Cryptography

Problem set 5 - 24-25 IV 2013

Problem 1 (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 2 (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 3 (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 4 (2 points) Extend your algorithm from Problem 3 to the case $d < \sqrt{N}$.

Problem 5 (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 6 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 $\mathcal{G}$.