The Jangada algorithm

Origin of the name (20101011)
The Jangada algorithm came from the name of a novel written by Jules Vernes 'La Jangaga'.

The principle (20101118;20101129)
We have an alphabet A. Each character c of the alphabet is written as c_{alph}. Each character has a position in the alphabet and is written as p_i. We define the position of character in a given alphabet like this :

We define

- c_{alph} A s.a[1] A=[FirstCharacter..LastCharacter] is read FirstCharacter till LastCharacter and c_{alph} is a character that belongs to a given alphabet.
- r_{alph} defines the position of the character in the given alphabet and is defined as r_{alph} $\mathbb{R}^{alph}$ s.a $\mathbb{R}^{alph}$=[1..length(alphabet)] where length(alphabet) $\mathbb{R}$ is the number of character(s) in the alphabet.

The position of a character in the message is r and c is the corresponding character in the message.
We define p a function that gives the character to the corresponding position:

$p_{mess}(r_{mes})\rightarrow c_{mess}$ *where* c_{mess} A and r_{mes} $\mathbb{R}^{alph}$

To get the character from the signature we say that r'_{sig} is the position of the character in the signature and c'_{sig} the given character from the signature at that position:

$p'_{sig}(r'_{sig})\rightarrow c'_{sig}$ *where* c'_{sig} A and r'_{sig} $\mathbb{R}^{alph}$

To crypt one letter from the message we define a function f that takes two arguments: a character from the message and it's corresponding character position from the signature:

$$f(c_{mes}, c_{sig})\rightarrow k_{mes}$$

To calculate f we get current character c_{mes} in the message. We take its corresponding position in the alphabet and we add it with the shift value calculated. If the value calculated is greater than the alphabet length we take the modulo of the length of the alphabet then we have the new position. Hence we get the character in the alphabet from value.

1 s.a: such as