MATH.en.JEAN

Le Protocole Russe

Auteur : Théo Audurier et Corto Garnier, Lycée Léonce Vieljeux, La Rochelle
Professeur encadrant le projet : Mr Vederine, Lycée Léonce Vieljeux, La Rochelle
Sujet : Mr.Lefloch, université de La Rochelle

Le sujet “Protocole Russe” est composé de trois questions:
La question 1 :
D’un paquet de 7 cartes numérotées 0,1,2,3,4,5,6 Alice & Bob reçoivent chacun 3 cartes et Charlie reçoit la carte restante. Comment Alice et Bob peuvent-ils s’informer mutuellement et ouvertement sur leurs cartes respectives sans que Charlie ne puisse connaître aucune des cartes qu’ils possèdent ?

La question 2 :
On modifie légèrement le problème initial: Charlie peut trouver certaines cartes possédées par Alice & Bob, mais pas toutes.

La question 3 :
Cette fois-ci on dispose de 13 cartes numérotées de 0,1,2,3,4,5,6,7,8,9,A,B,C. Alice, Bob et Charlie reçoivent respectivement 4,7 & 2 cartes. Comment Alice peut-elle informer ouvertement Bob sur ses cartes sans que Charlie puisse connaître la moindre de ses cartes ?

version 1
contributeur : Corto Garnier

La version 1 de cette article ne répond cas la question 1. Cette question développe presque toute les solutions qui permettent de résoudre les trois questions.

La question 1 :

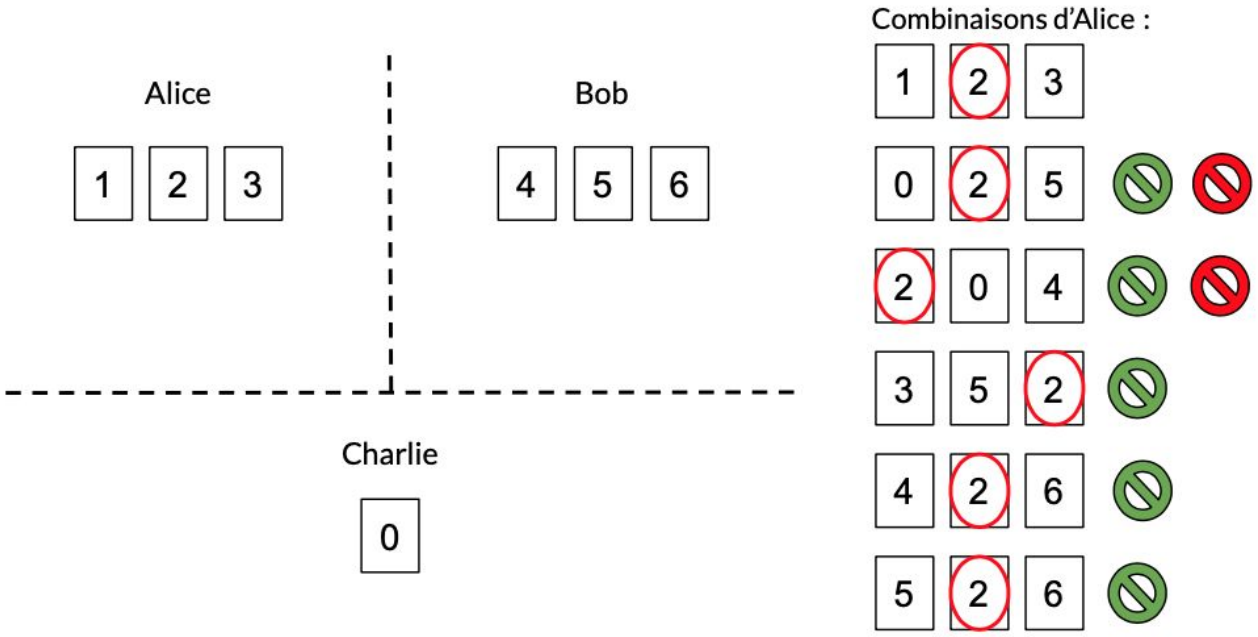
Première solutions : Les combinaison de carte

Le principe des combinaison de carte est qu’Alice forment diverse combinaisons de 3 cartes auxquelles elle ajoute sa véritable mains. Elle déclare, après avoir cité toute les combinaison qu’elle a créé, que l’une de ces combinaison correspond à sa main. Bob va alors éliminé les combinaison où apparaissent ses cartes et va découvrirent les cartes d’Alice. Ce dernier va alors dévoiler la carte de Charlie afin qu’Alice déduise ses cartes.

