Plain RSA encryption scheme

Algorithm $K_{\text{RSA}}^e$

\[
\ell_1 \leftarrow \lceil k/2 \rceil ; \ell_2 \leftarrow \lfloor k/2 \rfloor
\]
Repeat
\[
p \leftarrow \{ 2^{\ell_1-1}, \ldots, 2^{\ell_1} - 1 \}; \quad q \leftarrow \{ 2^{\ell_2-1}, \ldots, 2^{\ell_2} - 1 \}
\]
Until the following conditions are all true:
- TEST-PRIME($p$) = 1 and TEST-PRIME($q$) = 1
- $p \neq q$
- $2^{\ell_1-1} \leq p q$
\[
N \leftarrow p q
\]
Return $(N, p, q)$

Plain RSA is not secure

- Under the RSA assumption it is hard to recover a message given the public key and a ciphertext.

- \[
\begin{align*}
\text{easy} & \quad C = M^e \mod N \\
\text{easy with d} & \quad \text{hard without d}
\end{align*}
\]

- Nevertheless, the plain RSA is not a good encryption scheme.

- E.g. it is not IND-CPA secure. Why?

- One might try to add a random padding to a message before applying the RSA function, but as we saw it does not necessarily helps.

\[\text{RSA-OAEP}\]

Hash functions: \( G : \{0,1\}^{k_h} \rightarrow \{0,1\}^{k_h} \quad H : \{0,1\}^{k_h} \rightarrow \{0,1\}^{k_h} \)

Algorithm $K_{\text{RSA}}^e$

\[
(N, p, q) \leftarrow K_{\text{RSA}}^e \quad \Phi \leftarrow (p - 1)(q - 1) \quad e \leftarrow \mathbb{Z}_\Phi
\]
\[
d \leftarrow \text{MOD-INV}(e, \Phi)
\]
Return \((N, e), (N, p, q, d)\)

Output $M$ iff $z=0\ldots0$

\[G, H \text{ are hash functions}\]
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.