OpenSSL - ciphers

Convertis les listes de chiffrement en liste de préférence ordonnées. Peut être utilisé comme outil de test pour déterminer la liste de chiffrement.

OPTIONS

-v mode verbeux

-V idem à -v mais inclus les codes des suites de chiffrements en hexa.

-ssl3 Uniquement les chiffrements SSL v3

-ssl2 Uniquement les chiffrements SSL v2

-tls1 Uniquement les chiffrements TLS v1

cipherlist Une liste de chiffrement à convertir en une liste de préférence de chiffrement.

Format de liste de chiffrement

Une liste consiste en une ou plusieurs chaîne de chiffrement séparés par des ' **:**'. Une liste peut être une suite de chiffrements simple comme RC4-SHA. Elle peut représenter un certain algorithme. Par exemple SHA1 représente toutes les suites utilisant cet algorithme, et SSLv3 représente tous les algorithmes SSLv3.

Les listes de suite de chiffrement peuvent être combinées en une simple chaîne en utilisant le '**+**' (est un ET logique), un '**!**' pour les chiffrements à supprimer de la liste, un '**-**' pour ceux à supprimer, mais qui peuvent être rajoutés ultérieurement. En plus, la chaine de chiffrement **@STRENGTH** peut être utilisée pour trier la liste de chiffrement courante dans l'ordre de longueur de clé de chiffrement.

Chaînes de chiffrement

Liste des chaînes de chiffrement permises et leur signification :

DEFAULT Liste de chiffrement par défaut. Déterminé à la compilation. (pour openssl v1.0.0 est normalement à **ALL : !aNULL : !eNULL**). Doit être la première chaîne de chiffrement spécifiée.

COMPLEMENTOFDEFAULT Les chiffrement inclus dans ALL, mais non actifs par défaut.

ALL Toutes les suites de chiffrement sauf eNULL

COMPLEMENTOFALL Les suites de chiffrement non activés par ALL, actuellement eNULL.

HIGH Suites de chiffrements élevés. Actuellement, signifie toutes les longueurs de clé supérieurs à 128 bits, et certains chiffrements avec clé 128 bits.

MEDIUM Suites de chiffrements moyens. Actuellement, signifie toutes les longueurs de clé à 128 bits.

LOW Suites de chiffrements faibles. Actuellement, signifie toutes les longueurs de clé supérieurs à 56 ou 64 bits mais exclus les suites de chiffrement d'export

EXP, EXPORT Algorithmes de chiffrement d'export, incluant les clés à 56 et 64 bits.

EXPORT40 Algorithmes de chiffrement d'export de 40 bits

EXPORT56 Algorithmes de chiffrement d'export de 56 bits

eNULL, NULL Chiffrement qui n'offrent pas de cryptage.

aNULL Suites de chiffrement n'offrant pas d'authentification. Actuellement, les algorithmes DH anonymes. Vulnérables aux attaques MITM.

kRSA, RSA Suites de chiffrement utilisant les échanges de clé RSA

kEDH Suites de chiffrement utilisant les agréments de clé DH éphémères

kDHr, kDHd Suites de chiffrement utilisant les agréments de clé DH et les certificats DH signés par CA avec des clé RSA et DSS, respectivement.

aRSA Suites de chiffrement utilisant l'authentification RSA.

aDSS, DSS Suites de chiffrement utilisant l'authentification DSS

aDH Suites de chiffrement utilisant effectivement l'authentification DH.

kFZA, aFZA, eFZA, FZA Suites de chiffrement utilisant l'échange de clé, l'authentification et/ou le chiffrement FORTEZZA

TLSv1, SSLv3, SSLv2 Suites de chiffrement utilisant respectivement TLS v1, SSL v3 et SSL v2.

DH Suites de chiffrement utilisant DH, incluant DH anonyme.

ADH Suites de chiffrement utilisant DH anonyme.

