CS 435: Introduction to Cryptography **2012 Fall**

Homework 5

Professor Somesh Jha **Due:** December 14

1. Solve for x in the following system of congruences:

$$\begin{aligned} 13x &\equiv 4 \pmod{99} \\ 15x &\equiv 56 \pmod{101} \end{aligned}$$

Hint. First use Euclid's algorithm and then apply the Chinese Remainder Theorem.

2. 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.

Hint. Use the multiplicative property of RSA, i.e., that

$$E_k(x_1)E_k(x_2) \bmod n \;=\; E_k(x_1x_2 \bmod n)$$

3. (Problem 9.2) 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 ance Bob cannot detect that anything has gone wrong.

   What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

4. (Problem 9.3) Consider the following key-exchange protocol:

   i. Alice chooses $k, r \leftarrow \{0,1\}^n$ at random, and sends $s := k \oplus r$ to Bob.

   ii. Bob chooses $t \leftarrow \{0,1\}^n$ at random and sends $u := s \oplus t$ to Alice.

   iii. Alice computes $w := u \oplus r$ and sends w to Bob.

   iv. Alice outputs k and Bob computes $w \oplus t$.

   Show that Alice and Bob output the same key. Analyze the security of the scheme, i.e., either prove its security or show a concrete attack.