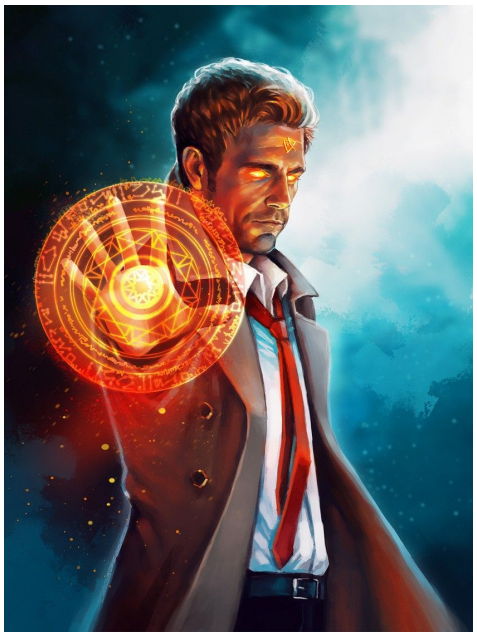
Magic Security

Éric BERTHOMIER
eric.berthomier@free.fr

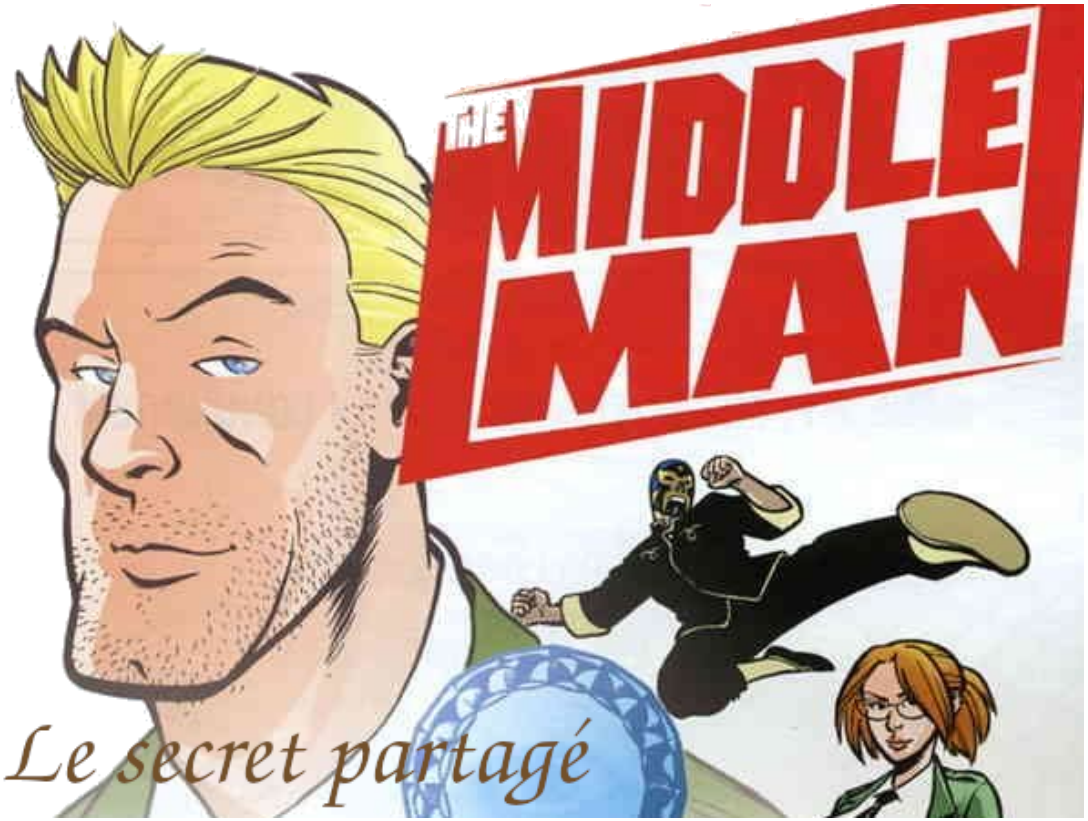
16 mars 2022



Version 1.0 - Version Stagiaire

Comment échanger un secret ?

Alice souhaite chiffrer un message à envoyer à Bob mais elle sait que Bruce les espionne ...



Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.
4. Mélanger les couleurs (partagée + secrète) chacun de votre côté.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.
4. Mélanger les couleurs (partagée + secrète) chacun de votre côté.
5. Prendre un papier et y indiquer la couleur obtenue.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.
4. Mélanger les couleurs (partagée + secrète) chacun de votre côté.
5. Prendre un papier et y indiquer la couleur obtenue.
6. Donner le papier à son binôme.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.
4. Mélanger les couleurs (partagée + secrète) chacun de votre côté.
5. Prendre un papier et y indiquer la couleur obtenue.
6. Donner le papier à son binôme.

Algorithme (1/3)

1. Se mettre par groupe de 2 (Alice et Bob).
2. Se mettre d'accord sur une couleur primaire commune.
3. Choisir chacun de son côté une couleur primaire secrète.
4. Mélanger les couleurs (partagée + secrète) chacun de votre côté.
5. Prendre un papier et y indiquer la couleur obtenue.
6. Donner le papier à son binôme.

	Alice	Bob
Couleur partagée		
Couleur secrète		
Couleur mélangée		

Algorithme (2/3) - Spy

Votre voisin est en fait un espion à la charge des lézards et a donc connaissance de la couleur que vous avez partagée.

Algorithme (2/3) - Spy

Votre voisin est en fait un espion à la charge des lézards et a donc connaissance de la couleur que vous avez partagée.
Donnez la couleur partagée à votre voisin sur un papier . . .

Algorithme (3/3) - Secret partagé

1. Mélanger la couleur de votre binôme à votre couleur secrète

	Alice	Bob
Couleur reçue du binôme		
Couleur secrète		
Couleur mélangée (Secret)		

Algorithme (3/3) - Secret partagé

1. Mélanger la couleur de votre binôme à votre couleur secrète

	Alice	Bob
Couleur reçue du binôme		
Couleur secrète		
Couleur mélangée (Secret)		

2. Demander à votre voisin Lézard de deviner votre secret partagé. . .

Démonstration

	Alice	Bob
Nombre partagé	A	A
Nombre secret	α	β
Somme	$A+\alpha$	$A+\beta$
Valeur reçue du binôme	$A+\beta$	$A+\alpha$
Nombre secret	α	β
Somme partagée (Secret)	$A+\beta+\alpha$	$A+\alpha+\beta$
Commutativité de l'addition	$A+\alpha+\beta$	$A+\alpha+\beta$

Rappel Mathématique : Modulo

Définition

- **La division euclidienne** ou division entière est une procédure de calcul qui, à deux entiers naturels appelés dividende et diviseur, associe deux autres entiers appelés quotient (quotient euclidien s'il y a ambiguïté) et reste.
- En informatique, le **modulo** est une opération qui au couple (a, b) d'entiers, associe le reste r de la division euclidienne de a par b.

5 6	2 3
1 0	2

5 1 5	2 3
5 5	2 2
9	

6 9 3 7 3	3 3
3 3	2 1 0 2
0 7 3	
7	

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6
3. Elle envoie à Bob la valeur $A = g^a \mod p = 56 \mod 23 = 8$

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6
3. Elle envoie à Bob la valeur $A = g^a \mod p = 56 \mod 23 = 8$
4. Bob choisit à son tour un nombre secret b=15

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6
3. Elle envoie à Bob la valeur $A = g^a \mod p = 56 \mod 23 = 8$
4. Bob choisit à son tour un nombre secret b=15
5. Bob envoie à Alice la valeur $B = g^b \mod p = 515 \mod 23 = 19$

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6
3. Elle envoie à Bob la valeur $A = g^a \mod p = 56 \mod 23 = 8$
4. Bob choisit à son tour un nombre secret b=15
5. Bob envoie à Alice la valeur $B = g^b \mod p = 515 \mod 23 = 19$
6. Alice peut maintenant calculer la clé secrète : $B^a \mod p = 196 \mod 23 = 2$

IRL : Diffie Hellman

Source : Wikipedia

1. Alice et Bob ont choisi un nombre premier p et une base g. Dans notre exemple, p=23 et g=5
2. Alice choisit un nombre secret a=6
3. Elle envoie à Bob la valeur $A = g^a \mod p = 56 \mod 23 = 8$
4. Bob choisit à son tour un nombre secret b=15
5. Bob envoie à Alice la valeur $B = g^b \mod p = 515 \mod 23 = 19$
6. Alice peut maintenant calculer la clé secrète : $B^a \mod p = 196 \mod 23 = 2$
7. Bob fait de même et obtient la même clé qu'Alice : $A^b \mod p = 815 \mod 23 = 2$

Magique . . .