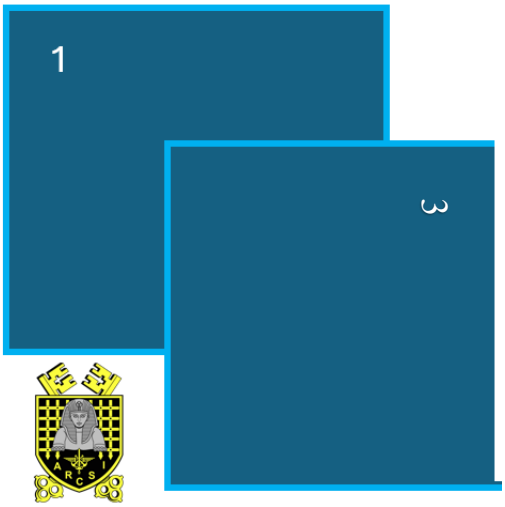
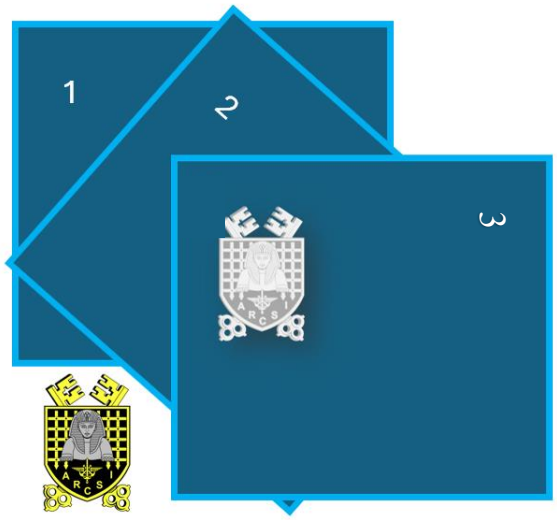
Introduction à la génération de clés aléatoires pour le chiffrement symétrique – version expert





Niveau de difficulté : lycée
Durée de l'activité : 5 minutes
Nombre de participants : 1 à 5 personnes
Public cible : 15 ans minimum et pour tout public
Coût estimé : Le prix de 3 écrans filtrants
Logistique : Mettre l'écran 2 à 45 degrés de l'écran 1 et l'écran 3 à 90 degrés de l'écran 1

MATÉRIEL NÉCESSAIRE

- 3 écrans filtrants

OBJECTIFS PÉDAGOGIQUES

• **Compétences développées :** Savoir qu'un photon a une probabilité de **cos^2 alpha** de passer à travers un écran filtrant dont les stries font un angle alpha avec l'axe du photon. Ceci peut être utilisé pour créer des clés secrètes aléatoires pour la cryptographie symétrique (comme l'AES).
• **Concepts abordés :** Production de nombres aléatoires en utilisant un cadran filtrant. Ceci est très utiles pour générer des clés symétriques secrètes.
• **Applications pratiques :** Avec 2 cadrans à 90 degrés, on ne voit plus ce qui est derrière le premier cadran. Si on insère un écran à 45 degrés entre les deux cadrans, un objet derrière les trois cadrans devient visible, mais altéré.

MODE D'EMPLOI

Étape de préparation et d'utilisation : Placer deux cadrans avec l'un à 90 degrés de l'autre. Un objet derrière les 2 cadrans n'est plus visible.
Placer le troisième cadran, entre les 2 cadrans, à 45 degrés du premier cadran, un objet derrière les 3 cadrans devient visible.

Méthode de chiffrement : Il s'agit de créer des clés secrètes symétrique parfaitement aléatoires.

SCÉNARIO D'ANIMATION

Introduction (5 min)

Expliquer que la probabilité qu'a un photon de traverser un cadran filtrant est égale à **$\cos^2$ alpha**, alpha étant l'angle que fait les stries du cadran filtrant avec l'axe du photon.
$\cos^2$ 45 degrés = ½ (racine de 2 sur 2 au carré). Donc une chance sur 2 de passer ou de ne pas passer.
Cette propriété peut être exploitée en mettant deux capteurs (un devant le cadran, qui produit un bit à zéro si le photon ne passe pas, et un qui produit un bit à un si le photon passe. On alimente ainsi une pile de bits à 0 ou à 1, qui se remplit quand on envoie une série de photos un ou un sur le cadran (256 bits pour l'AES256).

• **Accroche pour présenter l'activité :** Dire que cela sert à générer des nombres purement aléatoires, ce que les algorithmes actuels de créations de nombres aléatoires ne savent pas vraiment faire, car dans des grandes séries produites, les nombres des séquences peuvent se répéter.
• **Éléments de langage pour introduire le concept :** Trigonométrie et statistiques.

