ATIVIDADE 03 ESPIONAGEM

Sou diretor da empresa BCC - Business Competitiveness Consulting e preciso de serviços especializados para uma investigação. Descobrimos que uma falha de configuração no algoritmo de criptografia utilizado por um de nossos concorrentes permite a recuperação de dados criptografados com determinada chave. Fomos informados que, conhecendo um par (T,C) de Texto claro (original) e seu respectivo texto Cifrado com uma chave K_i, ou parte destes, é possível recuperar outros textos cifrados com a mesma chave, mesmo sem descobrir o cifrador e/ou chave utilizada. Conseguimos obter um conjunto de mensagens de comunicação cifradas com diferentes chaves. O trabalho consiste em descobrir quais mensagens foram cifradas com a mesma chave do par de texto conhecido (T,C) e decifrá-las. Fomos informados que vocês seriam OS especialistas para este trabalho.

Informações gerais:

- A criptografia é realizada com Cifrador de fluxo (Stream Cipher). Este tipo de cifrador tem como requisito de segurança nunca usar a mesma chave para duas cifragens.
- As mensagens capturadas são de 4 bytes, estruturadas como segue:

4	4	4	4	16
$Conta_{origem}$	$agência_{origem}$	$Conta_{destino}$	$agência_{destino}$	Valor

- A falha de segurança descoberta é que o sistema do concorrente utiliza a mesma chave sempre que a mensagem possui mesma conta de origem, ou seja, mesmo 1o byte.

Obs.: o concorrente teve o cuidado de escolher para cada conta uma chave tal que o resultado criptográfico seja diferente entre as contas. Exemplo: Dado Ca = Ma XOR Ka e Cb = Mb XOR Kb, Ca dif Cb.

ENTRADAS

A entrada é composta por mensagens de 4 bytes conforme a estrutura acima. A primeira linha contém a mensagem conhecida (texto claro - T). A segunda linha contém a mensagem T cifrada com a chave K, correspondendo ao texto cifrado C. A terceira linha contém o número de mensagens cifradas capturadas(N), seguido da lista de mensagens cifradas a serem avaliadas, uma por linha.

Exemplo:

3665112892
332770132
2
334678365
317861692

SAIDAS

Deve ser apresentado na saída a lista de valores das transações (campo valor das mensagens decifradas) que possuem a mesma agência e conta de origem da mensagem conhecida. Um valor por linha. Na ordem das mensagens recebidas.

Exemplo:

19765