

Certificación de personas **CriptoCert**

*I Encuentro del ENS.
Tendencias y Políticas de Seguridad*

*Alfonso Muñoz y Raúl Siles
Fundadores de **CriptoCert**
18 de junio de 2019*



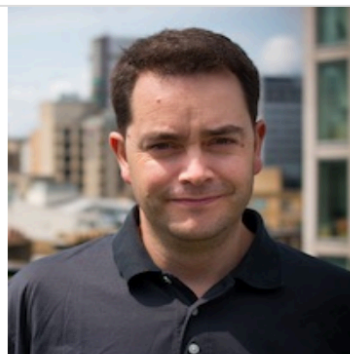
El equipo fundador de **CriptoCert**



DR. JORGE RAMIÓ

Docente y criptógrafo

Docente con más de 25 años de experiencia en el campo de la criptografía. Reconocido criptógrafo, ha recibido numerosos reconocimientos por la creación de la red temática Criptored, herramientas, proyectos criptográficos y asesoramiento a empresas.



D. RAÚL SILES

Experto en seguridad informática

Fundador y analista de seguridad senior de DinoSec. Durante casi 20 años, ha aplicado su experiencia en la realización de servicios de seguridad técnicos avanzados y ha innovado soluciones ofensivas y defensivas para grandes empresas y organizaciones en múltiples industrias de todo el mundo.



DR. ALFONSO MUÑOZ

Experto en seguridad informática y criptógrafo

Durante 15 años ha trabajado como especialista en seguridad informática y criptógrafo en proyectos avanzados con multinacionales y organismos públicos. Su labor ha sido reconocida con numerosos premios y menciones.



Índice

1. CriptoCert: *Elevator pitch*
2. Presente / Tendencias
 3. Wi-Fi WPA3.
 4. Adiantum.
 5. Stegomalware.
6. Futuro
 7. Criptografía ligera (IoT).
 8. Criptografía homomórfica.
 9. Criptografía post-cuántica.
10. Conclusiones

1. **CriptoCert:** *Elevator pitch*



www.cryptocert.com

[@cryptocert](https://twitter.com/cryptocert)

info@cryptocert.com

2. Presente / Tendencias



3. Wi-Fi WPA3



- Cifrado en tránsito
- WPA3-Personal: Simultaneous Authentication of Equals (SAE)
 - PAKE (Password-Authenticated Key Exchange/Agreement): Dragonfly
- WPA3-Enterprise: 192-bit security mode
 - Consistencia criptográfica
 - AES GCM-256, HMAC-SHA384, ECDHE/ECDSA 384-bit...
- Wi-Fi Enhanced Open™: Opportunistic Wireless Encryption (OWE)
 - Diffie-Hellman (DH): Finite fields or elliptic curve cryptography (FFC or ECC)
- Wi-Fi Easy Connect™: Wi-Fi Device Provisioning Protocol (DPP)

4. Adiantum



MARVEL



- **Adamantium**
- Guía CCN-STIC 453G: “Guía práctica de seguridad en dispositivos móviles Android 9” (marzo 2019)
- “Introducing Adiantum: Encryption for the Next Billion Users”
 - <https://security.googleblog.com/2019/02/introducing-adiantum-encryption-for.html> (Feb 2019)
- Cifrado en reposo
- Para todos los dispositivos móviles Android...
 - Sin aceleración criptográfica (CPU sin AES): gama baja
 - Android Go, IoT (relojes, TVs)... (ARM Cortex-A7)
 - Android 9+ & FDE o FBE & 32 o 64 bits ARM
 - Impacto mínimo en el rendimiento con robustez similar



