

TD 1 05/02/2025

P_{fa1} P_{fr1}

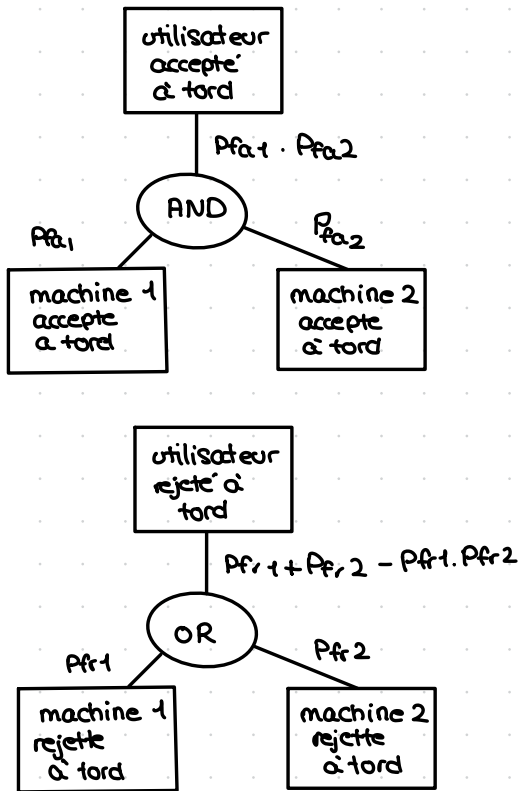
P_{fa2} P_{fr2}

politiques: 2 machines acceptent

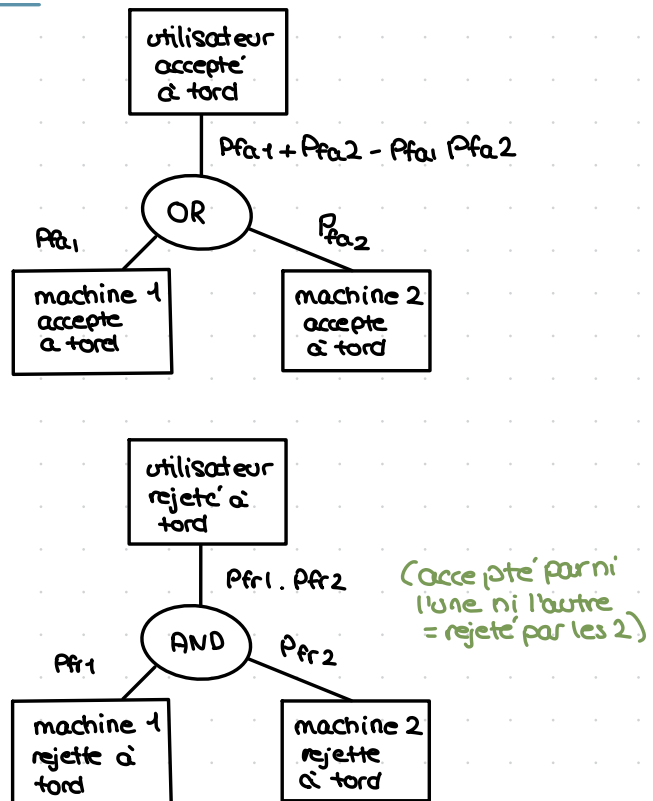
au moins une des deux machines accepte

1)

politique 1:



politique 2:



2) Appli numérique

$P_{fa1} = 0.1$ $P_{fr1} = 0.2$ $P_{fa2} = 0.3$ $P_{fr2} = 0.4$

politique 1: acceptation à tort: $0.1 \times 0.3 = 0.03$

rejet à tort: $0.2 + 0.4 - 0.2 \times 0.4 = 0.6 - 0.16 = 0.44$

politique 2: acceptation à tort: $0.1 + 0.3 - 0.1 \times 0.3 = 0.4 - 0.03 = 0.37$

rejet à tort: $0.2 \times 0.4 = 0.16$

3) Quelle politique conseiller?

politique 1: pour une zone très sensible (base militaire)

politique 2: améliore le confort d'accès (moins de refus): bibliothèque universitaire
(impact d'un faux rejet est plus critique)

Exo2:

1) nb de combinaisons par une attaque brute force

- 8 caractères minuscules: 26^8

- 8 caractères minuscules, sans répétition: $26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19 = A_{26}^8 = \frac{26!}{(26-8)!}$

- minuscules ou majuscules 5 1^{er}, chiffres 3 derniers: $(26 \cdot 2)^5 \cdot 10^3 = 52^5 \cdot 10^3$

- 7 caractères minuscules ou majuscules, 2 caractères spéciaux (15): $C_9^2 \cdot 52^7 \cdot 15^2$

↳ l'ordre compte

9 places où mettre

- les 2 caractères spéciaux

- 6 à 10 caractères composés uniquement de minuscules, majuscules, ou caractères spéciaux :

$$52 + 15 = 67$$

$$67^6 + 67^7 + 67^8 + 67^9 + 67^{10}$$

$$= \sum_{i=6}^{10} 67^i$$

- 8 caractères minuscules, majuscules ou caractères spéciaux, au plus 2

$$52^8 + 52^7 \cdot 15 \cdot C_8^1 + 52^6 + 15^2 \cdot C_8^2$$

$$\left(\sum_{s=0}^2 C_8^s \cdot 52^{8-s} \cdot 15^s \right) \quad \uparrow \text{ pour l'ordre des caractères spéciaux}$$

