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

Final Exam

Professor Somesh Jha Dec 12, 2020

1. **(20 points)** Let G be a cyclic group of order or size q (a prime) with generator g. Let $S \subseteq G$ be a subset of G of size k. Assume that *Eve* can compute the discrete logs of all the elements in set S. Show that *Eve* can compute discrete log of an arbitrary element of G with probability $\frac{k}{q}$.

2. **(20 points)** Let n be a positive integer. Justify whether following statements are true or false.
   (Stmt 1): For all x and y in Z_n there exists a $z \in Z_n$ such that $x \equiv yz \pmod{n}$.
   (Stmt 2): For all x and y in $Z_n^\star$ there exists a $z \in Z_n^\star$ such that $x \equiv yz \pmod{n}$.

3. **(30 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:

$$\begin{aligned} 2x &\equiv 2 \pmod{9} \\ 4x &\equiv 3 \pmod{5} \\ 5x &\equiv 2 \pmod{7} \end{aligned}$$

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