

Messages et déduction

x, y, z, \dots sont des variables

a, b, c, \dots sont des constantes (symbole de fonction d'arité 0)

pair et enc sont des symboles de fonction d'arité 2.

On pourra noter $\{m\}_k$ au lieu de $\text{enc}(m, k)$ et $\langle m_1, m_2 \rangle$ au lieu de $\text{pair}(m_1, m_2)$.

Exercice 1

On considère

$$S = \{\{k_2\}_{\langle k_1, \{k_1\}_{k_3} \rangle}, \langle k_1, k_1 \rangle, \{\{k_1\}_{k_3}\}_{k_1}\}.$$

1. Donner l'ensemble des sous-termes de S .
2. Montrer que k_1 et k_2 sont dérivables à partir de S .
3. Montrer que k_3 n'est pas dérivable à partir de S .

Exercice 2

On propose une autre procédure pour décider si, étant donné un ensemble de termes $S = \{t_1, \dots, t_n\}$ et un terme t , t est dérivable à partir de S , à l'aide du système \mathcal{I}_{DY} .

1. Décomposer le plus possible les termes t_1, \dots, t_n : calculer le point fixe par déchiffrement et projection.
2. Essayer de construire t à partir des termes obtenus à la première étape et des règles de chiffrement et déchiffrement.

Pourquoi cette procédure n'est pas correcte ? Quelles hypothèses faudrait-il ajouter ?