Cryptography cs 4995
Instructor: Prof. Michael Rabin

Problem Set 3

Due: Tuesday, Feb. 27 2007

1. **(Secret Communication between Low and High Computing Powered Parties)** We mentioned in class that if Bob has a public key $n = pq$ then Alice can rapidly encrypt secret messages to Bob using a slow processer by employing the encryption scheme $y = x^2 \bmod n$. Bob is assumed to have greater computing power, say on a notebook, and knowing p and q can decrypt.

   - Devise a method for Alice and Bob, using this set-up, to enable Bob to send encrypted messages to Alice which she can rapidly decrypt despite her relatively lower computing power. (This was briefly discussed in class.)
   - Point out a way for an adversary to cheat Bob under this protocol.

2. **(Authentication of Senders and Receivers)** In class, we have explained how Diffie-Hellman key exchange may be used for establishing a common AES key. Explain why this is unsafe to use. Assume now that both Alice and Bob have published public keys N_A, N_B and possess the corresponding private keys and sufficient computing power to encrypt and decrypt messages. Devise a protocol for Alice and Bob to establish a common AES (Advanced Encryption Standard) key, ensuring both that they are communicating with each other. Note that we are not assuming that Alice and Bob have digital signature keys. The challenge is to counter adversaries pretending to be Alice or Bob and possibly mounting ”Man-in-the-middle” attacks.

3. **(Low Exponent Attack)** A professor of cryptography sends three TA's having public keys N_A, N_B and N_C the same secret message M by use of the $M^2 \bmod n$ encryption method. You, a cs student, can observe the three cyphertexts, $Y_i = M^2 \bmod N_i$ for $i = A, B, C$. Find a way to obtain the message from the keys and the cyphertexts. (Hint: Use CRT.) This is a relatively hard problem; don't hesitate to consult the teaching assistants for help.

4. **(Small numerical example for: decoding implies factorization)** Working out this example will illustrate the method of proof given in class. Let the public key be $n = 143 (= 11 * 13)$. Assume that there exists a decoding algorithm AL such that given a $y \equiv x^2 \pmod{n}$ computes a value $z = AL(y)$ satisfying $y \equiv z^2 \pmod{n}$.

   To factor n, you choose a random $x \in \mathbb{Z}_n^*$ and compute $y \equiv x^2 \pmod{n}$. Say you got $y = 69$ and that $AL(69) = 115$.

   (a) Using the factorization of n, verify that there are four values $x_1, \ldots, x_4$. such that $(x_i)^2 \equiv 69 \pmod{n}$. This is not a step in the factoization, only in the proof that decoding leads to factorization.

(b) Which two of these four values would, if initially chosen as x, lead to: $(x - 115, n) = (11 \text{ or } 13)$?

5. Google Challenge: Pascal takes a deck of ordinary cards and spreads them out on a table. You see that some of the cards are face up, and some are face down. Pascal closes the deck, hands it to you, and lets you interleave shuffle it as many times as you wish. You return the deck to him, and he places his hands with the deck into an empty black sack. Working in the sack, he divides the deck into two sub-decks. Upon inspection you find that the number of cards face up in the first sub-deck is the same as the number of cards face up in the second. How did Pascal do this? Note: the solution is purely mathematical (there are no tricks such as using cards with rough fronts, non-standard markings, etc.).