rules.sonarsource.com

# Swift static code analysis: Neither DES (Data Encryption Standard) nor DESede (3DES) should be used

2 minutes

According to the US National Institute of Standards and Technology (NIST), the Data Encryption Standard (DES) is no longer considered secure:

> Adopted in 1977 for federal agencies to use in protecting sensitive, unclassified information, the DES is being withdrawn because it no longer provides the security that is needed to protect federal government information.
>
> Federal agencies are encouraged to use the Advanced Encryption Standard, a faster and stronger algorithm approved as FIPS 197 in 2001.

For similar reasons, RC2 should also be avoided.

## Noncompliant Code Example

```
let cryptor = try Cryptor(operation: .encrypt, algorithm: .des, options: .none, key: key, iv: []) // Noncompliant

let crypt = CkoCrypt2()
crypt.CryptAlgorithm = "3des" // Noncompliant
```

## Compliant Solution

```
let cryptor = try Cryptor(operation: .encrypt, algorithm: .aes, options: .none, key: key, iv: []) // Compliant

let crypt = CkoCrypt2()
crypt.CryptAlgorithm = "aes" // Compliant
```

## See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- MITRE, CWE-326 - Inadequate Encryption Strength
- MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm
- SANS Top 25 - Porous Defenses
- Derived from FindSecBugs rule DES / DESede Unsafe

## Deprecated

This rule is deprecated; use {rule:swift:S5547} instead.