Plain RSA encryption scheme

Algorithm $\mathcal{K}^{\$}_{\text{mod}}$
$\ell_1 \leftarrow \lfloor k/2 \rfloor$; $\ell_2 \leftarrow \lceil k/2 \rceil$
Repeat
$p \xleftarrow{\$} \{2^{\ell_1 - 1}, \ldots, 2^{\ell_1} - 1\}$; $q \xleftarrow{\$} \{2^{\ell_2 - 1}, \ldots, 2^{\ell_2} - 1\}$
Until the following conditions are all true:
– TEST-PRIME$(p) = 1$ and TEST-PRIME$(q) = 1$
– $p \neq q$
– $2^{k-1} \leq pq$
$N \leftarrow pq$
Return (N, p, q)

Algorithm $\mathcal{K}^{\$}_{\text{rsa}}$
$(N, p, q) \xleftarrow{\$} \mathcal{K}^{\$}_{\text{mod}}$
$\phi \leftarrow (p-1)(q-1)$
$e \xleftarrow{\$} Z^*_{\phi}$
$d \leftarrow$ MOD–INV(e, ϕ)
Return $((N, e), (N, p, q, d))$

Algorithm $\mathcal{K}$
$((N,e),(N,p,q,d)) \xleftarrow{\$} \mathcal{K}^{\$}_{rsa}$
Return $((N,e),(N,d))$

Algorithm $\mathcal{E}_{(N,e)}(M)$
$C \leftarrow M^e \mod N$
Return C

Algorithm $\mathcal{D}_{(N,d)}(C)$
$M \leftarrow C^d \mod N$
Return M

Plain RSA is not secure

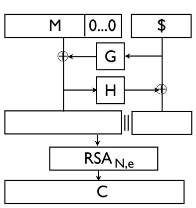
- Under the RSA assumption it is hard to recover a message given the public key and a ciphertext.

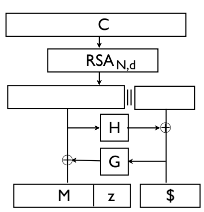
$$M \underset{\text{easy with d}}{\overset{\text{easy}}{\rightleftarrows}} C = M^e \bmod N$$

hard without d

- 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.

RSA-OAEP





Output M iff z=0...0

G,H are hash functions

RSA-OAEP

Hash functions: $G\colon \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$ $\quad H\colon \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$

Algorithm $\mathcal{K}$
$((N,e),(N,p,q,d)) \xleftarrow{\$} \mathcal{K}^{\$}_{rsa}$
Return $((N,e),(N,d))$

Algorithm $\mathcal{E}_{(N,e)}(M)$
$r \xleftarrow{\$} \{0,1\}^{k_0}$
$s \leftarrow M || 0^{k_1} \oplus G(r)$
$t \leftarrow r \oplus H(s)$
$C \leftarrow \langle s || t \rangle^e \mod N$
Return C

Algorithm $\mathcal{D}_{(N,d)}(C)$
$W \leftarrow C^d \mod N$
Parse W as $s||t$
$r \leftarrow H(s) \oplus t$
$M' \leftarrow s \oplus G(r)$
Parse M' as $M||z$
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.