MATH.en.JEAN

The Russian Protocol

Author: Théo Audurier and Corto Garnier, Lycée Léonce Vieljeux, La Rochelle
Professor supervising the project: Mr Vederine, Lycée Léonce Vieljeux, La Rochelle
Subject: Mr.Lefloch, University of La Rochelle

The subject “Russian Protocol” consists of three questions :
Question 1:
From a pack of 7 cards numbered 0,1,2,3,4,5,6 Alice & Bob each get 3 cards and Charlie receives the remaining card. How can Alice and Bob get to know each other openly about their respective cards without Charlie knowing any of the cards they have?

Question 2:
On slightly changes the original problem: Charlie can find some cards owned by Alice & Bob, but not all.

Question 3:
This time we has 13 cards numbered 0,1,2,3,4,5,6,7,8,9, A, B, C. Alice, Bob and Charlie receive 4.7 & 2 cards respectively. How can Alice openly tell Bob about his cards without Charlie knowing any of his cards?

version 1
contributor: Corto Garnier

Version 1 of this article only answer question 1. This question develops almost all the solutions which make it possible to resolve the three questions.

Question 1:

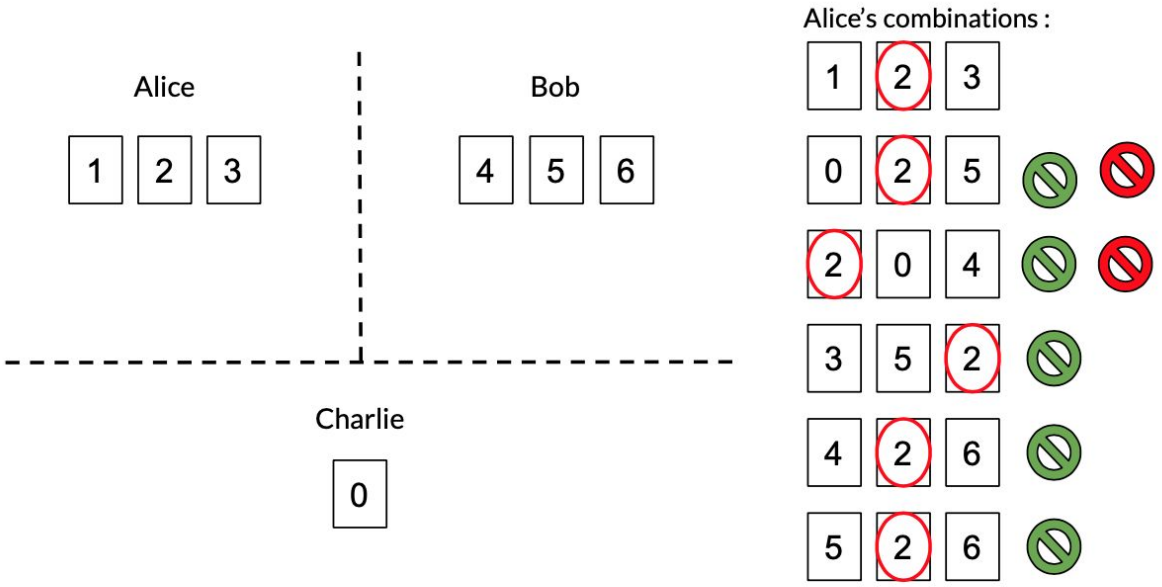
To answer this question we first followed a solution that we finally assigned to the question 2. The two solutions that we therefore worked on question 1 are the using of cards combinations and the Diffie-Hellman theorem.