AES Suites de chiffrement utilisant AES

CAMELLIA Suites de chiffrement utilisant Camellia

3DES Suites de chiffrement utilisant 3DES

DES Suites de chiffrement utilisant DES

RC4 Suites de chiffrement utilisant RC4

RC2 Suites de chiffrement utilisant RC2

IDEA Suites de chiffrement utilisant IDEA

SEED Suites de chiffrement utilisant SEED

MD5 Suites de chiffrement utilisant MD5

SHA1, SHA Suites de chiffrement utilisant SHA1

aGOST Suites de chiffrement utilisant GOST R 34.10 (soit 2001 soit 94) pour l'authentification

aGOST01 Suites de chiffrement utilisant l'authentification GOST R 34.10-2001

aGOST94 Suites de chiffrement utilisant L'authentification GOST R 34.10-94

kGOST Suites de chiffrement utilisant l'échange de clé VKO 34.10 (RFC 4357)

GOST94 Suites de chiffrement utilisant HMAC basé sur GOST R 34.10-94

GOST89MAC Suites de chiffrement utilisant GOST 28147-89 MAC

Noms des suites de chiffrement

Les listes suivantes donnent les noms des suites de chiffrement SSL ou TLS et leur équivalent OpenSSL.

Suites de chiffrement SSL v3.0

```
SSL_RSA_WITH_NULL_MD5 NULL-MD5
SSL_RSA_WITH_NULL_SHA NULL-SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5 EXP-RC4-MD5
SSL_RSA_WITH_RC4_128_MD5 RC4-MD5
SSL_RSA_WITH_RC4_128_SHA RC4-SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5 EXP-RC2-CBC-MD5
SSL_RSA_WITH_IDEA_CBC_SHA IDEA-CBC-SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA EXP-DES-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA DES-CBC-SHA
```

```
SSL_RSA_WITH_3DES_EDE_CBC_SHA DES-CBC3-SHA

SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA Not implemented.
SSL_DH_DSS_WITH_DES_CBC_SHA Not implemented.
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA Not implemented.
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA Not implemented.
SSL_DH_RSA_WITH_DES_CBC_SHA Not implemented.
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA Not implemented.
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA EXP-EDH-DSS-DES-CBC-SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA EDH-DSS-CBC-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA EDH-DSS-DES-CBC3-SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA EXP-EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA EDH-RSA-DES-CBC3-SHA

SSL_DH_anon_EXPORT_WITH_RC4_40_MD5 EXP-ADH-RC4-MD5
SSL_DH_anon_WITH_RC4_128_MD5 ADH-RC4-MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA EXP-ADH-DES-CBC-SHA
SSL_DH_anon_WITH_DES_CBC_SHA ADH-DES-CBC-SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA ADH-DES-CBC3-SHA

SSL_FORTEZZA_KEA_WITH_NULL_SHA Not implemented.
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA Not implemented.
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA Not implemented.
```

Suites de chiffrement TLS v1.0

```
TLS_RSA_WITH_NULL_MD5 NULL-MD5
TLS_RSA_WITH_NULL_SHA NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5 EXP-RC4-MD5
TLS_RSA_WITH_RC4_128_MD5 RC4-MD5
TLS_RSA_WITH_RC4_128_SHA RC4-SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 EXP-RC2-CBC-MD5
TLS_RSA_WITH_IDEA_CBC_SHA IDEA-CBC-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA DES-CBC3-SHA

TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA Not implemented.
TLS_DH_DSS_WITH_DES_CBC_SHA Not implemented.
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA Not implemented.
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_DES_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA Not implemented.
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA EXP-EDH-DSS-DES-CBC-SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA EDH-DSS-CBC-SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA EDH-DSS-DES-CBC3-SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA EXP-EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA EDH-RSA-DES-CBC3-SHA

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 EXP-ADH-RC4-MD5
TLS_DH_anon_WITH_RC4_128_MD5 ADH-RC4-MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA EXP-ADH-DES-CBC-SHA
TLS_DH_anon_WITH_DES_CBC_SHA ADH-DES-CBC-SHA
```

```
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA ADH-DES-CBC3-SHA
```

