Travaux Dirigés de LOGIQUE

STI 3ème année

Document supplémentaire : Logique des prédicats

Éléments de Correction

P. Clemente

1 Problème de cryptographie

1.1 Résolution 'à la main'

On se place dans le contexte de messages échangés entre des personnes, cryptés (ou chiffrés) et décryptés (ou déchiffrés) à l'aide d'une même clé de cryptage. Chaque clé est liée à une personne.
On considère l'ensemble des descriptions suivantes (ou axiomes) :

1. *Tous les messages qu'envoie Alice sont des messages chiffrés.*
2. *Alice ne partage sa clé de chiffrement/déchiffrement qu'avec tous ses amis.*
3. Ne pas oublier que *Ami* est une relation réflexive...
4. *Quelqu'un comprend un message chiffré si celui qu'il l'a chiffré partage sa clé avec lui.*
5. *Bob a compris un message envoyé par Alice.*

A partir de cet ensemble d'axiomes, le but de l'exercice va être de déterminer si la conclusion suivante est universellement valide ou pas :

6. *Bob est un ami d'Alice.*

Derrière le travail se cache le fait qu'un problème de modélisation dans un protocole peut conduire à des vulnérabilités importantes. Ici, le résultat est qu'on va croire que quelqu'un qui a réussi

Question 1. Donner la structure du langage $\mathcal{L}$ que l'on considère pour traiter ce problème. Préciser en particulier les constantes, les fonctions et les prédicats, et leur nombre d'arguments.

Aide : l'univers de base est constitué de personnes, messages et clés de chiffrement/déchiffrement.

Correction 1. *Le langage $\mathcal{L}$ est constitué éléments suivants :*

- *constantes :* $\{a, b\}$;
- *fonctions :* $\{cle(px)\}$;
- *prédicats :* $\{Partage(p_x, k_y, p_z), Envoi(p_x, m_y, p_z), Comprend(p_x, m_y), Chiffre(m_x, k_y), Ami(p_x, p_y)\}$.

Question 2. Donner l'interprétation de chaque élément non standard de la logique des prédicats décrit dans votre langage. Par exemples :

- La constante 'c_{p_a}' s'interprète par *Alice*.
- Le prédicat '$Envoi(c_{p_a}, m_1, p_x)$' s'interprète par c_{p_a} envoie un message m_1 à la personne p_x.

Correction 2. *Interprétation proposée des éléments de $\mathcal{L}$:*

- *constantes :* c_{p_a}, c_{p_b}, m_1 *s'interprètent respectivement comme Alice, Bob et un message donné.*
- *fonctions :* $cle(p_x)$ *s'interprète comme une fonction retournant la clé de chiffrement de la personne* p_x.
- *prédicats :*
  - $Partage(p_x, k_y, p_z)$ *: s'interprète comme* p_x *Partage la clé* k_y *avec* p_z.
  - $Envoi(p_x, m_y, p_z)$ *: s'interprète comme* p_x *Envoie le message* m_y *à* p_z.

- $Comprend(p_x, m_y)$: *s'interprète comme* p_x *Comprend le message* m_y.
- $Chiffre(m_x, k_y)$: *s'interprète comme le message* m_x *est Chiffré avec la clé* k_y.
- $Ami(p_x, p_y)$: *s'interprète comme* p_x *est Ami avec* p_y.

Question 3. Formaliser l'ensemble des hypothèses et la conclusion précédents en **logique des prédicats**.

Correction 3.

