

HIT — Cryptography — Homework 2

September 18, 2018

Problem 1. Assuming the existence of a variable output-length pseudorandom generator, present a construction of variable-length encryption scheme, and prove that your construction has indistinguishable encryptions in the presence of an eavesdropper. Hint: the construction of secure fixed-length encryption scheme also holds here.

Problem 2. Assume $f(s)$ and $f'(s)$ are PRGs. Is $g(s) = f(s) \oplus f'(s)$ also necessarily a PRG? How about $g(s) = f(s) \oplus s$?

Problem 3. Assuming the existence of a pseudorandom function, prove that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper, but is not CPA-secure. Hint: You will need to use the fact that in a CPA the adversary can choose its queries to the encryption oracle adaptively (i.e., new query may be constructed from previous queries).

Problem 4. Present a construction of a variable output-length pseudorandom generator from any pseudorandom function. Prove that your construction satisfies Definition: ‘a variable output-length pseudorandom generator’.

Problem 5. Show that the CBC mode do not yield CPA-secure encryption in the case that the IV is predictable. Hint: The messages presented by the adversary could be constructed from the predictable IV and previous queries.

Problem 6. Show that the CBC, OFB and CTR modes do not yield CCA-secure encryption schemes (regardless of F). Hint: If one bit of Ciphertext is flipped, so does one bit of Plaintext.