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

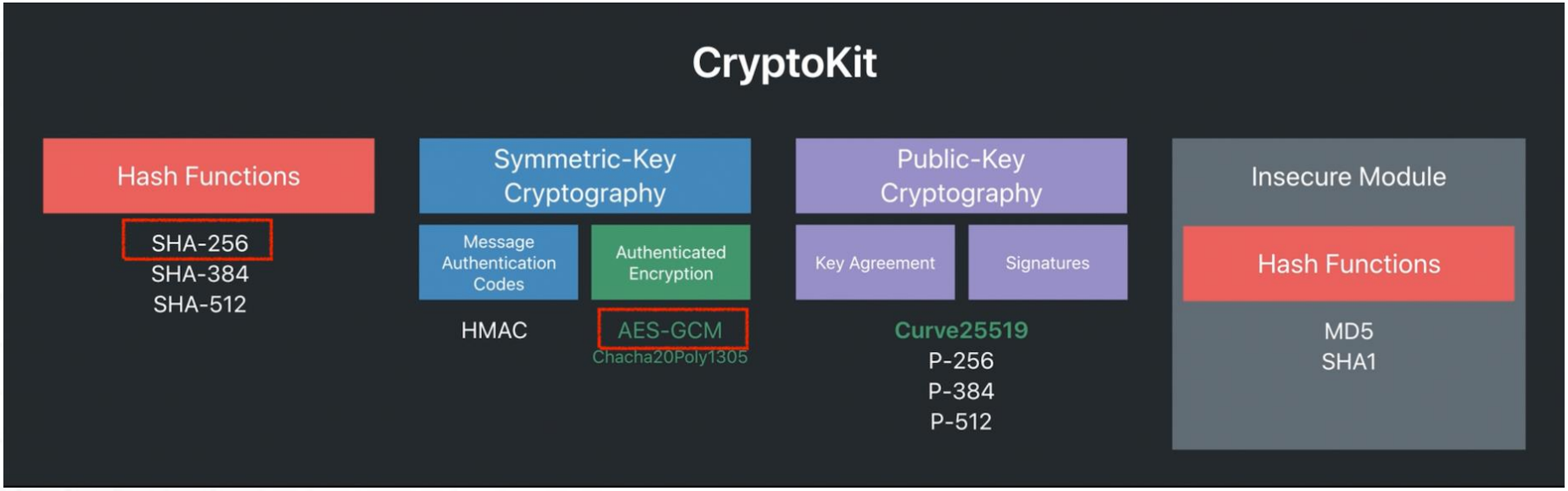
Cryptokit

- iOS 13
- Alto nivel
- Swift

CommonCrypto

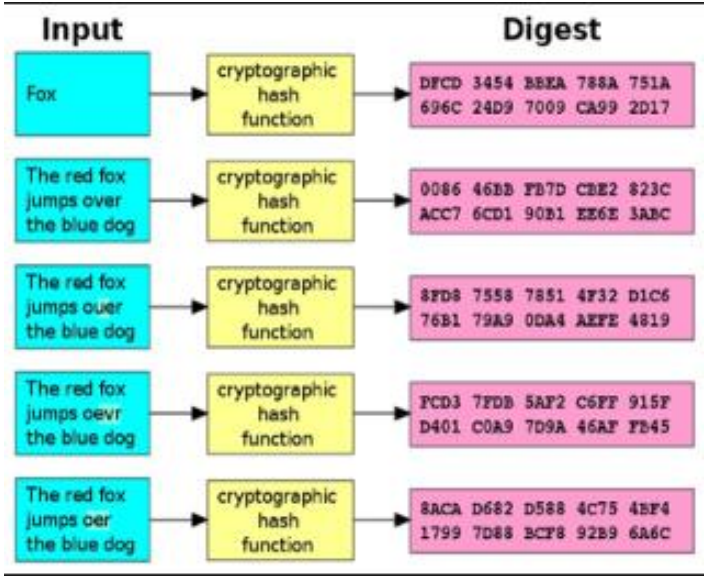
- Legacy
- Operaciones granulares
- Swift, C y Objective-C

