

# Chiffrement symétrique des données sous Oracle

## Description générale

Le chiffrement symétrique repose sur l'utilisation d'une clé unique pour chiffrer et déchiffrer les données. Avec Oracle, le package DBMS\_CRYPTO permet d'utiliser plusieurs algorithmes de chiffrement comme AES, DES et 3DES

## Module de chiffrement DBMS\_CRYPTO

Oracle fournit le package DBMS\_CRYPTO permettant d'effectuer des opérations de chiffrement et de déchiffrement de données de manière sécurisée.

Lien vers la documentation officielle

[:https://docs.oracle.com/en/database/oracle/oracle-database/19/arpls/DBMS\\_CRYPTO.html](https://docs.oracle.com/en/database/oracle/oracle-database/19/arpls/DBMS_CRYPTO.html)

## Droit d'exécution sur ce module

**Pour utiliser DBMS\_CRYPTO, il est nécessaire de disposer du privilège EXECUTE sur le package :** GRANT EXECUTE ON DBMS\_CRYPTO TO utilisateur;

## Type des données chiffrées

Les données à chiffrer peuvent être des chaînes de caractères (VARCHAR2, CLOB) ou des types binaires (BLOB). Il est recommandé d'utiliser RAW pour le stockage de données chiffrées.

## Chiffrement des données

Prenons un exemple sur une base de donnée existante et Dans la table Clients, on ajoute une colonne nomCli\_enc pour stocker les noms chiffrés : ALTER TABLE Clients ADD nomCli\_enc RAW(2000); Ensuite on chiffre les noms des clients existants et les stocke dans la colonne nomCli\_enc : UPDATE Clients SET nomCli\_enc = DBMS\_CRYPTO.ENCRYPT( src => UTL\_RAW.cast\_to\_raw(nomCli), typ => DBMS\_CRYPTO.ENCRYPT\_AES256 + DBMS\_CRYPTO.CHAIN\_CBC + DBMS\_CRYPTO.PAD\_PKCS5, key => UTL\_RAW.cast\_to\_raw('MaCleSecrete16Bytes'), iv => UTL\_RAW.cast\_to\_raw('InitialVector123') );

==== Déchiffrement des données ====

From:  
<https://wiki.siochaptalqper.fr/> - **Wiki SIO Chaptal**

Permanent link:  
<https://wiki.siochaptalqper.fr/doku.php?id=bloc3:bdd-symmetric-ciphering&rev=1742281814>

Last update: **2025/03/18 08:10**

