UNIVERSITY OF BIRMINGHAM

School of Computer Science

Security and Networks

Main Summer Examinations 2021

Security and Networks

Question 1

(a) Consider RSA encryption with $n = 35$, which is a product of two primes $p = 5$ and $q = 7$. Let $e = 5$. What is the plaintext corresponding to the ciphertext 9? Show your workings. **[10 marks]**

(b) Assume you construct a MAC by encrypting the message with AES in counter mode and taking the last block of this encryption. Is this a good MAC? Justify your answer. **[10 marks]**

Question 2

You are reviewing a web application for an online shop written in PHP for security issues. The web application keeps a log of the orders. Each log entry is the encryption of pair consisting of the order details and the hash of the order details.

(a) The web application uses a SHA256 hash of the current Unix timestamp (retrieved through `time()`) to generate a token to protect against Cross-Site Request Forgery (CSRF). Is this secure? Justify your answer.

[10 marks]

(b) Assume the encryption of the log entries uses AES in counter mode. However, the random number generator used for the counter mode is defective and produces only 100 different values. If an attacker has access to the logs and can create orders, is it possible for the the attacker to find the order details for at least some other orders? Justify your answer. **[10 marks]**

Question 3

(a) Assume malware manages to install a new certificate in the browser. Is it possible for an attacker who can read and modify network traffic to read TLS-encrypted sessions which the browser starts? Justify your answer. **[10 marks]**

(b) A webserver uses TLS for all connections. Does this prevent cross-site-scripting attacks? Justify your answer. **[10 marks]**