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

Base64

Mensaje	“mi”															
ASCII	m → 109								i → 105							
Binario (1 byte)	0	1	1	0	1	1	0	1	0	1	1	0	1	0	0	1
Conteo	-	64	32	-	8	4	-	1	-	64	32	-	8	-	-	1
Índices	011011 – 010110 – 1001															
Índices con 6 bits	011011 – 010110 – 100100 – 000000															
Base64	011011 (27) → b 010110 (22) → W 100100 (36) → k 000000 (0) → =															

Index	Binary	Char
0	000000	A
1	000001	B
2	000010	C
3	000011	D
4	000100	E
5	000101	F
6	000110	G
7	000111	H
8	001000	I
9	001001	J
10	001010	K
11	001011	L
12	001100	M
13	001101	N
14	001110	O
15	001111	P

Index	Binary	Char
16	010000	Q
17	010001	R
18	010010	S
19	010011	T
20	010100	U
21	010101	V
22	010110	W
23	010111	X
24	011000	Y
25	011001	Z
26	011010	a
27	011011	b
28	011100	c
29	011101	d
30	011110	e
31	011111	f

Index	Binary	Char
32	100000	g
33	100001	h
34	100010	i
35	100011	j
36	100100	k
37	100101	l
38	100110	m
39	100111	n
40	101000	o
41	101001	p
42	101010	q
43	101011	r
44	101100	s
45	101101	t
46	101110	u
47	101111	v

Index	Binary	Char
48	110000	w
49	110001	x
50	110010	y
51	110011	z
52	110100	0
53	110101	1
54	110110	2
55	110111	3
56	111000	4
57	111001	5
58	111010	6
59	111011	7
60	111100	8
61	111101	9
62	111110	+
63	111111	/

Conversión a hexadecimal

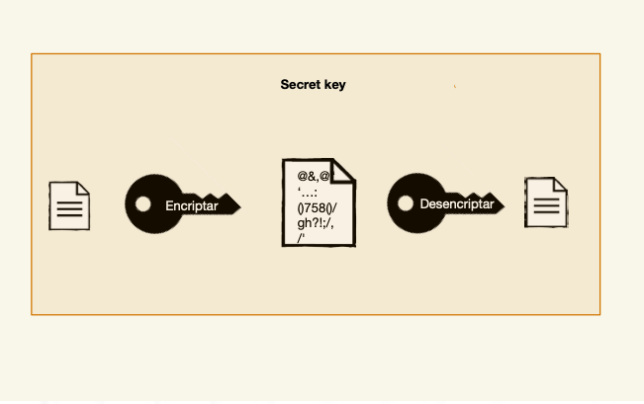
Mensaje	“mi”															
ASCII	m → 109								i → 105							
Binario (1 byte)	0	1	1	0	1	1	0	1	0	1	1	0	1	0	0	1
Conteo	-	64	32	-	8	4	-	1	-	64	32	-	8	-	-	1
Índices	0110110101101001															
Índices con 4 bits	0110 –1101 – 0110 – 1001															
Hexadecimal	0110 (6) → 6 1101 (13) → D 0110 (6) → 6 1001 (9) → 9															

Denary/Decimal	Binary	Hexadecimal
Base 10 Number System	Base 2 Number System	Base 16 Number System
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Encriptación simétrica y asimétrica

