



CryptoTools 3.0 API



Table of contents

TABLE OF CONTENTS	2
OBJECTS, METHODS AND ATTRIBUTES	3
ATTRIBUTES.....	3
<i>Key</i>	<i>3</i>
<i>Result.....</i>	<i>3</i>
<i>IV.....</i>	<i>3</i>
METHODS	3
<i>Encrypt.....</i>	<i>3</i>
<i>Decrypt.....</i>	<i>3</i>
<i>EncryptText.....</i>	<i>4</i>
<i>DecryptText.....</i>	<i>4</i>
<i>EncryptFile</i>	<i>4</i>
<i>DecryptFile</i>	<i>5</i>
<i>DeriveKeyFromPassword.....</i>	<i>5</i>



Objects, methods and attributes definitions

This section describes the methods and attributes of all the encryption and encoding objects available in the CryptoTools package. A list of all objects will that implement it will be provided.

Attributes

Key

The Key attribute is implemented by the following objects:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)

Result

The Result attribute is implemented by all encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)
- CryptoMD5 (MD5 Hashing algorithm)

IV

The IV attribute is implemented by the following two algorithms:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)

Methods

Encrypt

The Encrypt method is available in all four encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)
- CryptoMD5 (MD5 Hashing algorithm)

The Encrypt method encrypts a binary block of data and stores the result in the Result attribute.

Decrypt

The Decrypt method is available in the following encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)



The Decrypt method decrypts a binary block of data that was produced by a call to the Encrypt method. To decrypt the data, the Key attribute must be set to the same key that was used to encrypt the data.

Decrypt is not available for MD5 because the result produced by a hashing function is impossible to decrypt.

EncryptText

The EncryptText method is available in all four encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)
- CryptoMD5 (MD5 Hashing algorithm)

This method is a specialization of the Encrypt method. Instead of encrypting a block of binary data, the EncryptText function encrypts text. This function does not support UNICODE standard.

The EncryptText is not available for C and C++, as text is an array of bytes.

DecryptText

The DecryptText method is available in the following encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)

The Decrypt text method returns the original text string. The result can also be accessed as binary data through the Result attribute.

Decrypt is not available for MD5 because the result produced by a hashing function is impossible to decrypt.

EncryptFile

The EncryptFile method is available in all four encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)
- CryptoMD5 (MD5 Hashing algorithm)



Encrypt file is a helper function wrapping the functionalities of the Encrypt method plus all the code necessary to open the source file and create and save the result into the target file.

The EncryptFile method of the CryptoMD5 object returns the hash as a text string. The resulting hash can also be accessed through the Result attribute.

DecryptFile

The DecryptFile method is available in the following encryption components:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)
- CryptoBase64 (Text encoding)

DecryptFile will read the content of an encrypted file, decrypt it and save the result to the target file.

This function is not available for CryptoMD5 because hashing results are impossible to decrypt.

DeriveKeyFromPassword

The DeriveKeyFromPassword method is implemented by the following two algorithms:

- CryptoDES (Data Encryption Standard)
- CryptoTripleDES (Three keys DES)

This function generates an encryption key from the password it receives in parameter. This is a very helpful function for languages where it is complicated to work with byte arrays.

The following steps generate the encryption key:

1. The password is converted to a bytes array using ASCII characters mapping.
2. The salt bytes array, if not null, is concatenated to the password byte array.
3. The resulting bytes array is then hashed N times using MD5 hashing algorithm.

The resulting 128 bits hash is split in two parts, K1 and K2. For the DES encryption object, the key is set to the first part K1. For TripleDES, both parts are concatenated in the following manner: K1+K2+K1, to form the encryption key. This type of key, for TripleDES, is sometime called 2DES.