Cryptography

Problem set 6 - 16-17 IV 2015

Problem 1 Prove that if G, H are groups then $G \times H$ is a group.

Problem 2 Let $N = pq$ and let $[N, e_1], [N, e_2]$ be public keys of Alice and Bob respectively. Show that if Eve sends encrypted messages to Alice $c_1 = m^{e_1} \bmod N$ and Bob $c_2 = m^{e_2} \bmod N$ and you intercept them then you can recover m from c_1 and c_2. What is the success probability of your attack?.

Problem 3 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.

Problem 4 Let $N = pq$ be a product of two distinct primes. Show that if N and an integer d such that $3d = 1 \bmod \phi(N)$ are known, then it is possible to compute p and q in polynomial time.

Problem 5 Determine whether or not the following problem is hard. Let p be prime, and fix $x \in \mathcal{Z}^*_{p-1}$. Given p, x, and $y := [g^x \bmod p]$ (where g is a random value between 1 and $p-1$), find g; *i.e.*, compute $y^{1/x} \bmod p$. If you claim the problem is hard, show a reduction (to *i.e.*, discrete logarithm problem). If you claim the problem is easy, present an algorithm, justify its correctness, and analyze its complexity.

Problem 6 Prove formally that the hardness of the Computational Diffie-Helman (CDH) problem relative to $\mathcal{G}$ implies the hardness of the discrete logarithm problem relative to $\mathcal{G}$.

Problem 7 (1 point) Let p, N be integers with $p|N$. Prove or disprove that for any integer X:

1. $[[X \bmod N] \bmod p] = [X \bmod p]$,
2. $[[X \bmod p] \bmod N] = [X \bmod N]$.

Problem 8 (each part for 1 point) Let $|N|$ denotes the length of binary representation of N.

1. Show that if $N = M^e$ for some integers $M, e > 1$ then $e \leq |N| + 1$.
2. Given N and e with $2 \leq e \leq |N| + 1$, show how to determine in $poly(|N|)$ time whether there exists an integer M with $N = M^e$.
3. Given N, show how to let test in $poly(|N|)$ time whether N is a perfect power.

Problem 9 (2 points) Let $\langle N, e\rangle$ be a public and d a private key of the RSA encryption. You know that $d < \sqrt[4]{N}/3$. Find d. Hints:

- show that there exists such a k that $ed - k\phi(N) = 1$.
- try to approximate $\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| = \frac{1}{d\phi(N)}$ with public data and assumptions.
- use continued fraction to approximate d (k/d).

You can use the following data to illustrate your algorithm:
$\langle N, e\rangle = \langle 1335815453373977, 100169346544615\rangle$.

Problem 10 (2 points) Extend your algorithm from Problem 3 to the case $d < \sqrt{N}$.

Problem 11 (1 point) Let $\langle N, e\rangle$ be a public RSA key. For a plaintext m, let $c = m^e \bmod N$ be a corresponding ciphertext. Prove that there exists a positive integer k such that:

$$m^{e^k} = m \bmod N$$

and

$$c^{e^{k-1}} = m \bmod N.$$

Is this dangerous for RSA?

Problem 12 Prove that the hardness of the Decisional Diffie-Helman (DDH) problem relative to $\mathcal{G}$ implies the hardness of the Computational Diffie-Hellman problem (CDH) relative to $\mathcal{G}$.