COSC 530: Homework 4

Problem 1. (100 points.)

(Part A - 50 points.) Show that DDH is easy in the multiplicative group \( \mathbb{Z}_p^* \) for prime \( p \). That is, show that there is an efficient adversary whose DDH-advantage is close to 1 for this group.

(Part B - 50 points.) Show that RSA leaks the Jacobi symbol. That is, show that there is an efficient algorithm that on input \((N, e, y)\) for RSA parameters \( N, e \) and \( y \leftarrow \text{RSA}_{N,e}(x) \), outputs the Jacobi symbol of \( x \), for any \( x \in \mathbb{Z}_N^* \). (I didn’t cover Jacobi symbol in class — look it up.)

Problem 2. (100 points.)
Consider “plain RSA” encryption with message-space \( M = \{0, 1, \ldots, 2^{64}\} \), where a public key is \((N, e)\) and a secret key is \((N, d)\), obtained via some RSA generator. Encryption of \( x \in M \) is \( x^e \mod N \). Show that for 35% of the plaintexts \( x \in M \), an adversary can recover \( x \) from its encryption using only \( 2^{35} e \)-th powers mod \( N \).

**Hint:** Use the fact that about 35% of \( x \in M \) can be written as \( x = x_1 \cdot x_2 \) for \( x_1, x_2 \in \{0, 1, \ldots, 2^{34}\} \).

What does this tell you about the security of plain RSA in practice?

Problem 3. (100 points.)
Study Theorem 2 and its proof in [https://eprint.iacr.org/2008/067.pdf](https://eprint.iacr.org/2008/067.pdf) very carefully. Wait a day or two, then, without looking at the paper again, write the theorem and proof in your own words. (If you get stuck, go back to the first step.) Bonus points if you write it as a poem or song. Or if you find a different proof.