University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Review Questions

1. Exercise 3.3.
2. Exercise 3.4.
3. Exercise 3.6.
4. Exercise 3.7.
5. Exercise 3.8.
6. Consider the following (informal) definition of security for a private-key encryption scheme: The adversary outputs a set of *three* (equal-length) messages m_1, m_2, m_3; an index $i \in \{1, 2, 3\}$ is chosen uniformly at random; then m_i is encrypted and the resulting ciphertext is given to the adversary. The adversary outputs i', and succeeds if $i' = i$. A scheme Π is secure if for all probabilistic polynomial-time adversaries it holds that $\Pr[i' = i] \leq 1/3 + \mathsf{negl}(n)$.
   (a) Write a formal definition corresponding to the above.
   (b) Prove that if a symmetric-key encryption scheme Π is computationally indistinguishable, then Π is secure in the sense defined above.
7. Recall the "pseudo-one-time pad" encryption scheme where $\mathsf{Enc}_k(m) = G(k) \oplus m$. In class we proved that if G is a pseudorandom generator then the pseudo-one-time pad scheme is computationally indistinguishable. Prove the converse.
8. Let G be a pseudorandom generator whose output is twice as long as its input. Define a keyed function F as follows: $F_k(x) = G(k) \oplus x$ (the block length of F is twice the key length). Prove that F is not a pseudorandom function.
9. Exercise 3.14.
10. Exercise 3.15.
11. Exercise 3.16.
12. (*) Exercise 3.20.
13. (*) Exercise 3.21.

14. Exercise 4.2.

15. Exercise 4.3.

16. Exercise 4.4.

17. (*) Exercise 4.5.

18. Exercise 4.6.

19. Exercise 4.8.

20. Exercise 4.9.

21. (*) Prove that *appending* the message length before applying CBC-MAC does not yield a secure MAC for variable-length messages.

22. (**) Consider instantiating CBC-MAC using a deterministic, fixed-length message authentication code Π (with tag length equal to the message length) in place of a pseudorandom function. Show that it is possible for Π to be a secure MAC, yet for the resulting CBC-MAC to be insecure even for messages of some fixed block length.

23. Exercise 4.11.

24. Exercise 4.15.

25. Exercise 4.17.

26. Exercise 4.20.

27. Exercise 4.21.