(1) $\forall p_x \forall m \forall p_y (Envoi(c_{p_a}, m, p_y) \Rightarrow Chiffre(m, cle(c_{p_a})))$

(2) $\forall p_x (Partage(c_{p_a}, cle(c_{p_a}), p_x) \Leftrightarrow Ami(c_{p_a}, p_x))$

(3) $\forall p_x \forall p_y (Ami(p_x, p_y) \Leftrightarrow Ami(p_y, p_x))$

(4) $\forall p_x \forall p_y \forall m (Comprend(p_x, m) \wedge Chiffre(m, cle(p_y)) \Rightarrow Partage(p_y, cle(p_y), p_x))$
ou encore (équivalent) :
$\forall p_x \forall p_y \forall m (Chiffre(m, cle(p_y)) \Rightarrow (Comprend(p_x, m) \Rightarrow Partage(p_y, cle(p_y), p_x)))$

(5) Attention : le message n'a pas forcément été envoyé à Bob qui aurait pu l'intercepter :
$\exists p_x \exists m (Envoi(c_{p_a}, m, p_x) \wedge Comprend(c_{p_b}, m))$

(6) $Ami(c_{p_b}, c_{p_a})$

Question 4. Mettre sous forme prénexe, puis de skolem, puis clausale les axiomes et la conclusion précédents. Donner l'univers de Herbrand associé.

Correction 4.

Je donne directement la formes clausales (mais pour y arriver il faut d'abord donner les prénexes puis skolem...).

1. *On a donc l'ensemble* C *de formes clausales suivant :*
   (1) 1 clause : $\neg Envoi(c_{p_a}, m_1, p_{y_1}) \vee Chiffre(m_1, cle(c_{p_a}))$
   (2) 2 clauses :
   $\neg Partage(c_{p_a}, cle(c_{p_a}), p_{x_1}) \vee Ami(c_{p_a}, p_{x_1}))$
   et
   $Partage(c_{p_a}, cle(c_{p_a}), p_{x_2}) \vee \neg Ami(c_{p_a}, p_{x_2}))$
   (3) 2 clauses :
   $\neg Ami(p_{x_3}, p_{y_2}) \vee Ami(p_{y_2}, p_{x_3})$
   et
   $\neg Ami(p_{y_3}, p_{x_4}) \vee Ami(p_{x_4}, p_{y_3})$
   (4) 1 clause : $\neg Comprend(p_{x_5}, m_2) \vee \neg Chiffre(m_2, cle(p_{y_4})) \vee Partage(p_{y_4}, cle(p_{y_4}), p_{x_5}))$
   (5) 2 clauses : $Envoi(c_{p_a}, c_{m_1}, c_{p_x})$ *et* $Comprend(c_{p_b}, c_{m_1})$
   (6) 1 clause : $Ami(c_{p_b}, c_{p_a})$
2. ***Univers de Herbrand*** *On a au final 4 constantes* $(c_{p_a}, c_{p_b}, c_{m_1}, c_{p_x})$*, une fonction* $(cle(p_x))$*, les variables étant* $(m_1, m_2, p_{x_1}, p_{x_2}, p_{x_3}, p_{x_4}, p_{x_5}, p_{y_1}, p_{y_2}, p_{y_3}, p_{y_4})$.
   L'univers de Herbrand est donc : $H_\infty = \{c_{p_a}, c_{p_b}, c_{m_1}, c_{p_x}, cle(c_{p_a}), cle(c_{p_b}), cle(c_{p_x})...\}$.

Question 5. Prouver que la conclusion est universellement valide par rapport à l'ensemble d'hypothèses donné.

Correction 5. *On va procéder avec une résolution par réfutation. On ajoute donc la négation de la conclusion à l'ensemble des hypothèses. On obtient ainsi l'ensemble* C_2 *composé des 8 premières clauses, plus la négation de la conclusion :*