Suites de chiffrement AES de la rfc3268, étendant TLS v1.0

```
TLS_RSA_WITH_AES_128_CBC_SHA AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA AES256-SHA

TLS_DH_DSS_WITH_AES_128_CBC_SHA Not implemented.
TLS_DH_DSS_WITH_AES_256_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_AES_128_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_AES_256_CBC_SHA Not implemented.

TLS_DHE_DSS_WITH_AES_128_CBC_SHA DHE-DSS-AES128-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA DHE-DSS-AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA DHE-RSA-AES256-SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA ADH-AES128-SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA ADH-AES256-SHA
```

Suites de chiffrement Camellia de la rfc4132, étendant TLS v1.0

```
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA CAMELLIA128-SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA CAMELLIA256-SHA

TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA Not implemented.
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA Not implemented.

TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA DHE-DSS-CAMELLIA128-SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA DHE-DSS-CAMELLIA256-SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA DHE-RSA-CAMELLIA128-SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA DHE-RSA-CAMELLIA256-SHA

TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA ADH-CAMELLIA128-SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA ADH-CAMELLIA256-SHA
```

Suites de chiffrement SEED de la rfc4162, étendant TLS v1.0

```
TLS_RSA_WITH_SEED_CBC_SHA SEED-SHA

TLS_DH_DSS_WITH_SEED_CBC_SHA Not implemented.
TLS_DH_RSA_WITH_SEED_CBC_SHA Not implemented.

TLS_DHE_DSS_WITH_SEED_CBC_SHA DHE-DSS-SEED-SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA DHE-RSA-SEED-SHA
```

TLS_DH_anon_WITH_SEED_CBC_SHA ADH-SEED-SHA

Suites de chiffrement GOST du draft-chudov-cryptopro-cptls, étendant TLS v1.0

Note : Ces chiffrements nécessitent un moteur qui inclut les algorithmes cryptographique GOST tel que le moteur ccgost, inclus dans OpenSSL.

TLS_GOSTR341094_WITH_28147_CNT_IMIT GOST94-GOST89-GOST89
TLS_GOSTR341001_WITH_28147_CNT_IMIT GOST2001-GOST89-GOST89
TLS_GOSTR341094_WITH_NULL_GOSTR3411 GOST94-NULL-GOST94
TLS_GOSTR341001_WITH_NULL_GOSTR3411 GOST2001-NULL-GOST94

Exports additionnels 1024 et autres suites de chiffrement

Note : Ces chiffrements peuvent aussi être utilisé dans SSL v3

TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA EXP1024-DES-CBC-SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA EXP1024-RC4-SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA EXP1024-DHE-DSS-DES-CBC-SHA
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA EXP1024-DHE-DSS-RC4-SHA
TLS_DHE_DSS_WITH_RC4_128_SHA DHE-DSS-RC4-SHA

Suites de chiffrement SSL v2.0

SSL_CK_RC4_128_WITH_MD5 RC4-MD5
SSL_CK_RC4_128_EXPORT40_WITH_MD5 EXP-RC4-MD5
SSL_CK_RC2_128_CBC_WITH_MD5 RC2-MD5
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 EXP-RC2-MD5
SSL_CK_IDEA_128_CBC_WITH_MD5 IDEA-CBC-MD5
SSL_CK_DES_64_CBC_WITH_MD5 DES-CBC-MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 DES-CBC3-MD5

Exemples

Lister tous les chiffrements OpenSSL incluant les chiffrements NULL :
openssl ciphers -v 'ALL :eNULL'
Inclure tous les chiffrements excepté NULL et DH anonyme, et trier par force :
openssl ciphers -v 'ALL :!ADH :@STRENGTH'
Inclure seulement les chiffrements 3DES puis placer RSA en dernier :
openssl ciphers -v '3DES :+RSA'
Inclure tous les chiffrements RC4 mais laisser ceux sans authentification :
openssl ciphers -v 'RC4 :!COMPLEMENTOFDEFAULT'
Inclure tous les chiffrements avec authentification RSA mais laisser les chiffrements sans cryptage :
openssl ciphers -v 'RSA :!COMPLEMENTOFALL'