





RSA-OAEP	
Hash functions:	$G: \{0,1\}^{k_0} \to \{0,1\}^{k-k_0} \qquad H: \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$
Algorithm $((N,e),(N,p,q,d)) \stackrel{\$}{\leftarrow} \mathcal{B}$ Return $((N,e),(N,$	$\begin{array}{c c} n \mathcal{K} & \text{Algorithm} \mathcal{E}_{(N,e)}(M) \\ \begin{pmatrix} \zeta_{ssa}^* & r \stackrel{\$}{\leftarrow} \{0,1\}^{k_0} \\ d \end{pmatrix} & s \leftarrow M \  0^{k_1} \oplus G(r) \\ t \leftarrow r \oplus H(s) \\ C \leftarrow < s \  t >^e \mod N \\ \text{Return } C \end{array}$
	Algorithm $\mathcal{D}_{(N,d)}(C)$ $W \leftarrow C^d \mod N$ Parse $W$ as $s \mid  t$ $r \leftarrow H(s) \oplus t$ $M' \leftarrow s \oplus G(r)$ Parse $M'$ as $M \mid  z$ If $z = 0^{k_1}$ then return $M$ else return $\perp$

## Security of RSA-OAEP

- RSA-OAEP has not been proven IND-CCA secure.
- But it is proven IND-CCA secure assuming the RSA assumption, and when G,H are modeled as random oracles.
- Assuming the RSA problem is hard, RSA-OAEP is IND-CCA secure in the Random Oracle (RO) model.

## RO model

- The RO model assumes that all parties (adversary included) have oracle access to a truly random function.
- This is not true in reality. The model is ideal.
- In practice real hash functions such as SHA1 are used in place of random oracles.
- The belief is that security of the practical schemes holds in the standard model.
- However there are several examples of uninstantiable schemes (the schemes that are proven secure in the RO model but shown to be insecure for any instantiation of random oracles with a real function.)
- All currently known uninstantiable schemes are rather artificial.

6