First solutions: Card combinations

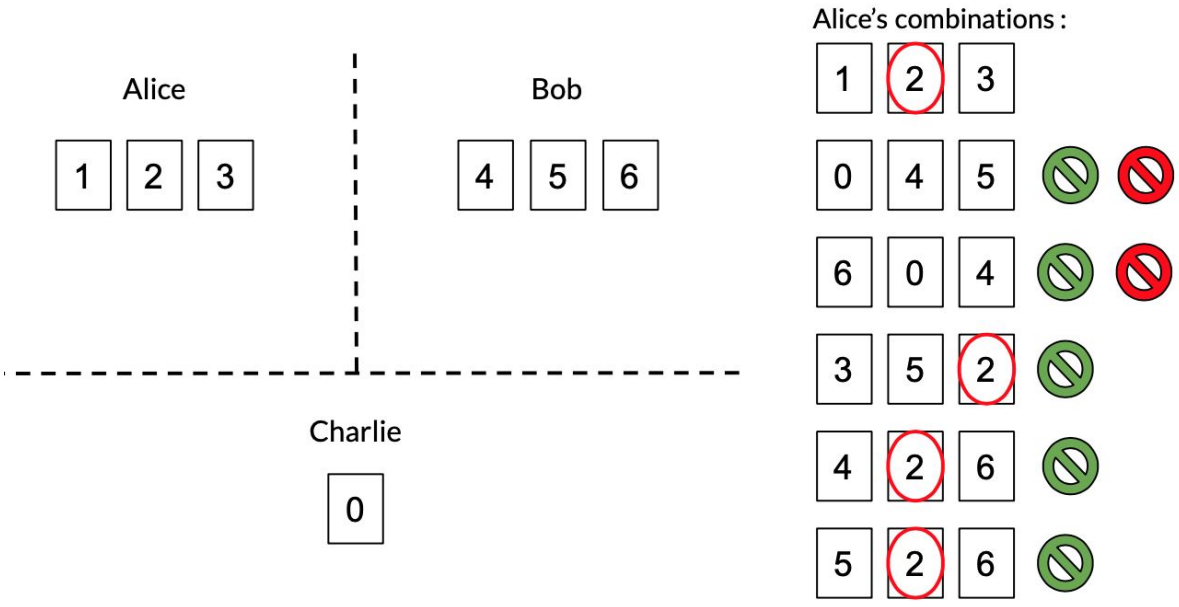
The principle of card combinations is that Alice form 6 combinations of 3 cards which contain her real hands. She declares, after having cited all the combinations she has created, that one of these combinations corresponds to her hand. Then, Bob will eliminate the combinations where his cards appear and will discover Alice's cards. The latter will then reveal Charlie's card so that Alice can deduct her cards.

For this technique to work, certain rules must be followed when creating combinations, these rules if they are not followed allow Charlie to guess Alice's cards, or at least one of his cards.

Rule 1: A number should not cover all combinations, or a number appear too often.
example:



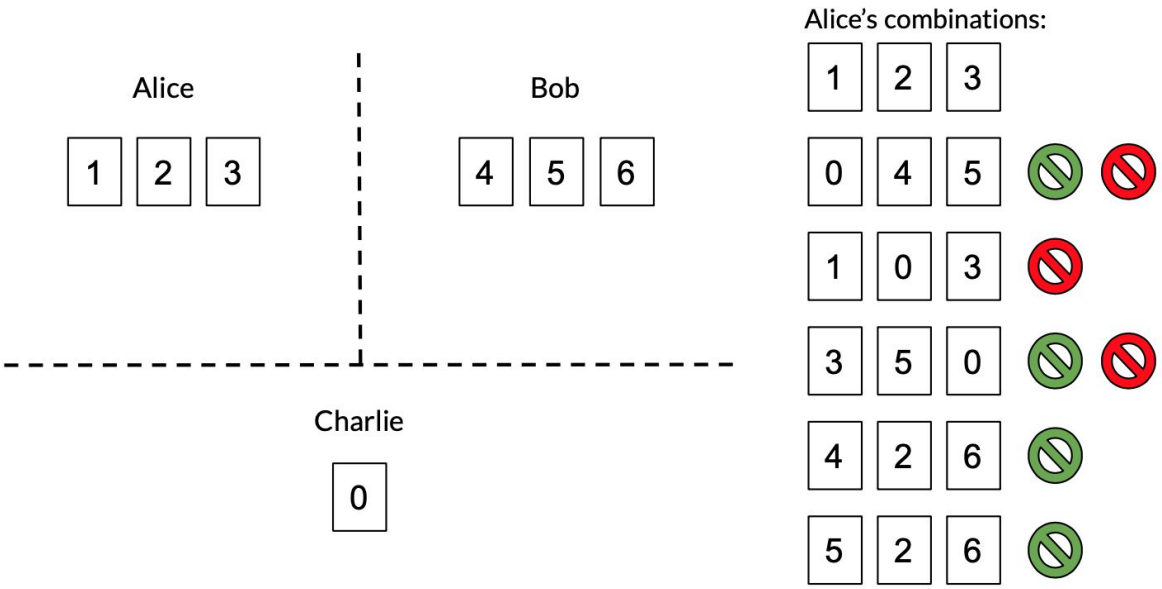
Here Charlie can only eliminate two of Alice's combinations, Bob can eliminate all of the false combinations and found Alice's cards. But Charlie knows that Alice has the 2 because he is in all combinations.
example:



Here Charlie is sure that Alice has the 2 because they are in all the combinations that he has not eliminated.