4. Adiantum: Detalles



- Dispositivos móviles actuales (utilizan AES)
 - ARMv8 Cryptography Extensions o x86-based device with AES-NI
 - Tamaño plaintext = ciphertext = sector disco (512 ó 4.096 bytes)
 - Length-preserving: AES-XTS o AES-CBC-ESSIV
 - Imposibilidad de usar AES-GCM o RFC7539 (ChaCha20 y Poly1305)
 - No hay espacio para almacenar un IV (o nonce) dinámico o MACs (integridad)
 - AES-XTS es lento: Velocidad de Adiantum x5 vs. AES-256-XTS (4 KB)
 - Cifrado en Android obligatorio por defecto desde Android 6+
 - AES con un rendimiento superior a 50MiB/segundo
- Adiantum: hash (NH + Poly1305) & cifrado flujo (XChaCha12) veloces
 - Variante para mensajes más pequeños: HPolyC

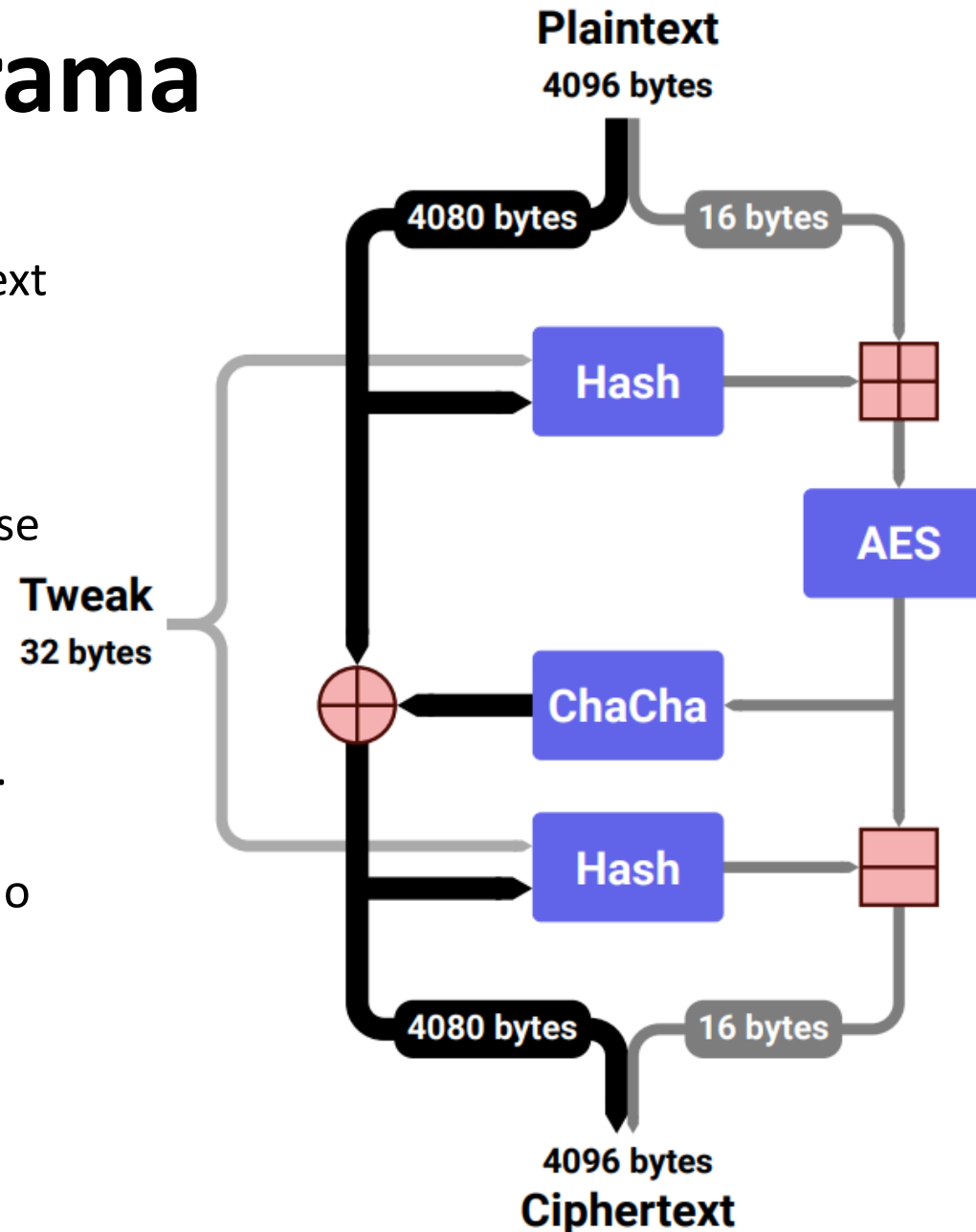
<https://source.android.com/security/encryption/adiantum>

