# ifEVPCipher

## Implemented By

- roEVPCipher

## Supported Methods

- Setup(encrypt as Boolean, format as String, key as String, iv as String, padding as Integer) as Integer
- Reinit() as Integer
- Process(bytes as Object) as Object
- Update(bytes as Object) as Object
- Final() as Object

## Description of Methods

### Setup(encrypt as Boolean, format as String, key as String, iv as String, padding as Integer) as Integer

Setup and initialize a new cipher context. The Setup function takes the following parameters:

- encrypt - true for encryption, false for decryption
- format - cipher format string, from openssl, listed at roEVPCipher
- key - hex-encoded key
- iv - hex-encoded initialization vector (can be empty string)
- padding - 1 to use standard padding, 0 for no padding

Returns 0 on success or non-zero on failure.

### Reinit() as Integer

Reinitialize an existing cipher context.  This can be called to reuse an existing roEVPCipher object to encrypt new data.  Returns 0 on success or non-zero on failure.

### Process(bytes as Object) as Object

The parameter should be an roByteArray.  The data in the array is encrypted or decrypted. Returns an roByteArray containing the result.

```
x = evp.Process(bytes)
```

is equivalent to

```
evp.Reinit()
x = evp.Update(bytes)
x = x + evp.Final()
```

### Update(bytes as Object) as Object

The parameter should be an roByteArray.  The data in the array is encrypted or decrypted.  Returns an roByteArray containing a subset of the

result.  Some or all of the result may not be returned until the next call to Update().

### Final() as Object

Signals that all data has been submitted by previous calls to Update().  Returns the last remaining encrypted or decrypted bytes.