Rule 2:
(if we keep the six combinations)
Alice must not place a number more than 3 times in the combinations.

Rule 3:
Alice must not place two cards she has in the same combination (except in the real card combination).
example:



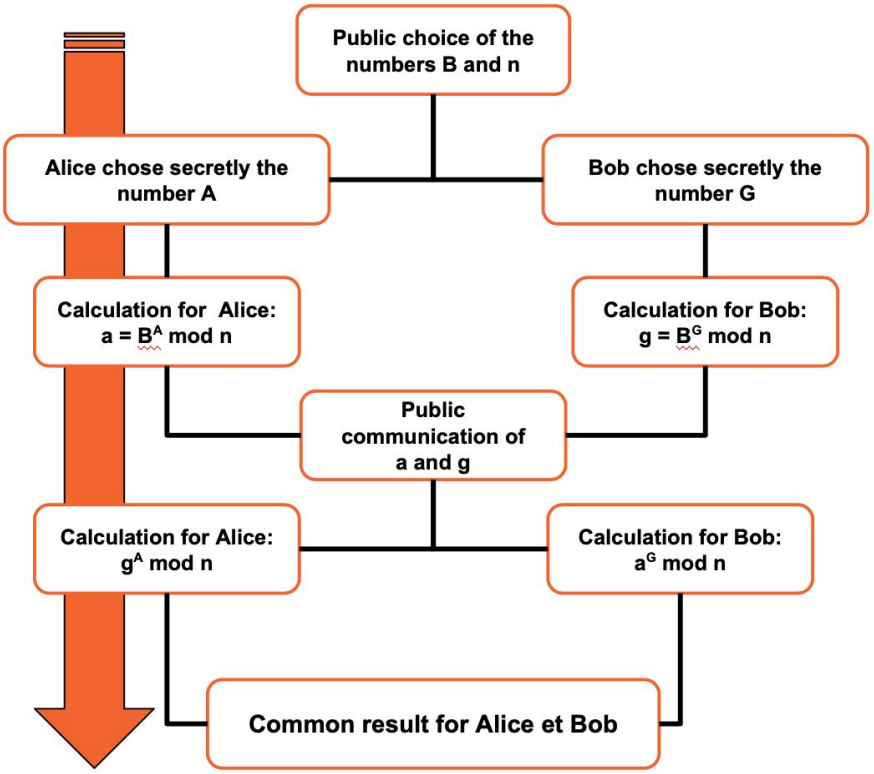
Here Charlie can't guess Alice's suit, but can't Bob too. In fact, he cannot eliminate the combination 1 0 3 because he has no combination card.

Rule 4:
(to rework)
Alice must create six combinations.

<u>Second solution: The Diffie-Hellman</u>

theorem The principle of the Diffie-Hellman theorem is simple. Alice and Bob can get a common result from two public numbers and two secret numbers not only for Charlie, but also for Bob (he don't know Alice's number) and Alice (she don't know the Bob's one). This common result will then serve as a key. this key will make it possible to pass information secretly, for example Alice's cards.

Let us detail the steps of the theorem:



To understand this theorem , you must know the rule of exponent of exponent and what a modulo is (mod in the previous diagram).

The rule of exponent of exponent:
For any positive number n, x and y (n can be negative but not x and y):

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

example:

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

The modulo:
The modulo is an operating symbol that returns the rest of a Euclidean division.
7 mod 3 = 1 because 7 ⊦ 3 = 2 and there remains 1
We say that 7 is congruent to 1 modulo 3 and we note:
7 ≡ 1 mod 3
But 7 is not the only number congruent to 1 mod 3:
10 ≡ 1 mod 3
13 ≡ 1 mod 3
And so on by adding 3 (from 1).
Let us detail the final computation:

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

It is therefore the rule of exponent of exponent which makes it possible to find a common result. The modulo is used to complicate Charlie's discovery of the numbers A and G. Indeed, if it is easy to put a exponent to a number, it is more difficult to find the exponent from the result, which added to the modulo becomes almost impossible . Indeed different power of B can be congruent to a mod n or to g mod n which multiplies the possibilities. The final key therefore depending on these exponents, Charlie is unlikely to find what is the key.