<https://github.com/google/adiantum>

<https://eprint.iacr.org/2018/720.pdf>

4. Adiantum: Diagrama

- Difusión: El cambio de 1 bit en el plaintext cambia todo el bloque de ciphertext
- Hashes: NH & Poly1305
 - Nonce para ChaCha
- Tweak: Asegurar que distintos sectores se cifran de forma diferente
- ChaCha12 in length-preserving mode (HCTR & HCH)
- Una invocación de AES-256 (16 bytes vs. 4.096 bytes del sector)
- Red de Feistel: las operaciones de cifrado y descifrado son idénticas y reversibles



5. Tendencias: No solo criptografía



EC3 - SPACE > Criminal Use of Information Hiding (Steganography) >>

Welcome!



STEGANOGRAPHY



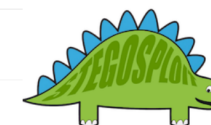
to cybercriminals exploitation

Initiative under Europol EC3:

Criminal Use of Information Hiding (CUIng)

Recently, various types of information hiding techniques (like steganography) are increasingly utilized by the current malware to hide its existence, communication attempts and confidential data exfiltration. This new trend is highlighted by the latest examples of malicious software that have information hiding capabilities, e.g., *Hammertoss*, *Stegoloader*, *Regin* or *Duqu*. These techniques have been utilized by cybercriminals but were also found useful by spies (e.g., the discovery of the Russian spy ring in US in 2010) and terrorists (arrest of one of al Qaeda's members in Berlin with video files containing hidden information in 2012). Information hiding has been also proved useful as a tool for insiders for sensitive data exfiltration.

Stegosploit



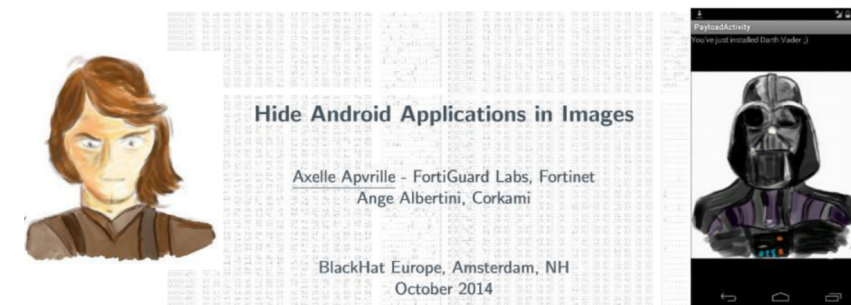
Exploit Delivery via Steganography and Polyglots

by Saumil Shah - saumil@net-square.com, [@therealsaumil](https://twitter.com/therealsaumil)

June 2015

TL;DR:

Stegosploit creates a new way to encode "drive-by" browser exploits and deliver them through image files. These payloads are undetectable using current means. This paper discusses two broad underlying techniques used for image based exploit delivery - Steganography and Polyglots. Drive-by browser exploits are steganographically encoded into JPG and PNG images. The resultant image file is fused with HTML and Javascript decoder code, turning it into an HTML+Image polyglot. The polyglot looks and feels like an image, but is decoded and triggered in a victim's browser when loaded.



