OpenSSL - enc

Routines de chiffrements symétriques

Permet de chiffrer ou déchiffrer des données en utilisant divers block ou flux de chiffrement en utilisant des clés basé sur mot de passe ou fournis explicitement. L'encodage/décodage en base 64 peut également être effectué en plus du chiffrement/déchiffrement.

OPTIONS

-in filename Fichier d'entrée

-out filename Fichier de sortie

-pass arg Source du mot de passe

-salt Utilise un Salt dans les routines de dérivation de clé pendant le chiffrement (défaut). Généré aléatoirement avec l'option -S

-nosalt N'utilise pas de Salt. Ne doit être utilisé que pour des tests un pour compatibilité avec des anciennes versions d'OpenSSL.

-S salt Le Salt à utiliser au format hexa

-e Chiffre la donnée en entrée (défaut)

-d Déchiffre la donnée en entrée

-a Traite les données en base 64.

-base64 Idem à -a

-A si -a, le traitement base64 se fait sur une ligne

-k password Le mot de passe à dériver de la clé. Pour la compatibilité avec d'anciennes versions d'OpenSSL. Remplacé par -pass

-kfile filename Le mot de passe à dériver de la clé depuis ce fichier. Pour la compatibilité avec d'anciennes versions d'OpenSSL. Remplacé par -pass

-K key La clé à utiliser en hexa. IV doit être spécifié avec -iv. Si la clé et le mot de passe sont spécifiés, IV est généré depuis le mot de passe.

-iv IV L'IV à utiliser en hexa

-p Afficher la clé et l'IV utilisé

-P Idem à -p mais quitte immédiatement

-bufsize number Définis la taille du tampon pour les E/S

-nopad Désactive le padding de block standard

-debug Débug les BIO utilisé pour les E/S

-z Compresse ou décompresse en texte clair en utilisant zlib avant le chiffrement ou après le déchiffrement.

-none Utilise le chiffrement NULL

Notes

Les moteurs qui fournissent de nouveaux algorithmes de chiffrement (tel que ccgost qui fournis l'algorithme gost89) devraient être configurés dans le fichier de configuration. Les moteurs spécifiés sur la ligne de commande peuvent seulement être utilisé avec des implémentations de chiffrement assisté par hardware supportés par OpenSSL core.

Chiffrements supportés

Noter que certains chiffrements peuvent être désactivés à la compilation.

```
base64 Base 64

bf-cbc Blowfish in CBC mode
bf Alias for bf-cbc
bf-cfb Blowfish in CFB mode
bf-ecb Blowfish in ECB mode
bf-ofb Blowfish in OFB mode

cast-cbc CAST in CBC mode
cast Alias for cast-cbc
cast5-cbc CAST5 in CBC mode
cast5-cfb CAST5 in CFB mode
cast5-ecb CAST5 in ECB mode
cast5-ofb CAST5 in OFB mode

des-cbc DES in CBC mode
des Alias for des-cbc
des-cfb DES in CBC mode
des-ofb DES in OFB mode
des-ecb DES in ECB mode

des-ede-cbc Two key triple DES EDE in CBC mode
des-ede Two key triple DES EDE in ECB mode
des-ede-cfb Two key triple DES EDE in CFB mode
des-ede-ofb Two key triple DES EDE in OFB mode

des-ede3-cbc Three key triple DES EDE in CBC mode
des-ede3 Three key triple DES EDE in ECB mode
des3 Alias for des-ede3-cbc
des-ede3-cfb Three key triple DES EDE CFB mode
des-ede3-ofb Three key triple DES EDE in OFB mode

desx DESX algorithm.

gost89 GOST 28147-89 in CFB mode (provided by ccgost engine)
gost89-cnt 'GOST 28147-89 in CNT mode (provided by ccgost engine)

idea-cbc IDEA algorithm in CBC mode
idea same as idea-cbc
idea-cfb IDEA in CFB mode
idea-ecb IDEA in ECB mode
idea-ofb IDEA in OFB mode

rc2-cbc 128 bit RC2 in CBC mode
rc2 Alias for rc2-cbc
rc2-cfb 128 bit RC2 in CFB mode
rc2-ecb 128 bit RC2 in ECB mode
rc2-ofb 128 bit RC2 in OFB mode
rc2-64-cbc 64 bit RC2 in CBC mode
rc2-40-cbc 40 bit RC2 in CBC mode

rc4 128 bit RC4
rc4-64 64 bit RC4
rc4-40 40 bit RC4

rc5-cbc RC5 cipher in CBC mode
rc5 Alias for rc5-cbc
```

```
rc5-cfb RC5 cipher in CFB mode
rc5-ecb RC5 cipher in ECB mode
rc5-ofb RC5 cipher in OFB mode

aes-[128|192|256]-cbc 128/192/256 bit AES in CBC mode
aes-[128|192|256] Alias for aes-[128|192|256]-cbc
aes-[128|192|256]-cfb 128/192/256 bit AES in 128 bit CFB mode
aes-[128|192|256]-cfb1 128/192/256 bit AES in 1 bit CFB mode
aes-[128|192|256]-cfb8 128/192/256 bit AES in 8 bit CFB mode
aes-[128|192|256]-ecb 128/192/256 bit AES in ECB mode
aes-[128|192|256]-ofb 128/192/256 bit AES in OFB mode
```

Exemples

Encoder un fichier binaire en base 64
openssl base64 -in file.bin -out file.b64
Décoder le même fichier
openssl base64 -f -in file.b64 -out file.bin
Chiffrer un fichier avec 3DES en mode CBC
openssl des3 -salt -in file.txt -out file.des3
Déchiffrer un fichier en fournissant le mot de passe
openssl des3 -d -salt -in file.des3 -out file.txt -k mypassword
Chiffrer un fichier puis l'encoder en base 64 avec blowfish en mode CBC
openssl bf -a -salt -in file.txt -out file.bf
Décode un fichier base 64 et le déchiffrer
openssl bf -d -salt -a -in file.bf -out file.txt
Déchiffre des données en utilisant une clé RC4 40 Bits
openssl rc4-40 -in file.rc4 -out file.txt -K 0102030405