CS 435: Introduction to Cryptography **2020 Spring**

Final Exam

Professor Somesh Jha May 8, 2020

1. **(20 points)** Prove that RSA is insecure against a chosen ciphertext attack. In particular, given a ciphertext y, describe how to chose a ciphertext $y' \neq y$, such that knowledge of the plaintext $x' = D_k(y')$ allows $x = D_k(y)$ to be computed.

2. **(10 points)** Let N be a positive integer, and m and m_1 be two positive integers in $Z_N^\star$. Show how to obtain a $m_2 \in Z_N^\star$ such that $m \equiv m_1 \cdot m_2 \pmod{N}$.

3. **(40 points)** Complete the following parts:

   i. Describe the RSA-signature scheme.

   ii. Describe how CRT can be used to speed up the signing step in the RSA-signature scheme.

   iii. Describe two attacks on the scheme given above (i.e., no-message attack and multiplicative attack).

   iv. Briefly describe how "Hash-then-Sign" paradigm addresses the attacks shown previously.

4. **(10 points)** Describe in detail the man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key k_A with Alice and a different key k_B with Bob, and Alice and Bob cannot detect that anything has gone wrong. Briefly describe a fix for this attack.

5. **(10 points)** In class we showed an attack on the plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a single signing query.

6. **(10 points)** Consider the system of equations given below:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ 3x &\equiv 3 \pmod{5} \\ 2x &\equiv 2 \pmod{7} \end{aligned}$$

   Transform the above system of equations so that CRT theorem applies, and then solve it.