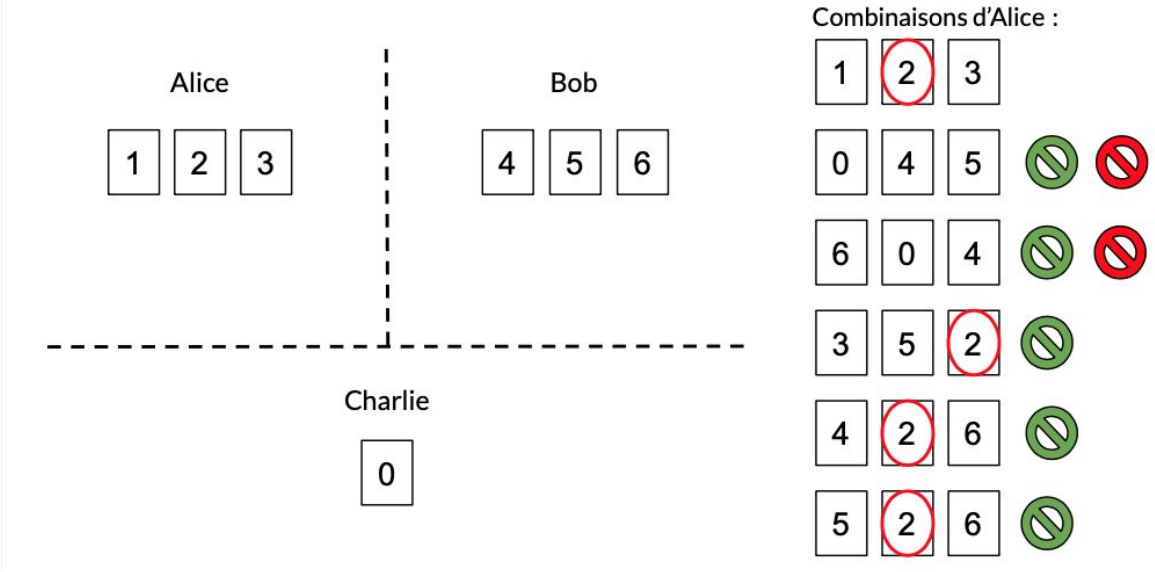
Pour que cette technique fonctionne, il faut suivre certaine règle au niveaux de la création des combinaisons, ces règle si elle ne sont pas suivit permette à Charlie de deviner les cartes d’Alice, ou tout du moins une de ses cartes.

Règle 1:

Il ne faut pas qu'un chiffre couvre toute les combinaisons, ou qu'un chiffre apparaissent trop souvent.
exemple :



