Introduction to Cryptography

Final – take home part

December 20, 2006

1. Assume that my RSA-key is (n, e) with

$$n = 108617454629908975349078168530107932195 71,$$
$$e = 65537.$$

Send me an RSA-encrypted message by email.

2. *The Trouble with Chinese Remainders.*

Consider the RSA signature protocol; Alice has a public RSA-key (n, e), where $n = pq$. To sign a message m (or its hash value), she computes $x = m^d \bmod n$ and sends (m, x) to Bob, who then checks that $x^e \equiv m \bmod n$.

Since d is a large integer, Alice will save computing time if she computes x as follows: compute $r \equiv m^{d_p} \bmod p$ and $s \equiv m^{d_q} \bmod q$, where $d_p e \equiv 1 \bmod p - 1$ $d_q e \equiv 1 \bmod q - 1$, and then use the Chinese remainder theorem to get x.

(a) Describe in detail how Alice computes x, and show that it works.

(b) Assume that an error occurs in the computation of s, but that r is computed correctly. Let s' and x' denote the results the computer gives instead of the correct values s and x. Explain why, most likely, $\gcd((x')^e - m, n)$ is a nontrivial factor of n.

(c) Let (n, e) as in problem 1, and consider the message

$$m = 31415926535897932384626433 83.$$

Alice computes

$$r = 6984458519368146710 9,$$
$$s = 8712412017968894072 6.$$

Use the Chinese Remainder Theorem to compute x' and use this (together with m, n and e) to factor n.

(d) Discuss methods to prevent this attack.

3. Use Pohlig-Hellman to solve the following DLP: $a \equiv g^x \bmod p$ for $p = 556988536090052377769$, $g = 3$, and $a = 2$.