Weak Tea

Code explanation

context

we have created a type called by short who’s just an std:: pair of short

step 0

First, we have generated all possible keys. The process is threaded to boost things.

step 1

The function myfind take for argument * the plain text P * the cipher-text C * all candidate for Ka as K * all candidate for Kb as k This function we encrypt the first given plain text with every K key and stock the value. In the map WList. We use an std::map because they are automatically sorted.

step 2

We start decrypting the cipher-text C with every k and check if the value inside the WList map isn’t null. If the result exists then the function add both K and k inside the vector KaCandidate and KbCandidate

step3

Do again from the step1 with the next cipher-text, plain text and refine Ka and Kb until there are no more C and P or the candidate list size is 1