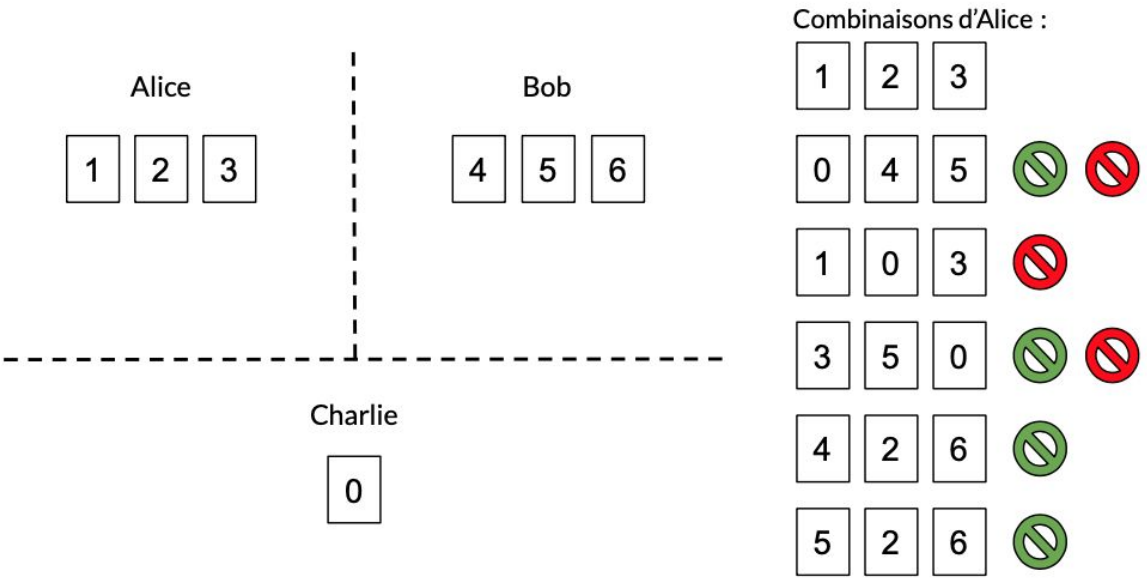
Ici Charlie ne peut éliminer que deux des combinaisons d'Alice, Bob lui peut par contre éliminé toute les fausse combinaison les cartes d'Alice. Mais Charlie sait qu'Alice à le deux car il est dans toute les combinaisons.
exemple:



Ici Charlie est sur qu'Alice a le 2 car il se trouvent dans toute les combinaisons qu'il n'a pas éliminé.

Règle 2 :
Il ne faut pas qu'Alice place un nombre plus de 3 fois dans les combinaison.

Règle 3 :
Il ne faut pas qu'Alice place deux cartes qu'elle possède dans la même combinaison (sauf dans la véritable combinaison de carte).
exemple :



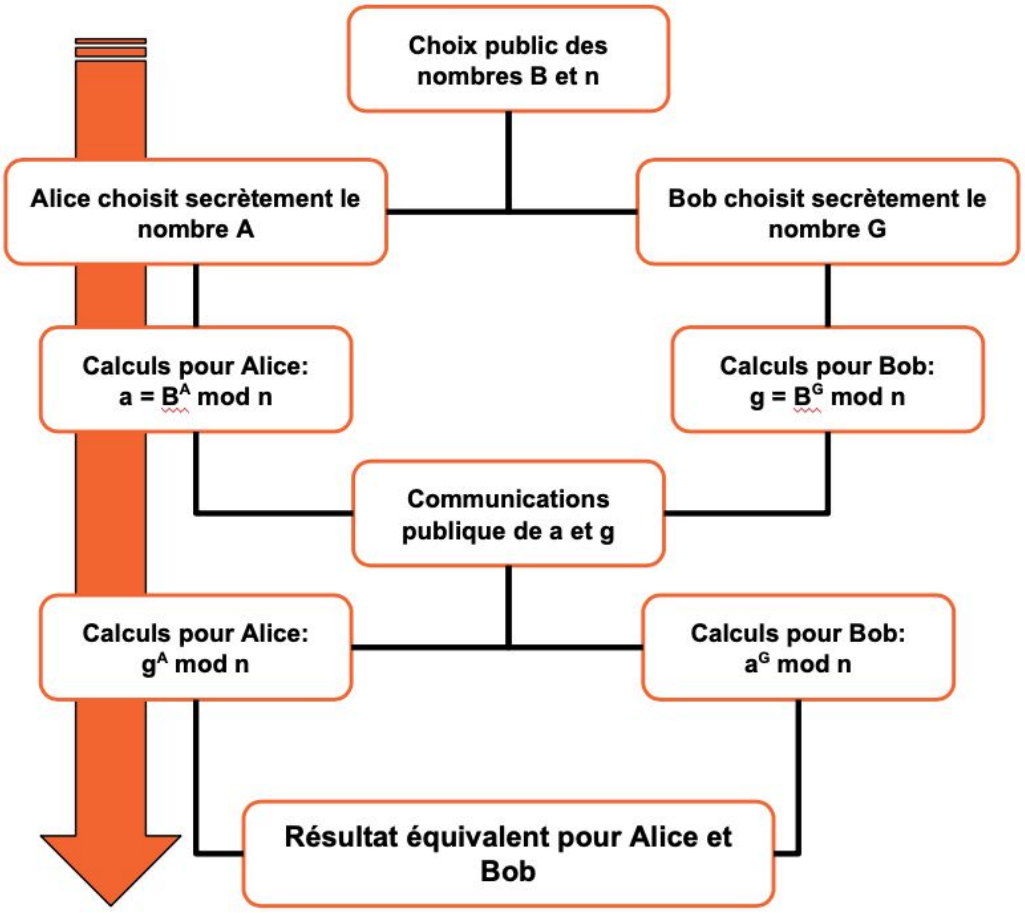
Ici, Charlie ne peut pas deviner la combinaison d'Alice, mais Bob non plus. En effet il ne peut pas éliminer la combinaison 1 0 3 car il ne possède aucune carte de la combinaison.

