



PROYECTO: CRIPTOLOGÍA SIMÉTRICA APLICADA A LA CIBERSEGURIDAD (CRIPTO-SAC).

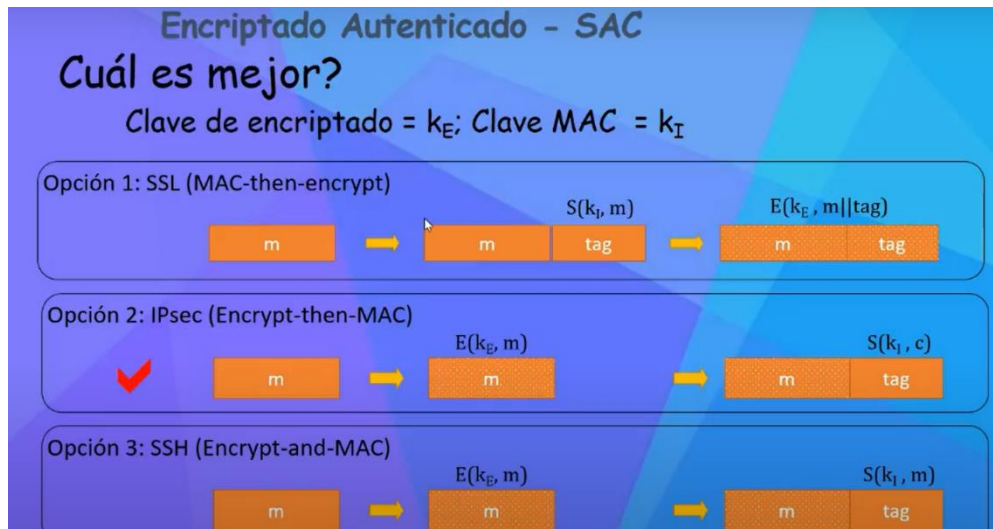
PDS
FIE 21
Cripto
Simétrica



DIRECTOR: Lic. EDITH GARCÍA

Objetivos del proyecto: investigar dentro de la criptografía simétrica aquellos algoritmos de clave secreta que cifran y autentican datos con un mismo esquema, logrando así la confidencialidad, autenticidad e integridad de la información, alcanzando también todas las características ideales de seguridad simplicidad y velocidad en un único algoritmo.

Imágenes ilustrativas:



Encriptado Autenticado - SAC
Performance
From Crypto++ 5.6.0 [Wei Dai]

AE Cipher	Code Size	Speed (MB/sec)	Raw Cipher	Raw Speed
AES/GCM	Large	108	AES/CTR	139
AES/CCM	smaller	61	AES/CBC	109
AES/EAX	smaller	61	AES/CMAC	109
AES/OCB*	small	129	HMAC/SHA1	147

* OCB mode may have patent issues. Speed extrapolated from Ted Kravitz's results.