Zeste de savoir

Preuve de la sécurité du masque jetable de Vernam

12 août 2019

Table des matières

Pour comprendre ce qui suit, il est nécessaire d'avoir des connaissances de base en probabilités. Les notations sont explicitées au tout début, mais leurs sens ne sont pas expliqués : ils sont considérés connus.

> **!** Il est donc important de savoir digérer les maths. Si ce n'est pas votre cas, passez votre chemin, je préfère ne pas avoir de mort sur la conscience !

Il faut bien entendu également savoir ce qu'est le masque jetable de Vernam. Pour ce faire, je vous redirige vers un autre article, sur l'histoire de la cryptographie, qui vous expliquera en gros ce procédé. Le voici : C'est toute une histoire : la cryptographie - Partie 3/3 . N'hésitez pas à lire les deux articles qui précèdent pour avoir les éventuels prérequis sur cet article.

1. Rappels des prérequis et notations

Avant de réaliser la preuve, il me faut définir quelques notations que je vais utiliser dans la suite de cet article.

- Γ (ou n'importe quelle lettre grecque majuscule) est un événement. Sa probabilité est notée $p[\Gamma]$;
- la probabilité d'une événement est notée $p[\Gamma]$ tel que $0 \leq p[\Gamma] \leq 1$;
- Ω est un événement particulier car il représente l'*univers*. Sa probabilité est donc toujours totale. Donc $p[\Omega] = 1$;
- X est une variable aléatoire, X est l'ensemble des valeurs x que peut prendre X ;
- $p[X = x]$ représente la probabilité que la variable aléatoire X ait la valeur x tel que $x \in \mathrm{X}$;
- $p[X = x \,|\, Y = y]$ est la probabilité que l'on ait $X = x$ en sachant qu'on a $Y = y$ tel que $x \in \mathrm{X}, y \in \mathrm{Y}$.

Je dois également rappeler quelques propriétés qui ne seront démontrées ici.

- $p[X = x \,|\, Y = y] = \dfrac{p[Y = y \,|\, X = x] \times p[X = x]}{p[Y = y]}$, cette propriété est appelée loi de Baye ;
- $p[\Omega] = \sum_{x \in \mathrm{X}} p[X = x] = 1$, cette propriété est déduite des axiomes de Kolmogorov (version simplifiée et version complète) ;

— $p[X = x] = \sum_{y \in Y} p[X = x \,|\, Y = y] \times p[Y = y]$.

Une fois ceci fait, il ne me reste plus qu'à utiliser tout cela pour démontrer que le masque jetable est tout à fait fiable.

2. Sécurité ?

Je vais juste commencer par définir ce que l'on entend par sécurité. *À priori*, on pourrait commencer par sortir une définition comme celle-ci :

> Est sécurisée toute méthode ne permettant pas de retrouver le message original sans la clé.
>
> *Une personne quelconque*

Alors, il y a de l'idée, mais que se passe-t-il si quelqu'un arrive à déchiffrer **80%** de votre message ? Votre méthode est-elle toujours sécurisée ? Difficile à dire. Il faut donc peaufiner notre définition...

> Est sécurisée toute méthode ne permettant pas de retrouver une quelconque partie du message original sans la clé.
>
> *Une autre personne quelconque*

Effectivement, c'est déjà mieux. Si une personne arrive à retrouver ne fût-ce que **50%** du message original, c'est que notre méthode n'est pas sûre. Donc, cette définition dit que si quelqu'un arrive à deviner un caractère du message original, la méthode n'est pas sécurisée. Je vais donc vous proposer une autre définition. Et bien évidemment, je n'aurais pas pris la peine de vous faire un rappel sur les probabilités si je ne comptais pas les utiliser... Voici la définition :

> Soit m le *m*essage clair et c le message *c*hiffré, est sécurisée toute méthode telle que $\forall m \in \mathrm{M}, c \in \mathrm{C} : p[M = m \,|\, C = c] = P[M = m]$.
>
> *Pas de moi...*

Alors que veut dire cette définition ? Que l'on considère une méthode comme sécurisée **SI ET SEULEMENT SI** la probabilité que le message clair soit m en sachant que le message chiffré est c est égale à la probabilité que le message clair soit m. Autrement dit, une méthode est considérée comme sécurisée **SI ET SEULEMENT SI** le fait que le message crypté soit c n'a aucune influence probabiliste sur le fait que le message clair soit m.