CCN-STIC-438 Esteganografía

<https://www.ccn-cert.cni.es/series-ccn-stic/400-guias-generales/115-ccn-stic-438-esteganografia/file.html>

Esteganografía, stegomalware y APTs

5. Tendencias: Stegomalware (2019)



Eugene Kaspersky @e_kaspersky · 5 jun.

Forget about #cryptography - #steganography is the new black for cyberespionage and the #PLATINUM APT group is here to use it to fly under #cybersecurity radars kas.pr/platinum via @securelist

 Traducir Tweet

Platinum is back

In June 2018, we came across an unusual set of samples spreading throughout South and Southeast Asian countries targeting diplomatic, gov...
securelist.com

Ursnif (Feb 2019)

OceanLotus APT Group (Abril 2019)

ScarCruft group APT (Mayo 2019)

Platinum APT Group (Junio 2019)

```

25 <!--1234567890--<body>
26 <table align="center" bgcolor="white" border="0" cellpadding="4" rules="no
27     <tr align="center" bgcolor="white" valign="middle">
28         <td bgcolor="white" align="center" colspan="1" rowspan="1"></td>
29         <td align="center" bgcolor="white" colspan="1" rowspan="1"></td>
30         <td bgcolor="white" align="center" colspan="1" rowspan="1"></td>
31         <td align="center" bgcolor="white" colspan="1" rowspan="1"></td>
32         <td bgcolor="white" align="center" colspan="1" rowspan="1"></td>
33         <td align="center" colspan="1" bgcolor="white" rowspan="1"></td>
34         <td bgcolor="white" align="center" colspan="1" rowspan="1"></td>
35         <td bgcolor="white" rowspan="1" align="center" colspan="1"></td>
36         <td align="center" rowspan="1" colspan="1" bgcolor="white"></td>
37         <td colspan="1" bgcolor="white" align="center" rowspan="1"></td>
38     </tr>
39 </table>
40 <table cellspacing="0" width="100" bgcolor="white" frame="void" align="cen

```

[illegible]

<https://securelist.com/platinum-is-back/91135/>



6. Futuro



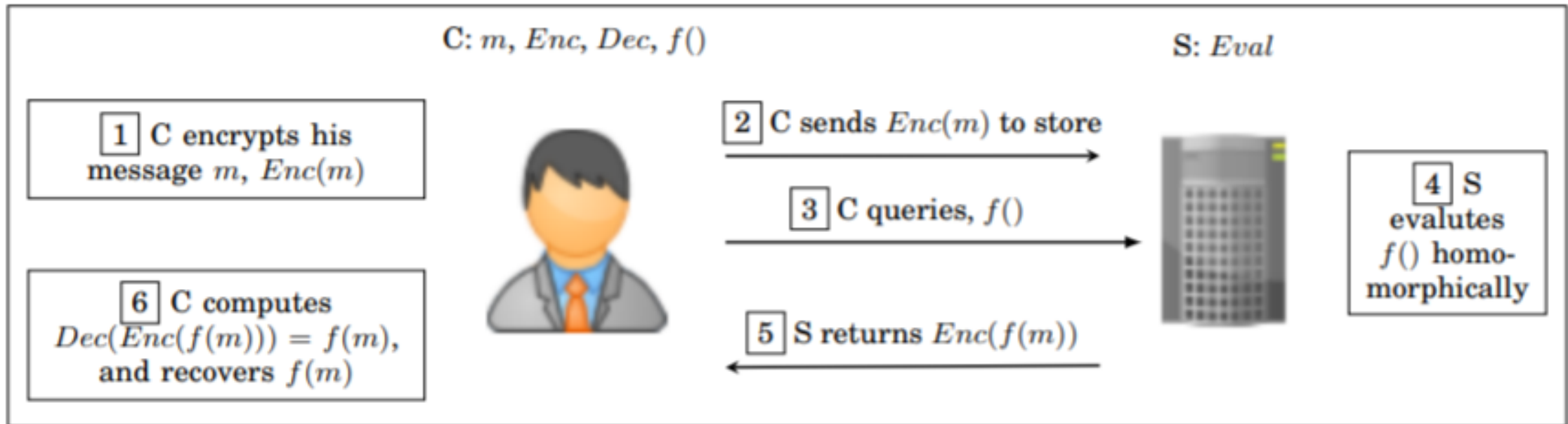
7. Futuro: Criptografía ligera (IoT)