Once the key is found, we add it to Alice's cards. Alice cards must not be added separately to the key.

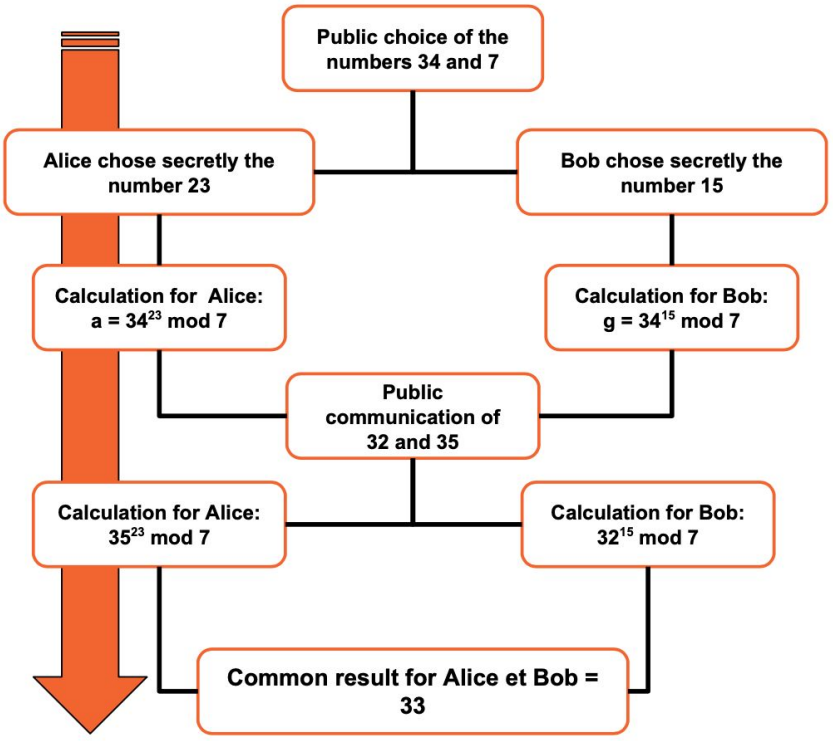
example:
The key is equal to 12, Alice has cards 1,2 and 3, Bob has cards 4, 5 and 6 and Charlie has card 0.
Alice adds her cards to the key: 1 + 2 + 3 + 12 = 18
She publicly gives the result to Bob who subtracts the key and gets 6.
He knows that the only way to get six is to add either 1,2 and 3, or 0, 1 and 5, or 0, 2 and 4.
As he has 4 and 5, he deduces that Alice has 1, 2 and 3.

example:
The key is equal to 12, Alice has cards 0, 2 and 5, Bob has cards 4, 5 and 3 and Charlie the card 1.
Alice adds each of her cards separately to the key: 0 + 12 = 12 2 + 12 = 14 5 + 12 = 17
She publicly gives the results to Bob who subtracts the key and finds 1, 2 and 3.
Charlie for his part subtracts for each value each card one by one:

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

It can therefore eliminate all the possibilities that appear only twice or less and the one obtained with the 1. So he discovers all of Alice's cards. In some case, this method may fonctionne but the first method is preferable.

example of the use of the whole theorem to answer all of question 1:
Alice has 0, 3 and 6, Bob has 4, 2 and 1, and Charlie has 5.



-Alice adds it up to the key: 0 + 3 + 6 + 33 = 42
-Bob subtracts the key: 42-33 = 9
-9 is equal to either 1 + 2 + 6, or to 0 + 5 + 4, or to 0 + 3 + 6, either three 2 + 3 + 4, or 1 + 3 + 5.
-Bob therefore deduces that Alice's cards are 0, 3 and 6 because it is the only possibility that does not contain one of her cards.
-Bob reveals Charlie's card
-Alice deducts Bob's cards

And in python:
The link below offers a module and a program to solve question 1 thanks to the Diffie-Hellman theorem.
You can access the program via this link:
https://github.com/CortoGarnier/MATH.en.JEAN