C'est très bien, mais il nous faut maintenant le prouver !

3. Preuve

Nous partons d'un certain postulat de départ qui est que

$$\forall m \in \mathrm{M}, c \in \mathrm{C} : p[M = m \,|\, C = c] = P[M = m]$$

Si nous arrivons à cette égalité, alors on sait que la méthode du masque jetable est tout à fait sûre. Mais avant toute chose, il nous faut être bien sûr de ce que veut dire chaque symbole. Commençons par définir $\mathbb{E}$ comme étant l'ensemble des symboles disponibles pour faire un message. Définissons que L est la longueur du message. On peut en déduire que M, l'ensemble des messages possibles vaut $\mathbb{E}^L$. Ce qui veut dire que l'on prend L éléments de $\mathbb{E}$ et qu'on les aligne. Pour alléger la démonstration, je vais faire la supposition que m et c sont de même longueur et donc que si k (qui est la clé) a exactement la même longueur que c et m (ce qui est une propriété du masque jetable de Vernam). Je vais également supposer que le chiffrage d'un message m avec une clé k donnera toujours le même résultat et que toute tentative donnera un résultat tant que m et k respectent les contraintes imposées par $\mathbb{E}$. Donc $\exists c = \text{Cryptage}(m,k) \,|\, c,k,m \in \mathbb{E}^L$. Récapitulons...

$$\begin{aligned}
&\mathbb{E} = \{a,b,c,...,A,B,C,...,0,1,2,...\}\\
&L \in \mathbb{N}\\
&\mathrm{M} = \mathbb{E}^L\\
&m,c,k \in \mathrm{M}
\end{aligned}$$

Je vous propose d'appliquer la loi de Baye à notre membre de gauche :

$$p[M = m \,|\, C = c] = \frac{p[C = c \,|\, M = m] \times p[M = m]}{p[C = c]}$$

Vous vous dites que ça ne nous avance pas... Mais détrompez-vous. il nous faut certes toujours trouver plein de choses, voire plus, mais celles-ci, nous pouvons les trouver ! Commençons par trouver $p[C = c \,|\, M = m]$. Pour ce faire, je vais me servir de la supposition faite plus haut qui disait que j'aurai **toujours** un résultat **unique** pour chaque appel à $\text{Cryptage}(m,k)$. Je peux donc changer $p[C = c \,|\, M = m]$ en $p[K = k]$. Effectivement, sachant que l'on a $(M = m)$, $(K = k) \iff (C = c)$. Et la probabilité que K soit k peut être facilement calculée. Le masque jetable implique une clé aléatoire prise dans M. La clé étant aléatoire, chaque élément de $\mathbb{E}$ est équiprobable. Et on en a L. Il y a donc $\#\left(\mathbb{E}^L\right)$ clés possibles tel que $\#\mathbb{E}$ représente le nombre d'éléments de $\mathbb{E}$. On a donc $p[K = k] = \frac{1}{\#(\mathbb{E}^L)}$.

Notre formule évolue donc en la formule suivante :

$$p[M = m \,|\, C = c] = \frac{\frac{1}{\#\left(\mathbb{E}^L\right)} \times p[M = m]}{p[C = c]}$$

Mais attention, cette même probabilité que C soit égale à c est exactement la même que $p[K = k]$ car k et c sont du même ensemble $\mathbb{E}$ et de même longueur L. Ce qui nous donne donc la formule suivante :

$$p[M = m \,|\, C = c] = \frac{\frac{1}{\#\left(\mathbb{E}^L\right)} \times p[M = m]}{\frac{1}{\#\left(\mathbb{E}^L\right)}}$$

Et là, on a le même élément au numérateur et au dénominateur. On peut donc les simplifier, ce qui nous laisse avec la formule suivante :

$$p[M = m \,|\, C = c] = p[M = m]$$

Et l'on a retrouvé notre équation de départ ! CQFD !

Nous avons donc prouvé que le masque jetable de Vernam est effectivement une méthode infaillible (du moins selon notre définition de *sécurité*).