### decrypt()

Java가 제공하는 Cipher 클래스를 이용해 암호화된 바이너리 값을 복호화하여 반환합니다.

#### 문법

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

필수 매개변수

**CIPHER**

알고리즘/모드/패딩 형식으로 구성된 문자열을 반환하는 표현식. 모드와 패딩을 생략하고 알고리즘만 입력하면 기본 암호 알고리즘을 적용합니다.

* AES만 입력하면 AES/CBC/NoPadding를 사용합니다.
* RSA만 입력하면 RSA/ECB/PKCS1Padding을 사용합니다.

사용할 수 있는 알고리즘, 모드, 패딩은 Java Security Standard Algorithm Names 문서를 참조하십시오: <https://docs.oracle.com/en/java/javase/11/docs/specs/security/standard-names.html>.

* 알고리즘은 **Cipher Algorithm Names** 섹션에서 확인할 수 있습니다.
* 모드는 **Cipher Algorithm Modes** 섹션에서 확인할 수 있습니다.
* 패딩은 **Cipher Algorithm Paddings** 섹션에서 확인할 수 있습니다.

로그프레소는 호환성을 위해 Java가 제공하는 다양한 암호 알고리즘을 지원합니다. 그러나 DES 계열이나 ECB 모드와 같이 안전하지 않은 암호 알고리즘이나 모드는 사용하지 않는 것이 좋습니다. Java에서 사용하는 암호화 클래스(Cipher Class)는 다음 주소에 있는 문서를 참조하십시오: https://docs.oracle.com/en/java/javase/11/docs/api/java.base/javax/crypto/Cipher.html

다음은 모든 Java 구현체가 반드시 지원해야 하는 형식입니다. DES, DESede 알고리즘, ECB 모드는 안전하지 않으므로 외부 시스템과 호환성 문제 등이 있을 때에만 사용하기 바랍니다. 괄호 안은 암호화 비트를 나타냅니다. - 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**

지정한 암호 알고리즘에 일치하는 크기의 바이너리 키를 입력합니다. 알고리즘에 따른 키 길이는 다음과 같습니다.

* AES: 16자(128비트), 24자(192비트), 32자(256비트) 중 선택
* RSA: 128자(1024비트), 256자(2048비트) 중 선택

암호화 키 길이는 암호 알고리즘이 요구하는 키의 길이를 8로 나눠 바이트로 환산한 값입니다.

**DATA**

복호화할 바이너리 데이터

선택 매개변수

**IV**

CBC와 같이 초기화 벡터(IV, Initial Vector)가 필요한 운영 모드를 사용할 때 바이너리 값

#### 사용 예

다음 쿼리문을 [encrypt()](https://docs.logpresso.com/ko/query/encrypt-function) 사용 예와 비교해 보십시오.

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