num. de clause	*résolvante*	*source*
1.	$\neg Envoi(c_{p_a}, m_1, p_{y_1}) \vee Chiffre(m_1, cle(c_{p_a}))$	(1)
2.	$\neg Partage(c_{p_a}, cle(c_{p_a}), p_{x_1}) \vee Ami(c_{p_a}, p_{x_1}))$	(2)
3.	$Partage(c_{p_a}, cle(c_{p_a}), p_{x_2}) \vee \neg Ami(c_{p_a}, p_{x_2}))$	(2)
4.	$\neg Ami(p_{x_3}, p_{y_2}) \vee Ami(p_{y_2}, p_{x_3})$	(3)
5.	$\neg Ami(p_{y_3}, p_{x_4}) \vee Ami(p_{x_4}, p_{y_3})$	(3)
6.	$\neg Comprend(p_{x_5}, m_2) \vee \neg Chiffre(m_2, cle(p_{y_4})) \vee Partage(p_{y_4}, cle(p_{y_4}), p_{x_5}))$	(4)
7.	$Envoi(c_{p_a}, c_{m_1}, c_{p_x})$	(5)
8.	$Comprend(c_{p_b}, c_{m_1})$	(5)
9.	$\neg Ami(c_{p_b}, c_{p_a})$	($\neg$6)

La résolution par réfutation est la suivante, en 6 lignes :

no. clause	*résolvante*	*source*	*substitution*
10.	$Ami(c_{p_a}, p_{x_1}) \vee \neg Comprend(p_{x_1}, m_2) \vee \neg Chiffre(m_2, cle(c_{p_a}))$	2, 6	$\sigma_1 = \{p_{x_5}/p_{x_1}, p_{y_4}/c_{p_a}\}$
11.	$Ami(c_{p_a}, c_{p_b}) \vee \neg Chiffre(c_{m_1}, cle(c_{p_a}))$	10, 8	$\sigma_2 = \{p_{x_1}/c_{p_b}, m_2/c_{m_1}\}$
12.	$Ami(c_{p_a}, c_{p_b}) \vee \neg Envoi(c_{p_a}, c_{m_1}, p_{y_1}))$	1, 11	$\sigma_3 = \{m_1/c_{m_1}\}$
13.	$Ami(c_{p_a}, c_{p_b})$	12, 7	$\sigma_4 = \{c_{p_x}/cle(c_{p_a}), p_{y_1}/c_{p_x})\}$
14.	$Ami(c_{p_b}, c_{p_a})$	13, 4	$\sigma_5 = \{p_{x_3}/c_{p_a}, p_{y_2}/c_{p_b}\}$
15.	$\square$	14, 9	

On a obtenu la clause vide en 15.

On a utilisé les clauses initiales $1, 2, 4, 6, 7, 8, 9$ *avec les valuations suivantes :*

1. $\neg Envoi(c_{p_a}, c_{m_1}, cle(c_{p_a})) \vee Chiffre(c_{m_1}, cle(c_{p_a}))$

2. $\neg Partage(c_{p_a}, cle(c_{p_a}), c_{p_b}) \vee Ami(c_{p_a}, c_{p_b}))$

4. $\neg Ami(c_{p_a}, c_{p_b}) \vee Ami(c_{p_b}, c_{p_a})$

6. $\neg Comprend(c_{p_b}, c_{m_1}) \vee \neg Chiffre(c_{m_1}, cle(c_{p_a})) \vee Partage(c_{p_a}, cle(c_{p_a}), c_{p_b}))$

7. $Comprend(c_{p_b}, c_{m_1}))$

8. $Envoi(c_{p_a}, c_{m_1}, c_{p_x})$

Rappel du théorème de Herbrand : "Un ensemble C_2 *de clauses est insatisfiable ssi il existe un ensemble fini* C_2' *d'instances de base de clauses de* C_2 *insatisfiable."*

Donc, puisqu'on a trouvé un ensemble de clauses de base C_2' *(contenant les clauses* $1, 2, 4, 6, 7, 8, 9$*), l'ensemble des clauses* C_2 *(c-à-d les clauses* $1, 2, 3, 4, 5, 6, 7, 8, 9$*) est nécessairement insatisfiable aussi.*

Cela invalide donc la négation de la conclusion. La conclusion est donc universellement valide par rapport à l'ensemble des hypothèses.