random $r \leftarrow \{0,1\}^n$ and send $\langle r, G(r) \oplus m \rangle$.
3. To encrypt $m \in \{0,1\}^n$, send $m \oplus F_k(0^n)$.
4. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose $r \leftarrow \{0,1\}^n$ at random, and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Problem 8 Prove that ECB mode of encryption does not yield CPA-secure encryption regardles of function F.

Problem 9 Prove that CTR mode of encryption does not yield CCA-secure encryption regardles of function F.