2) longueur $n \leq K$, pour $K=4, 6, 8$

- sans distinction majuscules / minuscules

$$K=4: \sum_{n=1}^4 26^n = 475\,254$$

$$K=6: \sum_{n=1}^6 26^n = 308\,915\,775$$

$$K=8: \sum_{n=1}^8 26^n = 217\,180\,147\,158$$

avec distinction majuscules / minuscules

$$K=4: \sum_{n=1}^4 52^n = 7,48 \text{ million}$$

$$K=6: \sum_{n=1}^6 52^n \approx 20 \text{ milliards}$$

$$K=8: \sum_{n=1}^8 52^n \approx$$

Formule générale: $\sum_{n=1}^K 26^n = \frac{26(26^K - 1)}{26 - 1}$

3) $n=6$, estimer le temps nécessaire si un essai prend 0.1s, 1 microseconde

52^6 possibilité

0.1s: $52^6 \times 0.1 \approx 1977 \cdot 10^9 \text{ secondes} \approx 2 \text{ milliards de secondes}, \frac{1.977 \times 10^9}{3.156 \times 10^7} \approx 62.6 \text{ ans}$

1ms: $T = 52^6 \times 10^{-6} \approx 1.977 \times 10^4$
 $\approx 5,5 \text{ heures}$

$\uparrow$ nb de secondes

4) système sensible à la casse, système sensible à la casse

$\rightarrow$ brute force: 26^n
soleil

$\rightarrow 52^n$
SOLEIL



trouver le mdp: $26^n + 2^n$

trouver maj/min

(SOLEIL)
↑
↑
↑
↑
↑
↑

borne: (attaque en 2 étapes): $26^n + 2^n$

5) intérêt + limites d'un questionnaire de mots de passe

mdp unique et long par service

Inconvénients: mdp maître est un point de défaillance

Exo3:

niveaux de sécurité: NC, C, S, TS

Catégories: OPINT, NUCL, R&D

$$L = \{NC, C, S, TS\} \quad P(\text{catégories}) = P(\{OPINT, NUCL, R\&D\})$$

$$(N, K) \sqsubseteq (N', K') \Leftrightarrow N \leq N', K \leq K' \quad ((N', K') \text{ domine } (N, K)) \quad e_1 \sqsubseteq e_2$$

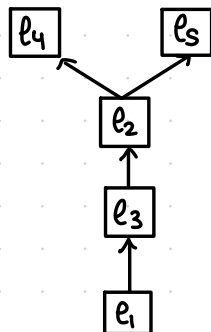
$\uparrow$
 e_1

* écrire vers le haut, lire vers le bas

labels: $e_1 = (C, \{OPINT\})$
 $e_2 = (S, \{OPINT, NUCL\})$
 $e_3 = (S, \{OPINT\})$
 $e_4 = (TS, \{OPINT, NUCL\})$,
 $e_5 = (S, \{OPINT, NUCL, R\&D\})$

1) ordre partiel:

$e_1 \subseteq e_3$
 $e_3 \subseteq e_2$
 $e_2 \subseteq e_5$
 $e_2 \subseteq e_4$



2) a) $\inf(e_1, e_2) = e_1$
 b) $\sup(e_3, e_5) = e_5$
 c) $\sup(e_2, e_5) = e_5$

Un **treillis** est un ensemble partiellement ordonné $(L, \leq)$ tel que, pour toute paire $(a, b) \in L \times L$, il existe :

- une **borne supérieure** (plus petit majorant), notée $a \oplus b$;
- une **borne inférieure** (plus grand minorant), notée $a \otimes b$.
- Un treillis possède un **plus grand élément** (majorant de tous), et un **plus petit élément** (minorant de tous), quand L est fini.

3) $Mq L \times PC$ Catégories est un treillis fini

$(TS, \{OPINT, R\&D, NUCL\}) \rightarrow \max$

$(NC, \{ \}) \rightarrow \min$

Ce treillis est 1 produit de 2 treillis fini donc c'est un treillis fini

$L \times P(C)$
 $\uparrow \{OPINT, R\&D, NUCL\} \rightarrow 3 \text{ els}$

$4 \cdot 2^3$ noeuds au total
 $\uparrow$ nb sous ensembles d'un ensemble à 3 éléments.

PARTIE B: No read up, No write Down

identifiant	Nom	Label de sécurité
U_1	Capitaine Thomas	$(\{S, \{OPINT, NUCL\}\})$
U_2	Colonel Nguyen	$(TS, \{OPINT\})$
U_3	Ingénieur Moreau	$(C, \{OPINT, NUCL, R\&D\})$

pas sa catégorie:
ni lire ni écrire

	D_1	D_2	D_3	D_4
U_1	L	E	-	L
U_2	L	-	L, E	L
U_3	L	E	-	-

identifiant	Label de sécurité
D_1	$(\{C, OPINT\})$
D_2	$(S, \{OPINT, NUCL, R\&D\})$
D_3	$(TS, \{OPINT\})$
D_4	$(S, \{OPINT\})$

$(S, L \subseteq L \cup$
 $S \subseteq TS$
 $\{NUCL\} \subseteq \{NUCL, R\&D\})$