### encrypt()

バイナリ値を指定したアルゴリズムとキーで暗号化し、結果を返します。

#### 構文

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

ログプレッソ・ソナーは互換性のために、Java が提供する様々な暗号アルゴリズムをサポートしています。ただし、DES 系列や ECB モードのような安全でない暗号アルゴリズムやモードの使用は推奨されません。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

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 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/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。

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等、やむを得ない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**

暗号化対象のバイナリデータ

オプションパラメータ

**IV**

CBC など初期化ベクトル（IV, Initial Vector）が必要な動作モードを使用する場合のバイナリ値

#### 使用例

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

json "{}"| eval encrypted=tobase64( encrypt("AES", frombase64("mRcOlK9V47rjVL/RBYQYRw=="), binary("hello, world!") ))