

## Homework #2

Due April 9, 2013, 15:40, beginning of the class

1. Find the solution of the system

$$x \equiv 3 \pmod{4}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{7}$$

in  $\mathbb{Z}_{140}$ , using the Chinese Remainder Theorem and the extended Euclid's algorithm. Show all your work.

2. On number theory basics.

- (a) Show that the RSA decryption operation is correct (i.e.,  $(x^e)^d \bmod n = x$ ) for all  $x \in \mathbb{Z}_n$  even if  $x \notin \mathbb{Z}_n^*$ . (Hint: Show the correctness both in  $\mathbb{Z}_p$  and in  $\mathbb{Z}_q$ , and argue by the CRT that it must be correct in  $\mathbb{Z}_n$ .)

- (b) Show that, for a prime  $p$ ,

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

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

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

- (d) 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  $\varphi(n)$ .)

3. In an RSA-based secure communications system, it may be desirable to simplify the key generation and management process by using a system-wide common modulus  $n$ , generated by a trusted key generation authority, and user-specific key pairs  $(e, d)$ . Show that such a common-modulus system is totally insecure against insider attacks by proving the following steps:

- (a) Eve, possessing a key pair  $(e_E, d_E)$ , can easily compute a multiple of  $\varphi(n)$ , say  $k \cdot \varphi(n)$ .

- (b) If Alice's public key  $e_A$  is relatively prime to  $k$ , Eve can find a decryption exponent for Alice and read all her messages.
  - (c) Eve can compute a decryption exponent for any user in the system, whether or not  $\gcd(e, k) = 1$ .
4. Consider a variant of the ElGamal signature scheme where  $p, q, g, \alpha, \beta, k, r$  are as in the original scheme as described in class and

$$s = (r\alpha + k)m^{-1} \bmod q.$$

- (a) What is the signature verification formula for this modified scheme?
  - (b) Show that this ElGamal variant is insecure. (Hint: Show that attacker Eve who has observed the signature of a message  $m$  can obtain the signature of any message she likes.)
5. A DH-based key exchange protocol for wireless mobile networks 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  $\alpha_i \in \mathbb{Z}_{p-1}$  and a public key  $P_i = g^{\alpha_i} \bmod p$ .
- To establish a session key between a mobile subscriber  $M$  and a base station  $B$ , the following protocol is executed:

$$\begin{aligned} B \rightarrow M & : g^{\alpha_B + R_B} \bmod p \\ M \rightarrow B & : \alpha_M + R_M \bmod (p-1) \end{aligned}$$

where  $R_B$  and  $R_M$  are one-time random secrets.

- $B$  calculates the session key as

$$K_{MB} = (g^{\alpha_M + R_M} P_M^{-1})^{R_B} \bmod p$$

and  $M$  calculates it as

$$K_{MB} = (g^{\alpha_B + R_B} P_B^{-1})^{R_M} \bmod p.$$

Then they complete the authentication with a challenge-response protocol with  $K_{MB}$ .

- (a) Show that the protocol is correct in the sense that  $B$  and  $M$  calculate the same  $K_{MB}$  value.
- (b) Show that an attacker who has compromised a session key from a previous run, for which she has recorded the messages, can impersonate  $B$ . (Hint: Let the attacker replay  $B$ 's message from the previous session.)
- (c) In fact this protocol can be broken without having any previous session keys compromised: Show how the attacker can impersonate  $B$  by just knowing his public key.