

# Encryption Functions

## Encryption Functions

### MD5(String s)

Calculates an MD5 checksum for the string.

### SHA1(String s)

Calculates an SHA-1 checksum for the string.

### SHA256(String s)

Calculates an SHA-256 checksum for the string.

### SHA384(String s)

Calculates an SHA-384 checksum for the string.

### SHA512(String s)

Calculates an SHA-512 checksum for the string.

### DSA(Number size)

Generates a [DSA](#) key pair of the given size.

### RSA(Number size)

Generates a [RSA](#) key pair of the given size.

### EC(Number size)

Generates a [Elliptic Curve](#) key pair of the given size.

### <Digest>with<Encryption>Sign(Object o,String key)

Computes a signature for the given object with the given private key using the given message digest with the given signature algorithm.

The following combinations are supported:

- NONEwithRSA
- MD2withRSA
- MD5withRSA
- SHA1withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA
- NONEwithDSA
- SHA1withDSA
- NONEwithECDSA
- SHA1withECDSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

#### Example

```
SELECT SHA256withRSASign("Hello World", "30820154020100300D...") FROM Stream
=> 51DC22BAFD51B112C72...
```

### <Digest>with<Encryption>Verify(Object o, String signature, String key)

- Encryption Functions
  - MD5(String s)
  - SHA1(String s)
  - SHA256(String s)
  - SHA384(String s)
  - SHA512(String s)
  - DSA(Number size)
  - RSA(Number size)
  - EC(Number size)
  - <Digest>with<Encryption>Sign(Object o, String key)
  - <Digest>with<Encryption>Verify(Object o, String signature, String key)

Verifies the signature for the given object with the given public key using the given message digest with the given signature algorithm.

The following combinations are supported:

- NONEwithRSA
- MD2withRSA
- MD5withRSA
- SHA1withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA
- NONEwithDSA
- SHA1withDSA
- NONEwithECDSA
- SHA1withECDSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

#### Example

```
SELECT SHA256withRSAVerify("Hello World", "51DC22BAFD51B112C72...",  
"305C300D06092A8648...") FROM Stream  
=> true
```