Règle 4 :
Nous n'avons pas encore trouvé le nombre de combinaison minimum. Nos test nous permettent tout de même de savoir qu'il se situe dans l'intervalle [4 ; 6]. Les exemples précédent parte du principe que le nombre minimale de combinaison est six mais les principes s'applique quelque soit le nombre de combinaison (sauf la règle 2 ou le nombre d'utilisation possible augmente et diminue avec le nombre de combinaison).

<u>Deuxième solution : Le théorème de Diffie-Hellman</u>

Le principe du théorème de Diffie-Hellman est simple. Alice et Bob peuvent obtenir un résultat commun à partir de deux nombre publique et de deux nombre inconnue non seulement de Charlie, mais aussi pour l'un des des deux nombres de Bob et pour l'autre d'Alice. Ce résultat commun va ensuite servir de clé. cette clé va permettre de faire passer secrètement des informations, par exemple les cartes d'Alice.

Détaillons les étapes du théorème :



Pour bien comprendre ce théorème il faut connaître la règle des puissances de puissances et ce qu'est un modulo (mod dans le schéma précédent).

La règle de puissance de puissance :
Pour tout nombre n, x et y positif (n peut être négatif mais pas x et y) :

$$(n^x)^y = n^{xy}$$

exemple :

$$(2^3)^4 = 2^{12}$$

Le modulo :
Le modulo est un symbole opératoir qui retourne le reste d'une division euclidienne.
7 mod 3 = 1 car 7 ⊦ 3 = 2 et qu'il reste 1
On dit que 7 est congru à 1 modulo 3 et on note:
7 ≡ 1 mod 3
Mais 7 n'est pas pas le seul nombre congru à 1 mod 3:
10 ≡ 1 mod 3
13 ≡ 1 mod 3
Et ainsi de suite en ajoutant 3 (à partir de 1).

Détaillons le calcule finale :

Alice calcule :	Bob calcule :
$g^A \bmod n$	$a^G \bmod n$
$((B^G)^A \bmod n) \bmod n$	$((B^A)^G \bmod n) \bmod n$
$(B^G)^A \bmod n$	$(B^A)^G \bmod n$
$B^{AG} \bmod n$	$B^{AG} \bmod n$

C'est donc la règle des puissances de puissances qui permet de trouver un résultat commun. Le modulo sert à compliquer à Charlie la découverte des nombres A et G.En effet, si il est facile de mettre une puissance à nombre, il est plus difficile de trouver la puissance à partir du résultat, ce qui ajouté au modulo devient presque impossible. En effet différente puissance de B peuvent être congru à a mod n ou à b mod n ce qui multiplie les possibilités. La clé finale dépendant donc de ces puissance, Charlie à peu de chance de trouver quelle est la clé.

Une fois la clé trouver, on l'additionne au cartes d'Alice. Il ne faut pas additionner les carte d'Alice séparément à la clé.

