Problem 1 (20 points)
Prove or disprove the following statements

- (10 points) \( \text{TIME}(n^{2006}) \) is closed under efficient, i.e., \( O(\log n) \)-space, reductions.
- (10 points) \( \text{NSPACE}(\log n) \) consists of the languages \( L \) such that each positive instance \( x \) of \( L \) has an \( O(\log n) \)-size certificate that can be verified in \( O(\log n) \) space.

Problem 2 (15 points)
Prove or disprove the following statement:

If \( L \) is an \( \text{NP} \)-complete language that also belongs to \( \text{co-NP} \), then \( \text{NP} = \text{co-NP} \).

Problem 3 (20 points)

- (5 points) What is a semantically secure encryption scheme?
- (5 points) What is an unforgeable signature scheme?
- (5 points) What is a secure commitment scheme?
- (5 points) What is a uniform family of polynomial circuits for a language?

Problem 4 (15 points)
Let \( f(n) \geq n \) be a proper complexity function. Prove or disprove that the following language is in \( \text{TIME}(f(\lfloor \frac{n}{4} \rfloor)) \):
\[
\{M; x \mid M \text{ halts on } x \text{ at “no” in } f(|x|) \text{ steps.}\}.
\]

Problem 5 (15 points)

- (5 points) Define the complexity class \( \text{IP} \).
- (10 points) Prove that \( \text{IP} \) is closed under polynomial-time reductions. You may use anything we have seen in class, with or without a proof, in a black-box manner.

Problem 6 (15 points)
Richard Karp proved in his famous 1972 paper that both of the following problems are \( \text{NP} \)-complete.

- \text{FEEDBACK VERTEX SET}: Given a directed graph \( G \) and an integer \( k \), the problem is to determine whether or not there is a subset \( V \) of \( G \)'s nodes with \( |V| \leq k \) such that the deletion of \( V \) (and its incident edges) from \( G \) resulting in an acyclic graph.

- \text{FEEDBACK ARC SET}: Given a directed graph \( G \) and an integer \( k \), the problem is to determine whether or not there is a subset \( E \) of \( G \)'s directed edges with \( |E| \leq k \) such that the deletion of \( E \) from \( G \) resulting in an acyclic graph.

You are asked to prove that one of the above two problems is \( \text{NP} \)-hard. You can choose any one you like. You may prove from sketch or by a reduction from any problem whose \( \text{NP} \)-hardness has been ensured in our class. (Hint: Karp’s proofs are reductions from Vertex Cover.)