### decrypt()

Javaが提供するCipherクラスを利用して、暗号化されたバイナリ値を復号化し、返します。

#### 構文

decrypt(CIPHER, KEY, DATA[, IV])

必須パラメータ

**CIPHER**

アルゴリズム/モード/パディング 形式の文字列を返す式です。モードやパディングを省略してアルゴリズムのみを指定した場合、デフォルトの暗号アルゴリズムが適用されます。

* AES のみを指定した場合は AES/CBC/NoPadding が使用されます。
* RSA のみを指定した場合は RSA/ECB/PKCS1Padding が使用されます。

: 利用可能なアルゴリズム、モード、パディングについては、Java Security Standard Algorithm Names ドキュメントを参照してください:<https://docs.oracle.com/en/java/javase/11/docs/specs/security/standard-names.html>

* アルゴリズムは **\_Cipher Algorithm Names\_** セクションで確認できます。
* モードは **\_Cipher Algorithm Modes\_** セクションで確認できます。
* パディングは **\_Cipher Algorithm Paddings\_** セクションで確認できます。

ログプレッソ・ソナーは互換性のためにJavaが提供する多様な暗号アルゴリズムをサポートしています。ただし、DES系やECBモードなど安全でない暗号アルゴリズムやモードの使用は推奨しません。Javaで利用される暗号化クラス（Cipher Class）については、以下のドキュメントを参照してください: https://docs.oracle.com/en/java/javase/11/docs/api/java.base/javax/crypto/Cipher.html

以下はすべてのJava実装で必ずサポートされる形式です。DES、DESedeアルゴリズムやECBモードは安全ではないため、外部システムとの互換性など特別な理由がある場合のみ使用してください。括弧内は暗号化ビット数を示します。- AES/CBC/NoPadding (128)- AES/CBC/PKCS5Padding (128)- AES/ECB/NoPadding (128)- AES/ECB/PKCS5Padding (128)- AES/GCM/NoPadding (128)- DES/CBC/NoPadding (56)- DES/CBC/PKCS5Padding (56)- DES/ECB/NoPadding (56)- DES/ECB/PKCS5Padding (56)- DESede/CBC/NoPadding (168)- DESede/CBC/PKCS5Padding (168)- DESede/ECB/NoPadding (168)- DESede/ECB/PKCS5Padding (168)- RSA/ECB/PKCS1Padding (1024, 2048)- RSA/ECB/OAEPWithSHA-1AndMGF1Padding (1024, 2048)- RSA/ECB/OAEPWithSHA-256AndMGF1Padding (1024, 2048)

**KEY**

指定した暗号アルゴリズムに適合するサイズのバイナリキーを入力します。アルゴリズムごとのキー長は以下の通りです。

* AES: 16文字（128ビット）、24文字（192ビット）、32文字（256ビット）から選択
* RSA: 128文字（1024ビット）、256文字（2048ビット）から選択
* 暗号化キーの長さは、暗号アルゴリズムが要求するキー長を8で割った値（バイト単位）です。

**DATA**

復号化するバイナリデータ

オプションパラメータ

**IV**

CBCなど初期化ベクター（IV, Initial Vector）が必要な動作モードを使用する場合に指定するバイナリ値

#### 使用例

以下のクエリは、[encrypt()](https://docs.logpresso.comnull) の使用例と比較してください。

json "{}"| eval decrypted= decode( decrypt("AES",frombase64("mRcOlK9V47rjVL/RBYQYRw=="), frombase64("y7+NQQ9/9xGtbBq5pgBvCA==") ))