keep coding

Desarrollo Seguro iOS

Bootcamp de desarrollo Mobile

CryptoKit

Introducción

- A partir de iOS 13
- Validación FIPS 140-2
- Capa de abstracción

Cryptokit vs CommonCrypto

keep coding

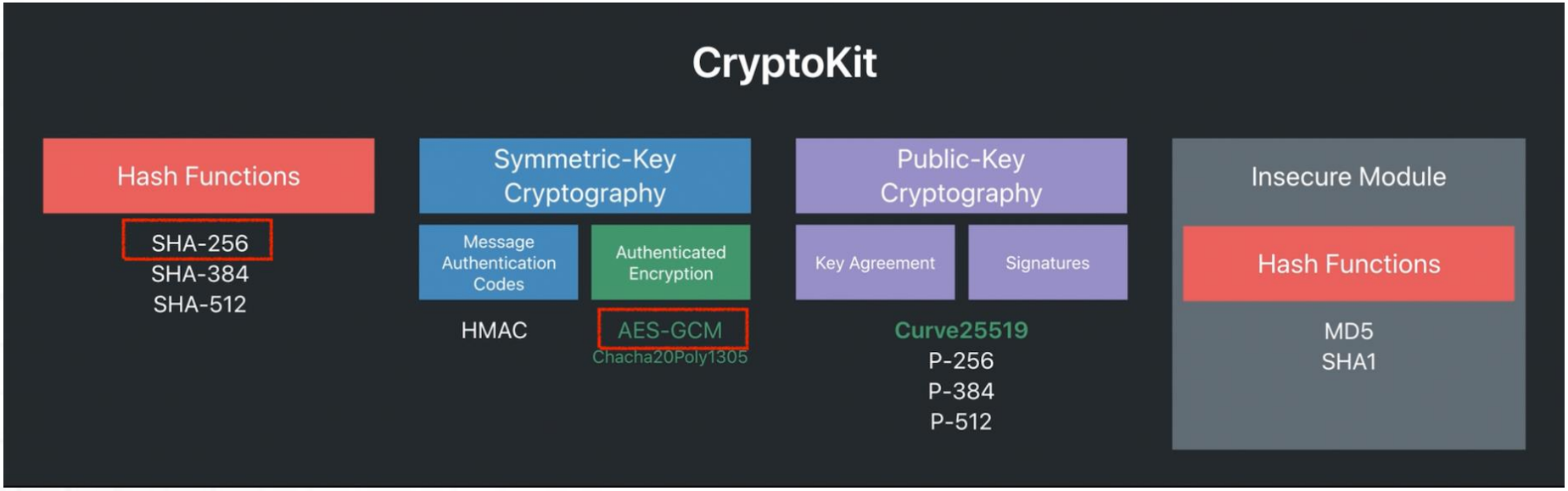
Cryptokit

- iOS 13
- Alto nivel
- Swift

CommonCrypto

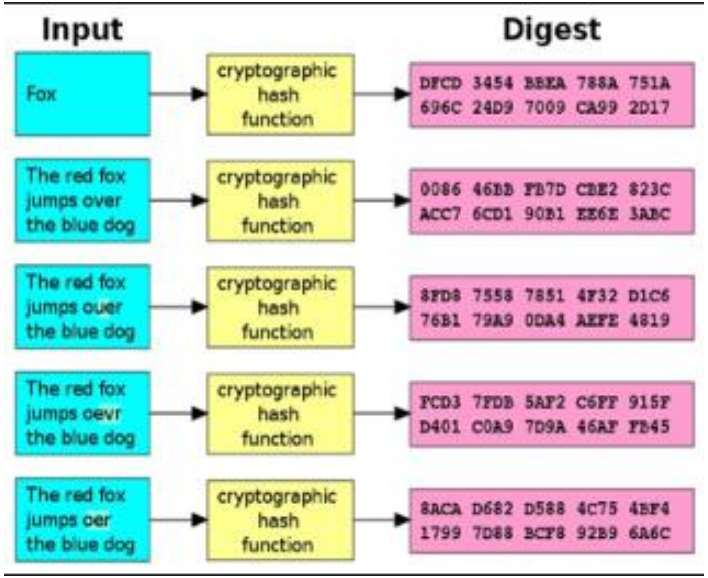
- Legacy
- Operaciones granulares
- Swift, C y Objective-C

Cryptokit


CryptoKit
Hash Functions
SHA-256
SHA-384
SHA-512
Symmetric-Key Cryptography
Message Authentication Codes
Authenticated Encryption
HMAC
AES-GCM
Chacha20Poly1305
Public-Key Cryptography
Key Agreement
Signatures
Curve25519
P-256
P-384
P-512
Insecure Module
Hash Functions
MD5
SHA1

Funciones hash

- Unidireccionales
- Deterministas
- Eficientes y rápidas
- Sin colisiones



Familia SHA

Función Hash	Tipos	Grado de Seguridad	Vulnerabilidades
SHA-0 y SHA-1	SHA-160	Bajo	Vulnerable a ataques de colisión
SHA-2	SHA-224 SHA-256 SHA-384 SHA-512	Medio	Vulnerables a ataques de extensión de cadena
SHA-3	SHA3-224 SHA3-256 SHA3-384 SHA3-512	Alto	Sin vulnerabilidades significativas

www.keepcoding.io cursos@keepcoding.io (+34) 916 33 1779