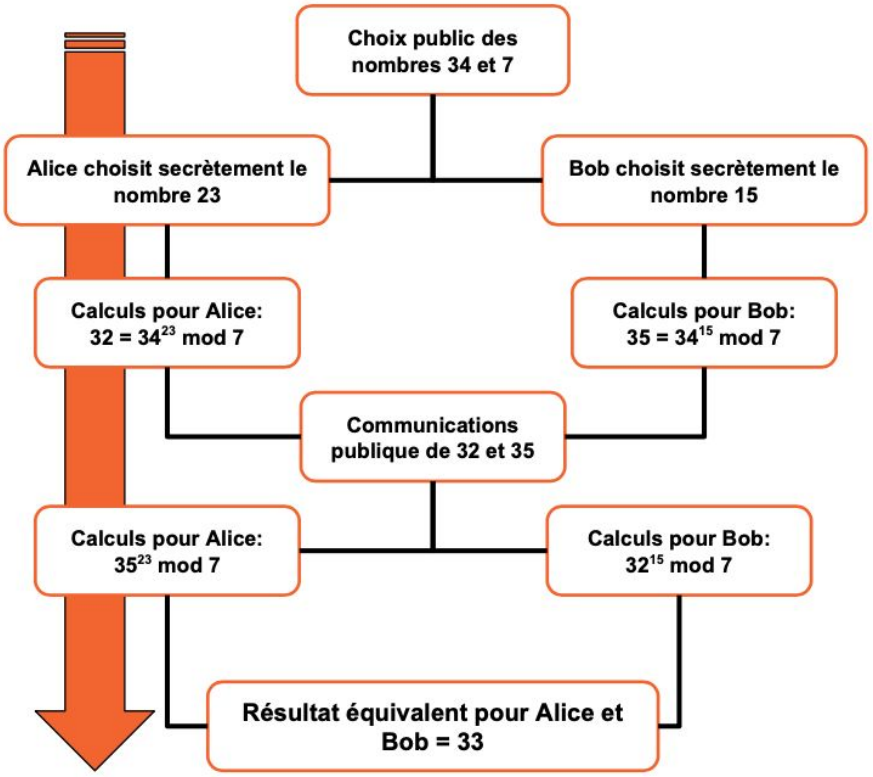
exemple :
La clé est égale à 12, Alice possède les cartes 1,2 et 3, Bob les cartes 4, 5 et 6 et Charlie la carte 0.
Alice additionne ses cartes à la clé : 1+2+3+12 = 18
Elle donne publiquement le résultat à Bob qui soustrait la clé et obtient 6.
Il sait que les seuls moyen d'obtenir six est d'additionner soit 1,2 et 3, soit 0, 1 et 5, soit 0, 2 et 4. Comme il possède le 4 et le 5, il déduit qu'Alice possède le 1, le 2 et le 3.

exemple:
La clé est égale à 12, Alice possède les cartes 0, 2 et 5, Bob les cartes 4, 6 et 3 et Charlie la carte 1.
Alice additionne chacune de ses cartes séparément à la clé : 0+12 =12 2+12=14 5+12=17
Elle donne publiquement les résultats à Bob qui soustrait la clé et trouve 1, 2 et 3.
Charlie de son côté soustrait pour chaque valeur chaque carte un par une:

12-0=12	12-1=11	12-2=10	12-3=9	12-4=8	12-5=7	12-6=6
14-0=14	14-1=13	14-2=12	14-3=11	14-4=10	14-5=9	14-6=8
17-0=17	17-1=16	17-2=15	17-3=14	17-4=13	17-5=12	17-6=11

Il peut donc éliminer toute les possibilités qui n'apparaissent que deux fois ou moins. Et celle qui sont obtenue avec le 1. Il découvre donc toute les cartes d'Alice. Dans certains cas, cette méthode peut marcher mais la première méthode est préférable.

exemple de l'utilisation de tout le théorème pour répondre à toute la question 1 :
Alice possède le 0, le 3 et le 6, Bob le 4, le 2 et le 1, et Charlie le 5.



-Alice additionne c'est carte à la clé : 0+3+6+33 = 42
-Bob soustrait la clé : 42-33 = 9
-9 est égale soit à 1+2+6, soit à 0+5+4, soit à 0+3+6, soit à trois 2+3+4, soit 1+3+5.
-Bob déduit donc que les cartes d'Alice sont 0, 3 et 6 car c'est la seul possibilité qui ne contient pas une de ses cartes.
-Bob dévoile la carte de Charlie
-Alice déduit les cartes de Bob

Et en python:
Le lien ci dessous propose un module et un programme permettant de résoudre la question 1 grâce au théorème de Diffie-Hellman.
Vous pouvez accéder au programme via ce lien :
https://github.com/CortoGarnier/MATH.en.JEAN