- Lightweight cryptography (LWC)
- Dispositivos limitados pero interconectados (wireless)
 - IoT, redes de sensores, salud, etc.
- Requisitos: AEAD, hashing, diseño (buen rendimiento con poca memoria, CPU limitada, poca energía, mensajes cortos...), implementación HW y SW, resistencia frente a ataques laterales y a fallos, análisis de terceros...
- Algoritmos candidatos (Ago 2018)
 - 57 algoritmos propuestos: 56 seleccionados (Round 1)
 - <https://csrc.nist.gov/Projects/Lightweight-Cryptography/Round-1-Candidates>
 - Análisis (Nov 2019): fortalezas y debilidades criptográficas, costes de implementación, rendimiento, etc.
- NIST: Proceso de solicitud, evaluación y estandarización
 - <https://csrc.nist.gov/projects/lightweight-cryptography>

8. Futuro: Criptografía homomórfica

Computación de datos cifrados (Outsourcing de computación junto Privacidad)



PHE – Partially Homomorphic Encryption
SWHE – Somewhat Homomorphic Encryption
FHE - Fully Homomorphic Encryption

HELib - <https://github.com/shaih/HElib>

PALIDASE - <https://git.njit.edu/palisade/PALISADE>

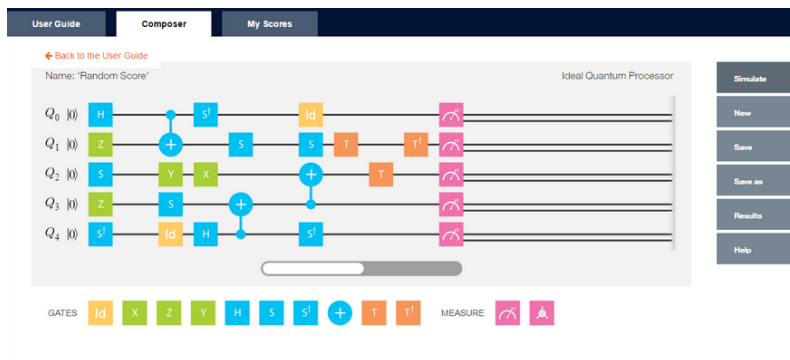
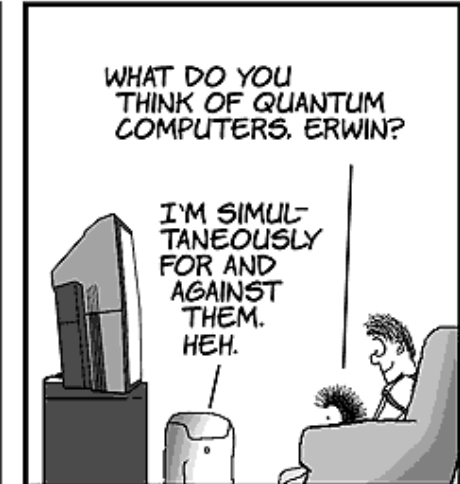
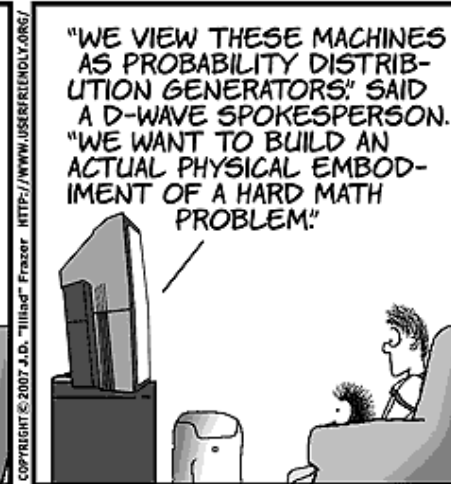
SEAL - <https://www.microsoft.com/en-us/research/project/simple-encrypted-arithmetic-library/>

