Explain what an adversary would have to do to violate the Computational Diffie-Hellman assumption (CDH)

Question #1

Why isn’t raw RSA, $E_N(M) = M^3 \mod N$, a secure way to encrypt a plaintext $M \in \mathbb{Z}_N$?
Explain what an adversary would have to do to violate the Computational Diffie-Hellman assumption (CDH)

Question #1

Do well at computing $g^{ab}$ from $g^a$ and $g^b$ (for a random $a$, $b$, in a group $<g> = G$)

Why isn’t raw RSA, $E_N(M) = M^3 \mod N$, a secure way to encrypt a plaintext $M \in \mathbb{Z}_N$?

Question #1

- Because it’s deterministic.
- Because it won’t achieve IND.
- Because the RSA assumption doesn’t ensure that all of $M$ is concealed by applying the RSA function.
RSA PKCS #1, v. 1

\[
\left( \begin{array}{c} 00 \\ 02 \\ $$ \cdots $$ \\ 00 \\ M \end{array} \right)^e \mod N
\]
$M \oplus G(R) \rightarrow \oplus \rightarrow S \rightarrow \langle e \mod N \rangle$

$G(R) \rightarrow G \rightarrow \oplus \rightarrow H \rightarrow \oplus \rightarrow T$

$R \rightarrow k_0$

$M \rightarrow k_1$

[Bellare-Rogaway 1994], [Shoup 2001]
[Fujisaki, Okamoto, Pointcheval and Stern 2001]
The Random-Oracle Paradigm

1. Design your protocol pretending there’s a **public random oracle** that all parties can access.
2. Prove your protocol secure **in the random-oracle model** (ROM).
3. Instantiate the random oracle (RO) by a cryptographic hash function, or something derived from one.

**Thesis**: significant assurance remains despite the heuristic final step.

\[
\text{Adv}^\text{ind} \overset{\text{cca}}{\Pi} (A, k) = \Pr[(pk, sk) \leftarrow \mathcal{K}(k); A \Rightarrow 1] - \\
\Pr[(pk, sk) \leftarrow \mathcal{K}(k); A \overset{H}{\Rightarrow} \mathcal{D}_{sk}^H(\cdot), H, H^H, \mathcal{D}_{pk}^H(\cdot), H]
\]
RSA PKCS #1, v. 1

$M$

$H$

$00$ $01$ $FF \cdots FF$ $00$ $H(M)$

$d \mod N$