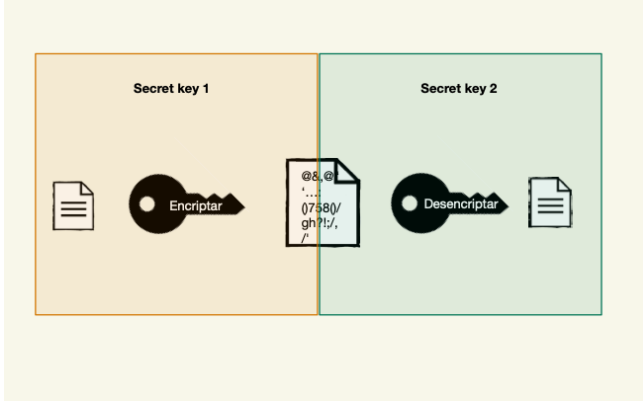
Simétrica

- Única clave
- Más rápida

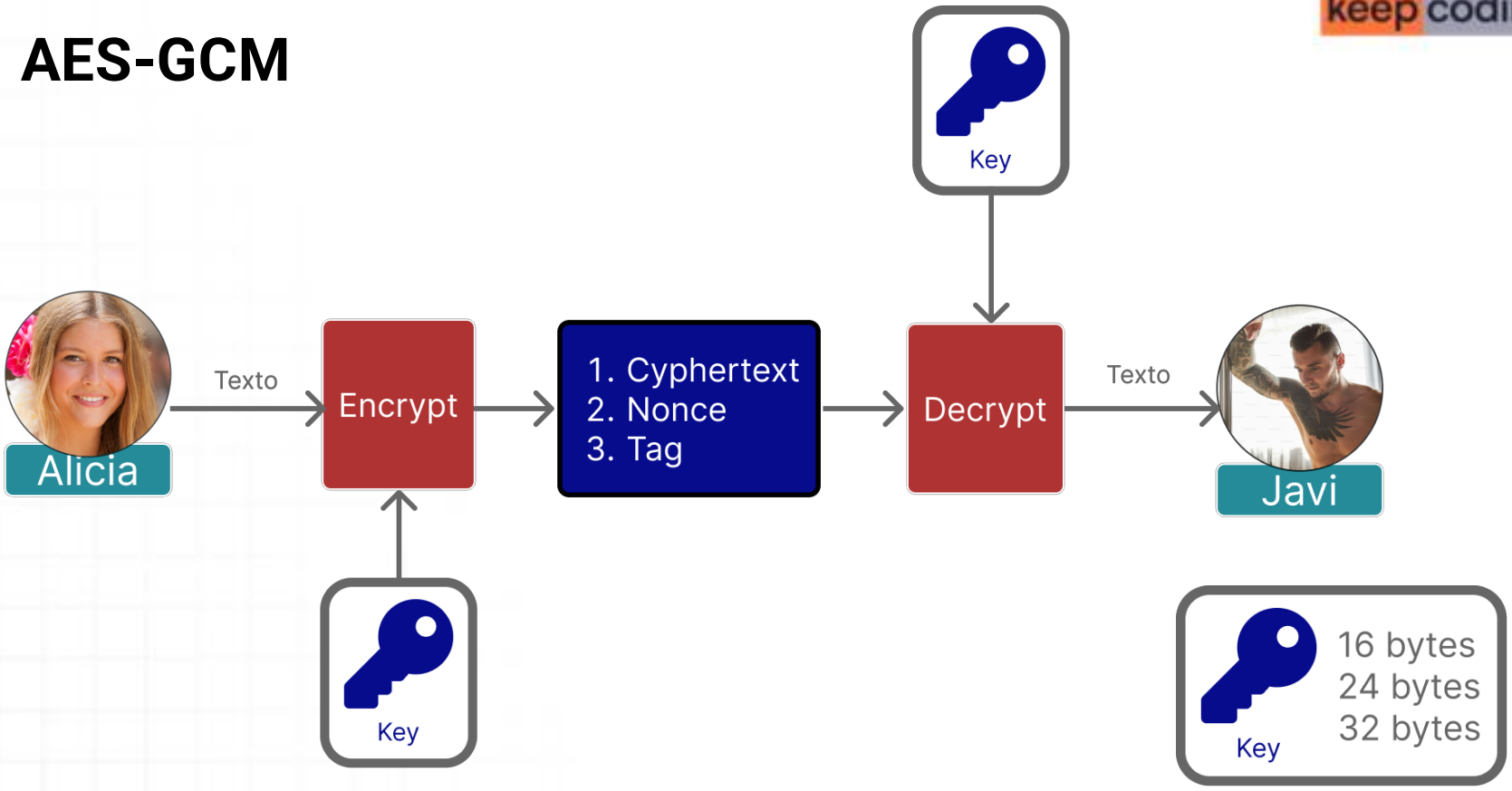


