IHDCM035 – Sécurité Informatique January 2025	First Name – LAST NAME	ID

Question 1: PRG Security

Soit le jeu d'attaque suivant utile à la définition d'un Secure PRG du cours:

Given PRG G over $(\mathcal{S}, \mathcal{R})$, where $\mathcal{S}$ defines the seed input space, and $\mathcal{R}$ defines a finite output space. And given an adversary $\mathcal{A}$, we have the following two experiments where the challenger computes r differently in each experiment:

1. $s \leftarrow\$ \mathcal{S}$, $r \leftarrow G(s)$. We note this experiment b=0;
2. $r \leftarrow\$ \mathcal{R}$. We note this experiment b=1.

and sends r to $\mathcal{A}$

Let W_b the event that $\mathcal{A}$ outputs 1 in Experiment b (i.e., $Pr[output = 1 | b = \{0,1\}]$). We define $\mathcal{A}$'s advantage in respect to G as:

$$PRGadv[\mathcal{A}, G] := |Pr[W_{b=0}] - Pr[W_{b=1}]|$$

1. Quelle condition(s) sur le jeu d'attaque est nécessaire pour obtenir un Secure PRG?

2. Soit $s \leftarrow\$ \{0,1\}^{128}$, $k_1 \leftarrow\$ \mathcal{K}$ avec $\mathcal{K}$ un grand ensemble. On définis un PRG $G : \{0,1\}^{128} \rightarrow \{0,1\}^{256}$ ainsi:

   $$G(s) := (t1, t2)$$

   où $t1 = k_1 \oplus s$ et $t2 = k_2 \oplus t1$, et k_2 est publique.

   G est-il est un Secure PRG? Justifiez.

IHDCM035 – Sécurité Informatique January 2025	First Name – LAST NAME	ID

IHDCM035 – Sécurité Informatique January 2025	First Name – LAST NAME	ID

Question 2: Intrusion Detection Systems

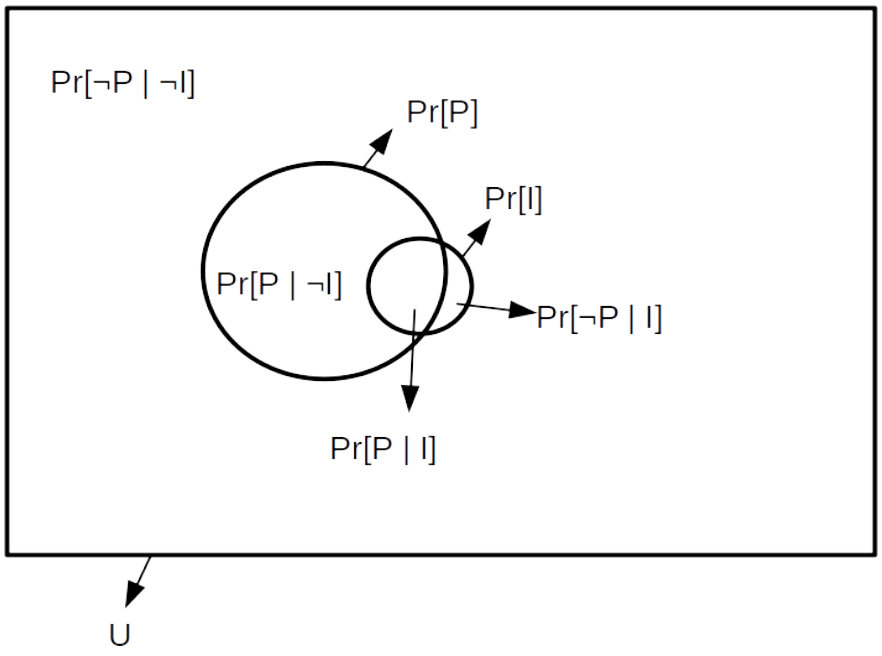
Supposez un IDS avec un $FPR = 0.01$ et un $FNR = 0.01$.

1. Quelle est la justesse (accuracy) de ce système IDS?

2. Expliquez le problème "base-rate fallacy", et discutez la garantie de sécurité de l'IDS en supposant une incidence de 1/100000 (on estime qu'une machine sur 100000 est infectée).

3. Expliquez comment évolue les garanties de sécurité de l'IDS si l'incidence augmente. La figure 2 peut vous aider.

Vous pourriez avoir besoin du schéma suivant et de théorème de Bayes pour répondre aux questions.



$$Pr[A|B] = \frac{Pr[B|A]Pr[A]}{Pr[B]}$$

where $Pr[B] = \sum_i Pr[B|A_i]Pr[A_i]$ from the law of total probability

IHDCM035 – Sécurité Informatique January 2025	First Name – LAST NAME	ID

Question 3: Software security 1.

Dessinez la stack frame de la fonction foo() et incluez toute information pertinente à l'execution de la fonction dans votre dessin.

```
1   static int foo(int a) {
2     int x;
3
4     x = a + 42;
5
6     return x;
7   }
8
9   int main(int argc, char *argv[]) {
10
11    return foo(0);
12  }
13
14
```