Exercises Submission
Automated Analysis of Security Protocols

Elia Scandaletti - 2087934

June 15, 2023

Exercise 1

1. The following tree solves the deduction

$sk_A, sk_B, \mathtt{aenc}(n_A, \mathtt{pk}(sk_B)), \mathtt{senc}(\mathtt{aenc}(n_B, \mathtt{pk}(sk_A)), n_A), \mathtt{senc}(s, \langle n_A, n_B\rangle) \vdash_{\mathcal{I}_{DY}} s$

$$\dfrac{\mathtt{senc}(s,\langle n_A,n_B\rangle) \qquad \dfrac{\dfrac{\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)) \quad sk_B}{n_A} \qquad \dfrac{\dfrac{\mathtt{senc}(\mathtt{aenc}(n_B,\mathtt{pk}(sk_A)),n_A) \quad \dfrac{\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)) \quad sk_B}{n_A}}{\mathtt{aenc}(n_B,\mathtt{pk}(sk_A))} \quad sk_A}{n_B}}{\langle n_A,n_B\rangle}}{s}$$

2. $\mathcal{I}_{DY}$ is called a local theory because, by definition of local theory, for any finite set of terms S, for any term t such that $S \vdash_{\mathcal{I}_{DY}} t$, there exist a proof tree Π of $S \vdash_{\mathcal{I}_{DY}} t$ such that every label in Π is in $\mathtt{st}(S) \cup \{t\}$.

This property of the $\mathcal{I}_{DY}$ inference system can be proven by induction on the size of Π.

$\mathcal{I}_{DY}$ being a local theory implies that for any S, for any t, $S \vdash_{\mathcal{I}_{DY}} t$ is decidable in polynomial time.

Exercise 2

1. The following tree solves the deduction

$sk_A, sk_B, \mathtt{aenc}(n_A, \mathtt{pk}(sk_B)), \mathtt{senc}(\mathtt{aenc}(n_B, \mathtt{pk}(sk_A)), n_A), \mathtt{senc}(s, \langle n_A, n_B\rangle) \vdash_{E_{enc}} s$

$$\dfrac{\dfrac{\mathtt{senc}(s,\langle n_A,n_B\rangle) \qquad \dfrac{\dfrac{\dfrac{\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)) \quad sk_B}{\mathtt{adec}(\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)),sk_B)}}{n_A} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\mathtt{senc}(\mathtt{aenc}(n_B,\mathtt{pk}(sk_A)),n_A) \quad \dfrac{\dfrac{\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)) \quad sk_B}{\mathtt{adec}(\mathtt{aenc}(n_A,\mathtt{pk}(sk_B)),sk_B)}}{n_A}}{\mathtt{sdec}(\mathtt{senc}(\mathtt{aenc}(n_B,\mathtt{pk}(sk_A)),n_A),n_A)}}{\mathtt{aenc}(n_B,\mathtt{pk}(sk_A))} \quad sk_A}{\mathtt{adec}(\mathtt{aenc}(n_B,\mathtt{pk}(sk_A)),sk_A)}}{n_B}}{\langle n_A,n_B\rangle}}{\mathtt{sdec}(\mathtt{senc}(s,\langle n_A,n_B\rangle),\langle n_A,n_B\rangle)}}{s}$$

Exercise 3

1. Let $M = \mathtt{h}(y)$ and $N = x$. Then we have $(M \neq_{E_{enc}} N)_{\varphi_1}$ and $(M =_{E_{enc}} N)_{\varphi_2}$.

2. φ_1 and φ_2 are statically equivalent because their only "difference" is hidden behind an asymmetric encryption of which the private key is not known.