Asimétrica

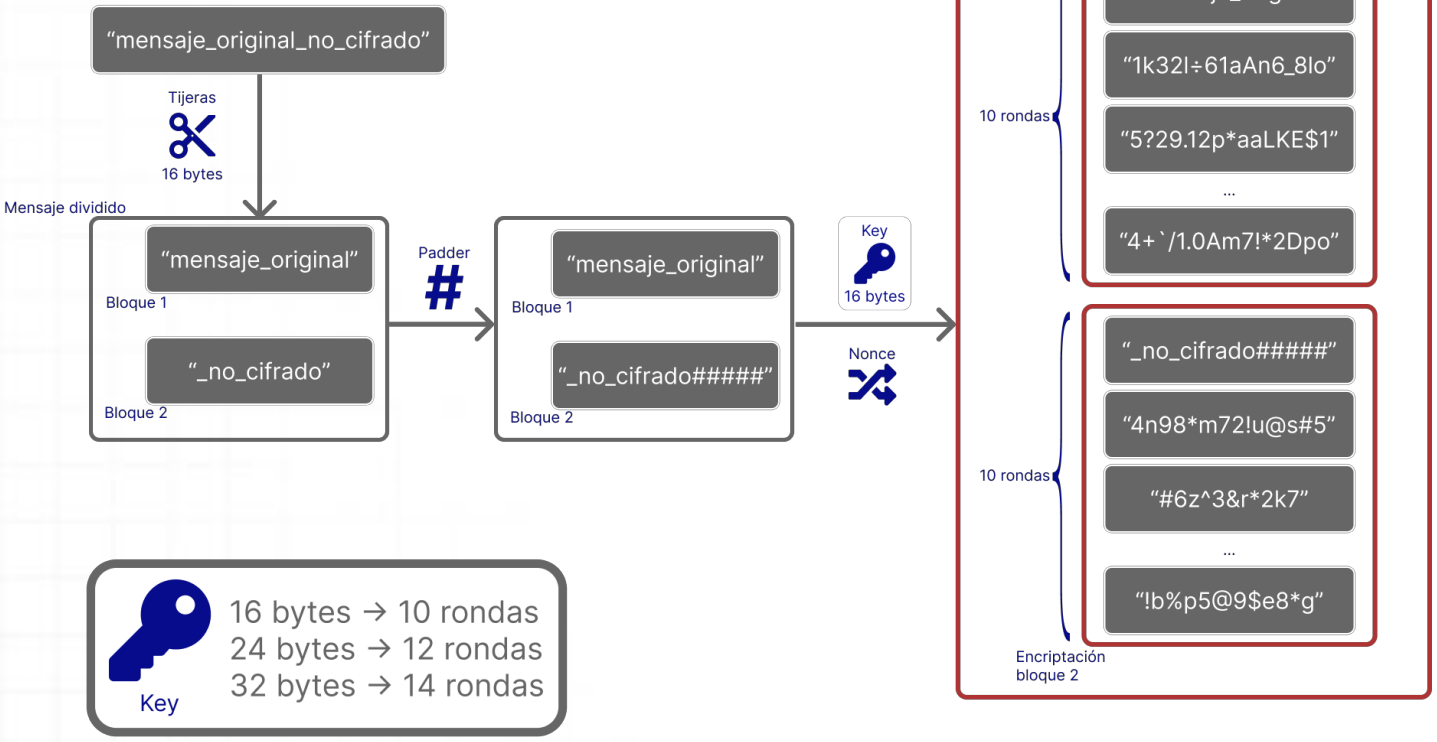
- Dos claves
- Computacionalmente costosa



