**CSCI/MATH 388:** Cryptography | Spring 2023
Department of Computer Science | Reed College
**Problem Set 5:** | **Instructor:** Chanathip Namprempre

---

# Problem Set 5

1. Answer the following questions regarding $\mathbf{Z}_{23}^*$.
   (a) What are the elements of $\mathbf{Z}_{23}^*$? List all of them.
   (b) What is the order of this group?
   (c) What is the order of 2?
   (d) What is the order of 5?
   (e) Is $\mathbf{Z}_{23}^*$ cyclic? If your answer is "yes," provide a generator. If your answer is "no," explain your answer.

2. Prove that the hardness of the DDH problem implies the hardness of the CDH problem. Use the definitions of these problems as specified in the lecture slides.

3. Let $p$ be an odd prime, and let $G$ be $\mathbf{Z}_p^*$. Suppose $g$ is a generator of $\mathbf{Z}_p^*$ but oddly enough is kept secret. Let $x \in \mathbf{Z}_{p-1}$, and let $y = g^x \bmod p$. Given inputs $p, x$, and $y$, is it possible to compute $g$ in polynomial time in the size of the inputs? Prove your answer. You may refer to algorithms we studied in class by name without explicitly defining how they work.

4. Compute $19^{571500000} \bmod 77$ by hand. Show your work and justify all the steps in your computation.

5. Prove that DDH is easy in $\mathbf{Z}_p^*$ when $p$ is an odd prime. Here, you may use without proof, the properties we studied in class about the Legendre (equivalently in this context, the Jacobi) symbol.

6. Suppose DDH is hard for a group $G$. Consider the ElGamal encryption scheme $(\mathsf{KG}, \mathcal{E}, \mathcal{D})$ based on $G$ as studied in class and recalled here for your convenience. (In the description, $g$ is a generator of $G$, and $m$ is its order.) Is this scheme secure under IND-CCA? Prove your answer.

| **Alg** $\mathsf{KG}$ | **Alg** $\mathcal{E}_X(M)$ | **Alg** $\mathcal{D}_x(Y, W)$ |
|---|---|---|
| $x \stackrel{\$}{\leftarrow} \mathbf{Z}_m$ | $y \stackrel{\$}{\leftarrow} \mathbf{Z}_m$ ; $Y \leftarrow g^y$ | $K \leftarrow Y^x$ |
| $X \leftarrow g^x$ | $K \leftarrow X^y$ | $M \leftarrow W \cdot K^{-1}$ |
| Return $(X, x)$ | $W \leftarrow K \cdot M$ | Return $M$ |
| | Return $(Y, W)$ | |

   As always, be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

7. Let $(N_1, e_1)$ and $(N_2, e_2)$ be the RSA public keys for Alice and Bob, respectively. Suppose however that by coincidence, $N_1$ and $N_2$ are not coprime. Can you compute the decryption exponents $d_1$ and $d_2$ belonging to Alice and Bob, respectively? Why or why not? Prove your answer.