0. This problem is a reading exercise, and will not be graded. Read the following from Jonathan Katz’s lecture notes from his Fall 2002 course: (a) Section 3.1, Lecture 14, on Pseudorandom Permutations; and (b) CFB mode and Counter mode, Lecture 17.

1. Suppose \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) is an one-way permutation. Consider the function \( h : \{0,1\}^n \rightarrow \{0,1\}^n \), where \( h(x) \) is the AND of all the \( n \) bits of \( x \). Show that \( h \) is \textbf{not} a hardcore bit for \( f \); do this by showing that given \( f(x) \), we can predict \( h(x) \) with probability 1 (i.e., with absolute certainty), in polynomial time.

2. Let \( G : \{0,1\}^* \rightarrow \{0,1\}^* \) be a PRG such that \( |G(x)| = |x| + 1 \), for all strings \( x \). Let \( p(k) \) be any particular polynomial function of \( k \), and define \( H : \{0,1\}^k \rightarrow \{0,1\}^{k+p(k)} \) by \( H(x) = G(G(G(\cdots(x))) \))", where \( G \) is applied \( p(k) \) times. (Thus, we stretch the given \( k \)-bit string \( x \) to a new string of length \( k + p(k) \).) Prove that \( H \) is a PRG. (We had done this in class for the special case where \( p(k) = 2 \).

3. Consider the following message authentication scheme. Suppose the messages are elements of the field \( \mathbb{Z}_p \) for some known prime \( p \); the secret key (for authentication) is a pair of elements \( a \) and \( b \) of \( \mathbb{Z}_p \). (Thus, \( a,b \) are known to Alice and Bob, but not to the adversary.) To authenticate a message \( M \in \mathbb{Z}_p \), the tag computed is \( (aM + b) \mod p \). Show that this message authentication scheme is insecure.

G1. (For graduate students only.) Suppose \( G : \{0,1\}^k \rightarrow \{0,1\}^{k+1} \) is a PRG. Let \( h_1(x) \) be the \( k \)-bit string denoting the first \( k \) bits of \( G(x) \), and let \( h_2(x) \) be the bit denoting the last bit of \( G(x) \). Show that the following function \( H : \{0,1\}^k \rightarrow \{0,1\}^{k+2} \) is also a PRG:

\[
H(x) = G(h_1(x)) \circ h_2(x),
\]

where “\( \circ \)” denotes concatenation. (\textbf{Hint:} Use an appropriate hybrid argument.)