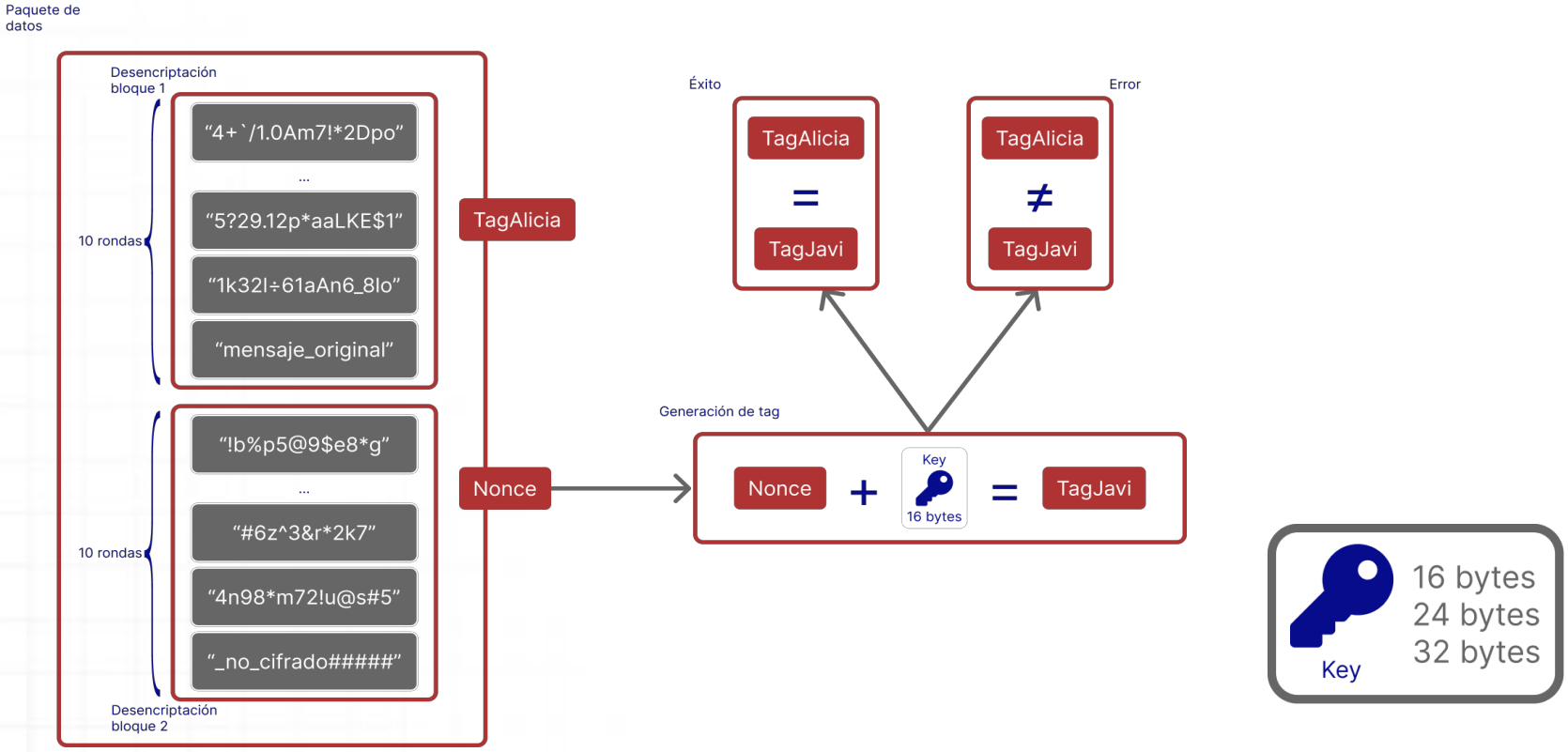
AES-GCM


Key
Alicia
Texto
Encrypt
1. Cyphertext
2. Nonce
3. Tag
Decrypt
Texto
Javi
Key
Key
16 bytes
24 bytes
32 bytes

Encriptación AES-GCM



Desencriptación AES-GCM



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