Cryptage des données sur AS400

- Les articles -

Date de mise en ligne : lundi 11 octobre 2004

Description :

Cryptage des données sur AS400 (Sans Cryptographic Access Provider 128 bits)

Environnement iSeries

Attention le cryptage de données est règlementé, renseignez vous sur la législation en vigueur.

Le cryptage de donnée sur l'AS400 est géré par un coprocesseur (4758 Coprocessor) disponible avec l'acquisition d'un carte de cryptage (Cryptographic Access Provider 128 bits). Un lot d'api est fourni pour pouvoir crypter des fichiers grace à des algorithmes reconnus du marché (tel que DES).

Cependant, il est possible de crypter un fichier sur l'AS400 grace à l'instruction XOR (ou exclusif disponible avec SQL ou en RPG). Voici les bases d'un tel cryptage...

XOR est une fonction récursive, ce qui signifie que si vous l'appliquer 2 fois de suite (avec la même clé) vous revenez au point de départ.

Par exemple (clé utilisée :"CLESECRETE") :

```
UPDATE MABIB/MONFICHIER SET MAZONE = XOR(MAZONE,'CLESECRETECLESECR')
```

Maintenant MAZONE est cryptée.

```
UPDATE MABIB/MONFICHIER SET MAZONE = XOR (MAZONE,'CLESECRETECLESECR')
```

Maintenant MAZONE est décryptée.

Votre clé doit être de longueur égale à la zone que vous souhaitez crypter (dans l'exemple MAZONE fait 17 caractères).

Attention surtout si un caractère se répète souvent ou pire encore si votre zone est succeptible de comporter plusieurs espaces (sur AS400 un XOR sur un espace à l'aide d'un caractère rend ce caractère en minuscule). Pour palier à ces inconvénient vous devrez combiner la clé avec par exemple un N° de ligne et remplacer vos espaces par des caractères moins facilement identifiables.

Nouveau V5R4 : SQL prend en charge directement le cryptage DES.

Post-scriptum :

Un tel cryptage peut être mis en place pour des données moyennement sensible. Pour des applications plus sensibles telles que des transactions bancaires il faut équiper son AS400 d'une carte de cryptographie. RDV sur le site d'IBM pour en savoir plus.