9. Futuro: Computación cuántica y criptografía

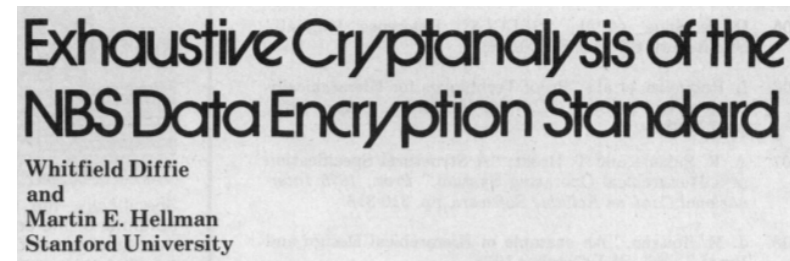


IBM Q System one (20 qubits)

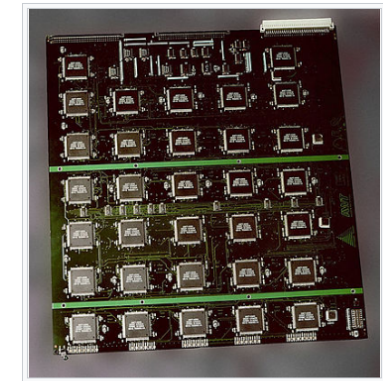
USER FRIENDLY by J.D. "Illiad" Frazer



<https://quantumexperience.ng.bluemix.net>



In 1977, Diffie and Hellman proposed a machine costing an estimated US\$20 million which could find a DES key in a single day



The EFF's US\$250,000 DES cracking machine contained 1,856 custom chips and could brute force a DES key in a matter of days — the photo shows a two-sided DES Cracker circuit board fitted with 64 Deep Crack chips

9. Futuro: Computación cuántica y criptografía

- ▶ When will a quantum computer be built?
 - 15 years, \$1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariani)
- ▶ Impact:
 - Public key crypto:
 - RSA
 - Elliptic Curve Cryptography (ECDSA)
 - Finite Field Cryptography (DSA)
 - Diffie-Hellman key exchange
 - Symmetric key crypto:
 - AES
 - Triple DES
 - Hash functions:
 - SHA-1, SHA-2 and SHA-3

Need larger keys
Need larger keys

Use longer output

Timeline

- ▶ Fall 2016 – formal Call For Proposals
- ▶ Nov 2017 – Deadline for submissions
- ▶ 3–5 years – Analysis phase
 - NIST will report its findings
- ▶ 2 years later – Draft standards ready
- ▶ Workshops
 - Early 2018 – submitter's presentations
 - One or two during the analysis phase

Recomendaciones:

- Algoritmos de clave pública (cifrado y firma)
 - **Criptografía postcuántica**
 - McEliece, con códigos Goppa, $n=6960$, $k=5413$, y $t=119$
 - NTRU, basado en retículos, versión de Stehlé-Steinfeld
 - XMSS (Extended Merkle Signature Scheme)
 - SPHINCS-256
- Algoritmos simétricos y autenticación (simétrica)
 - Cifrado en bloque: AES-256
 - Cifrado en flujo: Salsa20, clave de 256 bits
 - GCM: Galois Counter Mode, nonce de 96 bits, autenticador de 128 bits
 - Poly1305, MAC basado en AES

10. Conclusiones

- Criptografía clásica
 - Criptografía moderna
 - Criptografía futura
 - Esteganografía
-
- **Certificación de personas: CriptoCert**



CriptoCert

www.cryptocert.com

@cryptocert

info@cryptocert.com

Muchas gracias

