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

Question #1

Why isn't **raw RSA**, $\mathcal{E}_N(M) = M^3 \bmod N$, a secure way to encrypt a plaintext $M \in \mathbb{Z}_N$?

Question #1

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 $\langle g \rangle = G$)

Why isn't **raw RSA**, $\mathcal{E}_N(M) = M^3 \bmod N$, a secure way to encrypt a plaintext $M \in \mathbb{Z}_N$?

Question #1

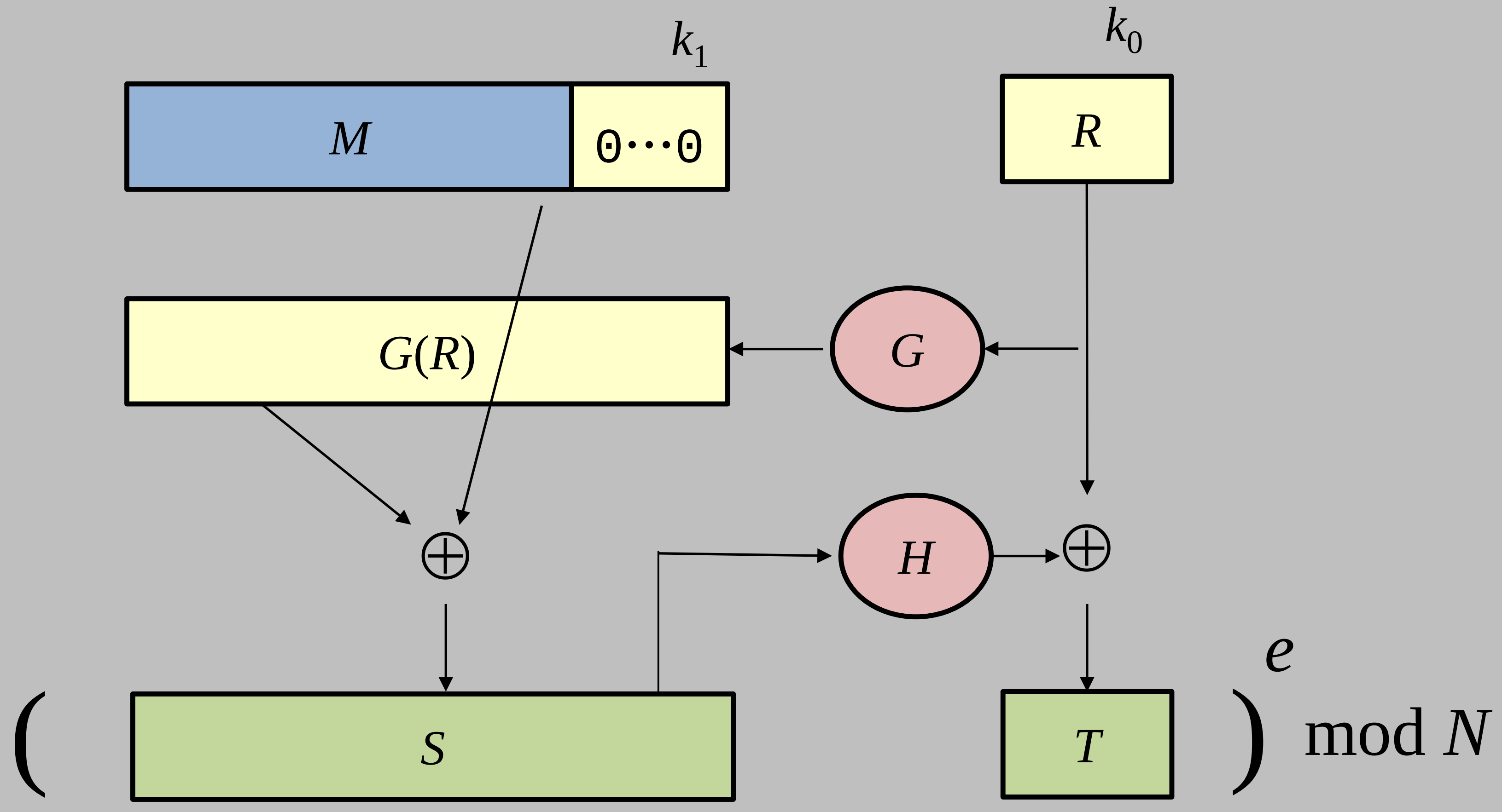
- Because it's deterministic.
- Because it won't achieve IND.
- Because the RSA assumption doesn't ensure that all of M is concealed by the applying the RSA function.

RSA PKCS #1, v. 1

$$\left(\boxed{00}\ \boxed{02}\ \boxed{\$\$ \cdots \$\$}\ \boxed{00}\ \boxed{\qquad\qquad M \qquad\qquad}\right)^{e} \bmod N$$

OAEP

[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.

$$\mathbf{Adv}^{\mathrm{ind}\,\mathrm{cca}\,\mathrm{rom}}_{\Pi}(A,k) = \Pr[H \twoheadleftarrow \Omega;\ (pk, sk) \twoheadleftarrow \mathcal{K}^{H}(k) : A^{\mathcal{E}^{H}_{pk}(\cdot),\ \mathcal{D}^{H}_{sk}(\cdot),\ H} \Rightarrow 1] -$$

$$\Pr[H \twoheadleftarrow \Omega;\ (pk, sk) \twoheadleftarrow \mathcal{K}^{H}(k) : A^{\mathcal{E}^{H}_{pk}(0^{|\cdot|}),\ \mathcal{D}^{H}_{sk}(\cdot),\ H} \Rightarrow 1]$$

RSA PKCS #1, v. 1