COMP 537: Cryptography **Fall 2023**

Problem Set 3

Instructions: You **must** typeset your solution in LaTeX using the provided template. Please submit your problem set via Gradescope. Include your name and the names of any collaborators at the top of your submission.

Acknowledgment: Several of the problems in this problem set come from the Boneh-Shoup textbook.

Problem 1: DDH PRG [15 points]. Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Consider the following PRG defined over $(\mathbb{Z}_q^2, \mathbb{G}^3)$:

$$G(\alpha, \beta) := (g^\alpha, g^\beta, g^{\alpha\beta}).$$

(a) Prove that G is a secure PRG assuming that the DDH assumption holds in $\mathbb{G}$.

(b) Let $\mathbb{G}$ be the prime order order subgroup of $\mathbb{Z}_{23}^*$ generated by $g = 2$. What are the elements of the group $\mathbb{G}$, and what is the order q of group $\mathbb{G}$? In addition to stating the answer, please explain why this is the answer.

(c) Let $\mathbb{G}$ be the prime order order subgroup of $\mathbb{Z}_{23}^*$ generated by $g = 2$. What is the output of $G(5,6)$?

Note: you should be able to do this without a calculator, but it's ok to use one if you want.

Problem 2: Non-Binding Signatures [15 points]. It turns out that secure signatures are not necessarily *binding*. That is, suppose the signer generates a signature σ on a message m. The definition of a secure signature does not preclude the signer from producing another message $m' \neq m$ for which σ is a valid signature. It turns out binding isn't needed for many applications, so it's left out of the definition. That said, many signature schemes we have seen are in fact binding.

(a) Please give an example of a signature scheme that is *not* binding: for a given $(\mathsf{pk}, \mathsf{sk})$, the signer can find two distinct messages m_0 and m_1 where the same signature σ is valid for both messages under pk.

Hint: Consider using a hash and sign approach to building the signature scheme but with the discrete log-based hash function we discussed in class.

(b) Describe how the signer can produce a second message for the same signature.

(c) Give the intuition for why the scheme is secure. You should state the relevant assumptions and why they are needed, but you don't need to give a proof.

Problem 3: Attacking RSA-FDH [5 points]. Consider the RSA-FDH signature scheme. The public key is a pair (N, e) where N is an RSA modulus, and a signature on a message $m \in \mathcal{M}$ is defined as $\sigma := H(m)^{1/e} \in \mathbb{Z}_N$, where $H : \mathcal{M} \to \mathbb{Z}_N$ is a hash function. Suppose the adversary could find three messages $m_1, m_2, m_3 \in \mathcal{M}$ such that $H(m_1) \cdot H(m_2) = H(m_3)$ in $\mathbb{Z}_N$. Show that the resulting RSA-FDH signature scheme is no longer existentially unforgeable under a chosen message attack.

Problem 4: RSA Signatures with Same Modulus [15 points]. This problem explores why every party has to be assigned a different modulus $N = pq$ in the RSA trapdoor permutation. Suppose we try to use the same modulus $N = pq$ for everyone. Every party is assigned a public exponent $e_i \in \mathbb{Z}$ and a private exponent $d_i \in \mathbb{Z}$ such that $e_i \cdot d_i = 1 \bmod \varphi(N)$. At first, this appears to work fine. To sign a message, $m \in \mathcal{M}$, Alice would publish the signature $\sigma_a \leftarrow H(m)^{d_a} \in \mathbb{Z}_N$ where $H : \mathcal{M} \to \mathbb{Z}_N^*$ is a hash function. Similarly, Bob would publish the signature $\sigma_b \leftarrow H(m)^{d_b} \in \mathbb{Z}_N$. Since Alice is the only one who knows d_a and Bob is the only one who knows d_b, this seems fine.
Unfortunately, this scheme is completely insecure. Bob can use his secret key d_b to sign messages on behalf of Alice.

(a) Show that Bob can use his public-private key pair (e_b, d_b) to obtain a multiple of $\varphi(N)$. Denote this integer by V.

(b) Suppose Bob knows Alice's public key e_a, and assume for now that e_a is relatively prime to V. Show that for any message $m \in \mathcal{M}$, Bob can compute $\sigma \leftarrow H(m)^{1/e_a}$. In other words, Bob can invert Alice's trapdoor permutation and obtain her signature on m.

Hint. Recall since e_a and V are relatively prime, Bob can find an integer d such that $d \cdot e_a = 1 \bmod V$, i.e., Bob can compute the inverse of $e_a \bmod V$.

(c) Show how to make your solution in part (b) work even if e_a is not relatively prime to V.

Optional Feedback [5 points]. Please answer the following questions to help design future problem sets. You are not required to answer these questions (the points are free), and if you would prefer to answer anonymously, please use the anonymous feedback form. However, we do encourage you to provide feedback on how to improve the course experience.

(a) Roughly how long did you spend on this problem set?

(b) What was your favorite problem on this problem set?

(c) What was your least favorite problem on this problem set?

(d) Any other feedback for this problem set? Was it too easy/difficult?

(e) Any other feedback on the course so far?