Quiz #3: Asymmetric Encryption and Message Deduction

Consider the following equational theory for RSA. Let $N = p \cdot q$ with p and q large primes, consider the following two symbols: $\mathsf{pair}(x, y), \mathsf{fst}(x), \mathsf{snd}(x)$ represent message concatenation and first/second projection, $\mathsf{inv}(x)$ represents the inverse of x modulo $\phi(N)$, and $\mathsf{exp}(x, y)$ represents modular exponentiation of x with y (modulo N). Let E_{RSA} be defined by the following equations:

$$\mathsf{exp}(\mathsf{exp}(x, y), \mathsf{inv}(y)) = x \qquad \mathsf{exp}(\mathsf{exp}(x, y), z) = \mathsf{exp}(\mathsf{exp}(x, z), y)$$
$$\mathsf{fst}(\mathsf{pair}(x, y)) = x \qquad \mathsf{snd}(\mathsf{pair}(x, y)) = y$$

Question 1. Is this a subterm convergent equational theory? Argue why either way. Quoting the book:

> "A *convergent theory* is an equational theory induced by a convergent rewriting system. The theory is *subterm convergent* if there is a corresponding (convergent) rewriting system such that any rewrite rule $l \to r$ is such that r is a subterm of l or a constant."

Question 2. Define a message deduction problem $S \vdash_{E_{RSA}} y$ that resembles the RSA experiment in page 312 of the "Introduction to Modern Cryptography" book:

> **The RSA experiment $\mathsf{RSA\text{-}inv}_{\mathcal{A},\mathsf{GenRSA}}(n)$:**
>
> 1. *Run* $\mathsf{GenRSA}(1^n)$ *to obtain* (N, e, d).
> 2. *Choose a uniform* $y \in \mathbb{Z}_N^*$.
> 3. $\mathcal{A}$ *is given* $N, e, y,$ *and outputs* $x \in \mathbb{Z}_N^*$.
> 4. *The output of the experiment is defined to be* 1 *if* $x^e = y \bmod N$, *and* 0 *otherwise.*

> ***DEFINITION 8.46*** The RSA problem is hard relative to GenRSA *if for all probabilistic polynomial-time algorithms* $\mathcal{A}$ *there exists a negligible function* negl *such that* $\Pr[\mathsf{RSA\text{-}inv}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1] \leq \mathsf{negl}(n)$.

That is, choose the right set of messages S to give to the attacker in such a way that it cannot deduce the secret x. In particular, choose appropriate terms to represent the public and private key pair (e, d), and the encrypted message y in such a way that the attacker *cannot* deduce x, but such that anyone in possession of the private key can deduce x.

Question 3. Consider the following two frames:

$$\varphi_1 = \nu n, k\{\mathsf{inv}(k)/x, \mathsf{exp}(\mathsf{pair}(n, s), k)/y\} \qquad \varphi_2 = \nu n, k\{\mathsf{inv}(k)/x, \mathsf{exp}(n, k)/y\}$$

These two frames are not statically equivalent under the equational theory E_{RSA}. Show how to construct two terms M, N such that $(M =_{E_{RSA}} N)_{\varphi_1}$ but $(M \neq_{E_{RSA}} N)_{\varphi_2}$, or viceversa.