Heidi: Cyberspace Consultant

Robert R. Enderlein

Hard Task

After some thought, Heidi suspects that the cipher from the previous problem is insecure, but doesn't quite know how to convince her client of that fact. Maybe showing him that you can recover the encryption key given a few plaintext/ciphertext pairs in a few seconds will do the trick? Sometimes, even consultants need consultants, so Heidi decided to once again outsource that task to you.

In this task, you must implement a function with the following signature:

```
long long int challenge(int plaintext1, int ciphertext1,
int plaintext2, int ciphertext2, int plaintext3, int ciphertext3);
```

It receives as input three plaintext/ciphertext pairs of 16 bits each. The function should return the two 16-bit encryption keys with:

```
return answer(key1, key2);
```

The encryption function of Heidi's client is the same one as in the previous problem.

For your convenience, Heidi has implemented a sample brute force cracker. It is however much too slow... she expects something that is a few thousand times faster.

Tâche Difficile

Après y avoir réfléchi, Heidi suspecte que le chiffrement du problème précédent n'est pas sûr, mais elle ne sait pas comment en convaincre son client. Peut-être que lui montrer que l'on peut déduire en quelques secondes la clef de chiffrement à partir de quelques textes et leurs versions chiffrées suffirait à le convaincre? Parfois, même les consultants ont besoin de consultants, Heidi décide ainsi de vous sous-traiter cette tâche.

Dans cette tâche, vous devez implémenter une fonction avec la signature suivante:

```
long long int challenge(int texte1, int texteChiffre1,
int texte2, int texteChiffre2, int texte3, int texteChiffre3);
```

qui reçoit comme entrées trois paires de textes / textes chiffrés de 16 bits chacun. La fonction doit retourner les deux clefs de chiffrements à 16 bit avec:

```
return answer(clef1, clef2);
```

La fonction de chiffrement du client de Heidi est la même que dans le problème précédent.

Pour vous simplifier la tâche, Heidi a déjà implémenté une fonction qui retrouve les clefs avec une attaque par force brute. Elle est cependant bien trop lente... elle souhaite que vous trouviez quelque chose plusieurs milliers de fois plus rapide.

Schwierige Aufgabe

Heidi investiert noch etwas Zeit und analysiert den Verschlüsslungsalgorithmus aus der vorhergehenden Aufgabe etwas genauer. Sie kommt zum Schluss, dass der Algorithmus nicht sicher ist. Sie fragt sich

aber wie sie ihren Kunden davon überzeugen kann. Vielleicht bringt es etwas dem Kunden zu zeigen, dass man innerhalb von Sekunden die Schlüssel herausfinden kann, vorausgesetzt man kennt mehrere Plaintext/Ciphertext Paare. Auch hier braucht Heidi wieder die Hilfe eine Beraters und bittet darum euch um Hilfe.

Eure Aufgabe ist es, eine Funktion zu schreiben mit der folgenden Signatur:

```
long long int challenge(int plaintext1, int ciphertext1,
  int plaintext2, int ciphertext2, int plaintext3, int ciphertext3);
```

Die Funktion nimmt drei Plaintext/Ciphertext Paare wobei Plaintext und Ciphertext immer aus je 16-bit bestehen. Die Funktion sollte die zwei 16-bit Schlüssel berechnen und folgendermassen zurückgeben:

```
return answer(key1, key2);
```

Die Verschlüsselung von Heidi's Kunde ist die gleiche wie im vorhergehenden Problem.

Um euch etwas zu helfen hat Heidi eine Bruteforcelösung implementiert, welche die Schlüssel herausfinden kann. Leider ist dieser Ansatz viel zu langsam. Heidi erwartet eine Lösung welche mehrere tausend mal schneller ist.