Problem Set 7 – Due Wednesday, June 1, 2011

Problem 25. Problem 6.6 from [PP].

Problem 26. The conjectured running time to factor a number \( n \) with the “Number Field Sieve” (NFS), the best known algorithm for factoring, is about

\[
O(e^{1.923 (\ln n)^{1/3} (\ln \ln n)^{2/3}}).
\]

In December of 2009 a number of 768 bits was factored, RSA-768, using the NSF. The project required about \( 2^{67} \) machine cycles (roughly 1500 years of compute time).

Part A. Estimate how much longer it will take to factor a number of 1024 bits instead?

Part B. Use “Moore’s Law” to estimate when RSA-1024 will be factored. State the assumptions you are making for doing your estimate.

Problem 27. Suppose you wish to generate a random RSA modulus \( n \) that is the product of two 1024-bit primes \( p \) and \( q \) and for which \( e = 3 \) is a valid encryption exponent. Your algorithm is to generate random odd 1024-bit numbers until you find a first prime \( p \); then generate random 1024-bit numbers until until you find a second prime \( q \); then start all over again 3 is not a valid encryption exponent for \( n = pq \).

Estimate the expected number of random odd numbers you will need to generate.

Problem 28. Let \( \Pi = (K, E, D) \) be a public-key encryption scheme. Can it be IND-secure\(^1\) with each of the following “defects”? Briefly justify each answer that you make.

Part A. Encryption of a plaintext \( P \) leaks the last bit of \( P \)—it is easily computable from the ciphertext \( C \).

Part B. Encryption of a plaintext \( P \) leaks the length of \( P \)—it is easily computable from the ciphertext \( C \).

Part C. Encryption of a plaintext \( P \) leaks the identity of the key \( pk \) with which it is encrypted—it is easy to distinguish if a given ciphertext was meant for Alice (it’s encrypted under her key) or for Bob (it’s encrypted under his).

Part D. Encryption of a equal-length plaintexts \( P \) and \( P' \) can take radically different amounts of time.

Part E. Encryption of the secret key \( sk \) under its public key \( pk \) leaks \( sk \)—it is easily computable from the ciphertext \( C \).

\(^1\) I refer here to the definition given in class—that \( \text{Adv}^{\text{IND}}_{\Pi}(A) = \Pr[A^{E_{K}(\cdot)}(pk) \Rightarrow 1] - \Pr[A^{E_{K}(\cdot^{-1})}(pk) \Rightarrow 1] \) is “small” for all “reasonable” \( A \).