Cryptology 2014
(Home work 3)

April 10, 2014

- Due on April 25, 10 am. Hard copies of solutions are to be submitted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.

1. Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

2. Suppose Bob has an RSA cryptosystem with modulus N and encryption exponent e_b and Charlie has a RSA cryptosystem with the same same modulus N but an different encryption exponent e_c. Suppose also $\gcd(e_b, e_c) = 1$. Now, Alice encrypts the same plaintext x to send to Bob and Charlie, i.e., she computes $y_b = x^{e_b} \bmod N$ and $y_c = x^{e_c} \bmod N$, and then sends y_b to Bob and y_c to Charlie. Show that an adversary who intercepts both y_b and y_c can recover the plaintext x.

3. Let g is an element of prime order in the group $\mathbb{Z}_p^*$. Suppose we have an efficient algorithm which computes the Diffie Hellman function in base g, i.e., we have an algorithm $\mathcal{A}$ such that $\mathcal{A}(g^x, g^y) = g^{xy}$ for all $x, y \in \{1, 2, \ldots q\}$. Let $h = g^\alpha$ for some $\alpha \in \{1, 2, \ldots, q-1\}$. Show that given α there is an efficient algorithm $\mathcal{B}$ which can compute the Diffie-Hellman problem at base h, i.e., $\mathcal{B}(h, \alpha, h^x, h^y) = h^{xy}$. Algorithm $\mathcal{B}$ can use algorithm $\mathcal{A}$ as a subroutine.

4. A set of users $A_1, A_2, \ldots, A_n$ and B wish to generate a secret *conference key*, i.e, all valid users should know the key, but an eavesdropper should not be able to obtain any information regarding the key. They decide to use the following protocol: Let p be a public prime and $g \in \mathbb{Z}_p^*$ be of order q, where q is a large prime such that $q|(p-1)$. The element g is also public. Now, B selects $b \xleftarrow{\$} \{1, 2, \ldots, q-1\}$ and computes $y = g^b \in \mathbb{Z}_p^*$. Each user A_i picks a secret $a_i \xleftarrow{\$} \{1, 2, \ldots, q-1\}$ and computes $x_i = g^{a_i} \in \mathbb{Z}_p^*$. User A_i sends x_i to B. User B responds to user A_i by sending $z_i = x_i^b \in \mathbb{Z}_p^*$.

   (a) Show that A_i given z_i (and a_i) can determine y.

(b) Explain why y (or a hash of y) can be securely used as a conference key. You need to explain why at the end of the protocol all parties $A_1, A_2, \ldots, A_n$ and B know y, and also explain informally why an adversary cannot determine y.

(c) Prove part (b). You need to show the following: If there exists an efficient algorithm $\mathcal{A}$ that given the public values in the above protocol, outputs y, then there also exists an efficient algorithm $\mathcal{B}$ that breaks the computational Diffie-Hellman assumption in the subgroup of $\mathbb{Z}_p^*$ generated by g. Use algorithm $\mathcal{A}$ as a subroutine for your algorithm $\mathcal{B}$