Démonstration (5 min)

• Instructions pour présenter l'outil : On manipule les 3 cadrans.

Conclusion (5 min)

• Générer des clés de chiffrement secrètes symétrique est une des deux actions possibles pour le chiffrement quantique, l'autre étant la diffusion de la clé par intrication quantique.
• Lien avec la cybersécurité moderne : Production de clés secrètes aléatoires.

CONSEILS POUR L'ANIMATEUR

• **Difficultés fréquemment rencontrées :** Perdre un des cadrans, l'aspect magique qui occulte l'aspect technique.
• **Astuces pour faciliter l'animation :** Très facile, pas besoin d'astuce.
• **Adaptations possibles selon le public :** Convient aux jeunes, ayant des notions de trigonométrie.

Un photon arrivant sur le cadran 1, passe si son axe est à 0 degré des stries du cadran 1. Il aborde le cadran 2 (incliné à 45 degrés par rapport au cadran 1, donc une chance sur deux de passer et il a maintenant (s'il est passé) un angle de 45 degrés par rapport au cadran 3 (incliné à 90 degrés par rapport au cadran 1, donc à 45 degrés par rapport à l'axe du photon. Il a donc encore une chance sur

deux de passer, donc par rapport au cadran 1, une chance sur quatre.

Avec deux cadrans inclinés à 90 degrés l'un de l'autre, le photon n'aurait aucune chance de passer.

Voir en : https://www.unige.ch/actualites/archives/2004/nombres-aleatoires-sur-demande/#:~:text=L'Universit%C3%A9%20de%20Gen%C3%A8ve%20et,%3A%20www.randomnumbers.info.

Introduction à la génération de clés aléatoires avec des filtres – Version simplifiée

Niveau : collège / début lycée
Durée : 5 minutes
Nombre de participants : 1 à 5
Public : dès 10 ans
Coût : prix de 3 filtres
Installation : poser le filtre 2 à 45° du filtre 1 et le filtre 3 à 90° du filtre 1

MATERIEL NECESSAIRE

- 3 filtres transparents ou écrans filtrants

OBJECTIFS

Ce que l'on apprend :

- Un photon (un petit rayon de lumière) peut passer à travers un filtre selon l'angle des stries sur le filtre.
- Cette propriété permet de créer des **clés secrètes aléatoires** pour protéger des messages (comme un coffre-fort numérique).
- Avec trois filtres placés différemment, on peut rendre un objet derrière eux visible ou invisible, selon l'angle des filtres.

MODE D'EMPLOI

---

1. Placer **le filtre 1 et le filtre 3** à 90° l'un de l'autre. L'objet derrière devient **invisible**.
2. Placer le **filtre 2 entre les deux**, à 45° du filtre 1. L'objet derrière les trois filtres devient **visible**, mais légèrement modifié.

But : générer une **clé secrète aléatoire** pour protéger des informations.

SCENARIO DE L'ANIMATION

Introduction (5 min)

- Expliquer que la lumière a une **chance de passer** à travers un filtre selon l'angle.
- Exemple : un filtre à 45° laisse passer la lumière **une fois sur deux**.

- On peut utiliser cela pour créer des **0 et des 1**, comme dans un code secret.
- En envoyant beaucoup de photons, on remplit une **suite de 256 bits**, qui peut devenir une clé pour protéger des messages.

Accroche : c'est comme fabriquer des nombres vraiment aléatoires, que les ordinateurs ne peuvent pas créer parfaitement.

Démonstration (5 min)

- Manipuler les **trois filtres** et montrer comment l'objet devient visible ou invisible.
- Observer comment les angles changent les chances que la lumière passe.

Conclusion (5 min)

- Créer des **clés secrètes aléatoires** est utile pour le **chiffrement quantique**, c'est-à-dire protéger des informations très importantes.
- Ces clés sont utilisées en **cybersécurité moderne**.

CONSEILS POUR L'ANIMATEUR

- **Difficultés fréquentes :** perdre un filtre, ou se concentrer sur la "magie" plutôt que la science.
- **Astuce :** facile à faire, pas besoin de préparation compliquée.
- **Adaptation :** convient aux enfants avec un peu de mathématiques (angles, probabilités simples).

Exemple visuel simple

- Un photon arrive sur le **filtre 1** (0°) → passe.
- Filtre 2 à 45° → passe **1 fois sur 2**.
- Filtre 3 à 90° → passe encore **1 fois sur 2**.

Probabilité totale de passer : $1/2 \times 1/2 = 1/4$.

- Avec **deux filtres à 90°**, la lumière ne passerait **jamais**.

Source : Université de Genève – Nombres aléatoires sur demande
https://www.unige.ch/actualites/archives/2004/nombres-aleatoires-sur-demande