CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Homework #5

Due November 15, 2012, beginning of the class

1. On Euler's φ function.

   (a) Show that, for a prime p,

   $$\varphi(p^i) = (p-1)p^{i-1}.$$

   (b) Show that, for co-prime m_1 and m_2,

   $$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

   (c) Use the results in the previous two parts to obtain $\varphi(n)$ for an arbitrary n. (Hint: Consider the prime factorization of n, and then combine the previous results by the CRT to obtain $\varphi(n)$.)

2. Question 4, the midterm exam of Fall 2011.

3. A protocol to establish a fresh session key using long-term, certified Diffie-Hellman public keys is as follows:

   - The system has a common prime modulus p and a generator g. Each party i has a long-term private key $\alpha_i \in Z_{p-1}$ and a public key $P_i = g^{\alpha_i} \bmod p$.
   - To establish a session key between i and j, party i generates a random $R_i \in Z_{p-1}$, computes $X_i = \alpha_i + R_i \bmod p-1$, and sends X_i to j. Similarly, j computes a random $R_j \in Z_{p-1}$, $X_j = \alpha_j + R_j \bmod p-1$, and sends X_j to i.
   - i computes the session key as

     $$K_{i,j} = (g^{X_j} P_j^{-1})^{R_i} \bmod p$$

     and j computes

     $$K_{j,i} = (g^{X_i} P_i^{-1})^{R_j} \bmod p.$$

   (a) Show that the protocol is correct (i.e., $K_{i,j} = K_{j,i}$).

   (b) Show that a passive attacker Trudy who has broken a session key $K_{A,B}$ between Alice and Bob can compute any future session keys between these two parties.

   (c) Describe a simple addition to the session key computation which will preclude this and any similar attacks on this protocol.