
# *Crypto Go*
# *Una herramienta didáctica para aprender criptografía jugando*

A.I. GONZÁLEZ-TABLAS FERRERES · M.I. GONZÁLEZ VASCO

uc3m | Universidad Carlos III de Madrid

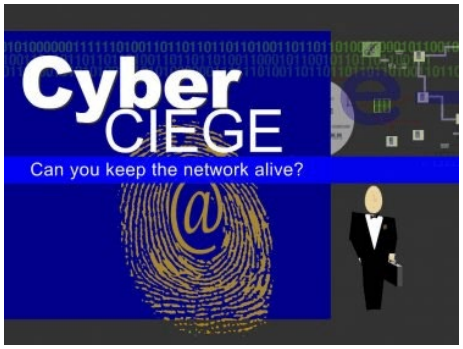
Universidad Rey Juan Carlos

RECSI 2022

Crypto Go HMAC EAX SALSA AES 20/20 FFX SHA-3

# Introducción

- Mayor respeto y uso de juegos “serios” en educación
- Particularmente relevante en el contexto de ciberseguridad (CTFs, CDXs,…)
- Tipologías variadas de juegos
  - CyberCIEGE
  - Elevation of Privilege
  - OWASP Cornucopia





# Nuestro Objetivo

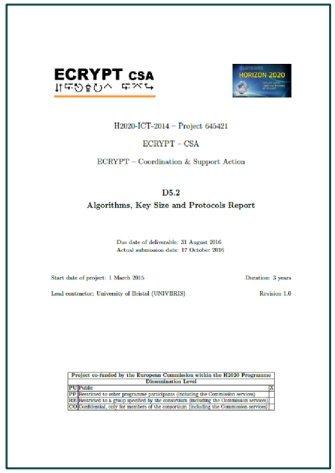
Proponer un juego de cartas sencillo, de mecánica rápida y sistema de puntuaciones simple

- ~ Burro
- Muy inspirado en SUSHI GO


Objetivo didáctico: que los jugadores sean capaces de reconocer cuáles son las primitivas y los esquemas criptográficos adecuados para cubrir ciertos objetivos de seguridad

- Criptografía simétrica (0-key, 1-key)
- Confidencialidad + Autenticación

Referencia esencial:
ECRYPT CSA: “D5.2 algorithms, key size and protocols report”, *H2020-ICT-2014)*, 2016.


ECRYPT CSA

H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D5.2
Algorithms, Key Size and Protocols Report

# Cartas criptográficas (1)

**NOMBRE ALGORITMO**

Descripción breve sin develar su nivel de seguridad

Color indicativo del tipo de algoritmo (primitiva/construcción combinada)

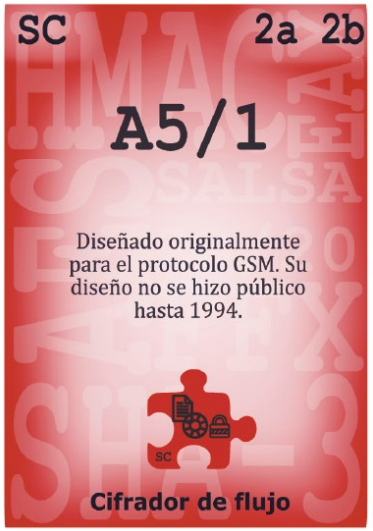

Mismo reverso para todas las cartas

# Cartas criptográficas (2)

**Cartas de Primitivas**


Cifradores de Bloque (CB)


Funciones Hash (H)




Cifradores de Flujo (SC)

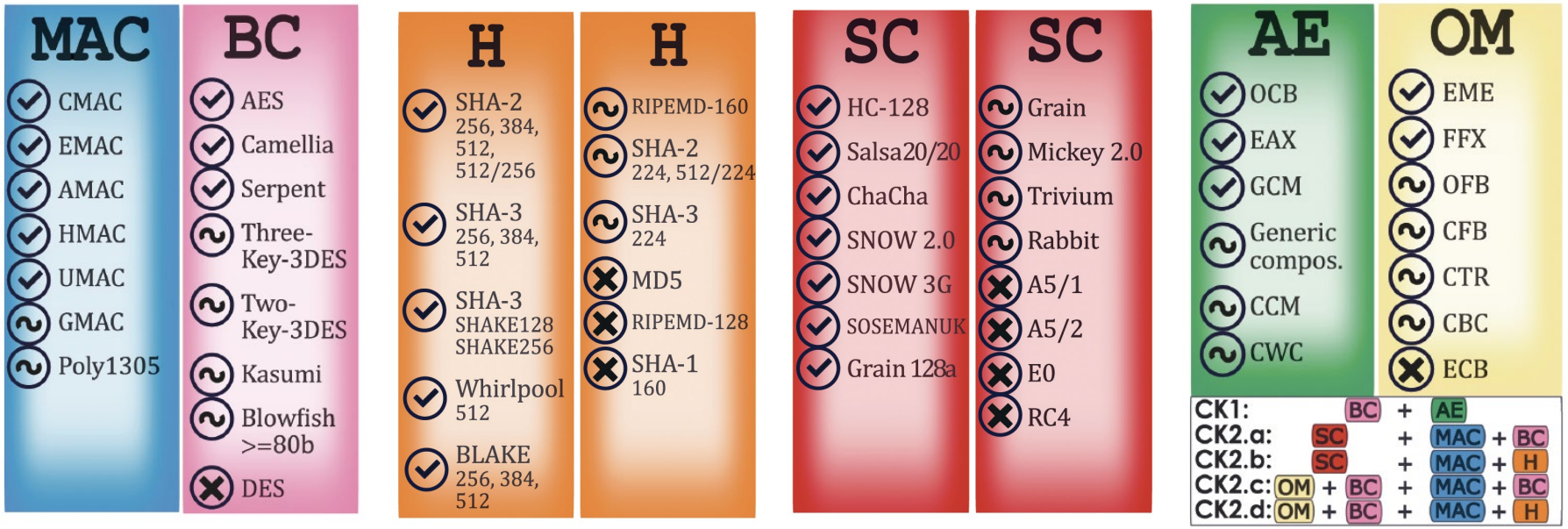
# Cartas criptográficas (3)

**Cartas para Construcciones Combinadas**




| Modos de Operación (OM) | Cifrado Autenticado (AE) | Funciones MAC (MAC) |
|---|---|---|
| BC + OM | AE + BC<br>(*OM + MAC*) | MAC + [BC OR H] |

# Cartas auxiliares



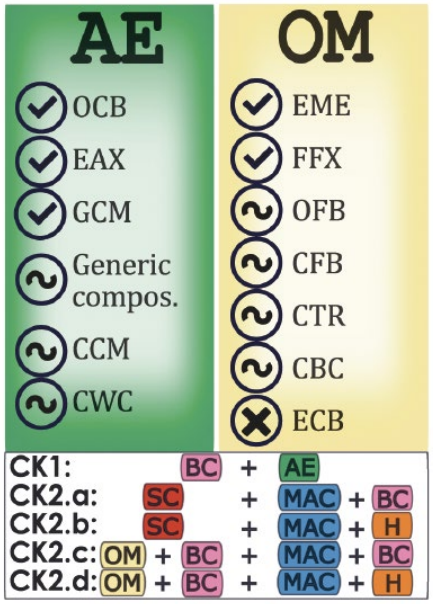

Future  Legacy  Not recommended

Cada jugador dispone de una copia personal

# Objetivos del juego

**Conseguir el mayor número de Crypto-Kits, combinando cartas criptográficas, con el mayor nivel de seguridad**

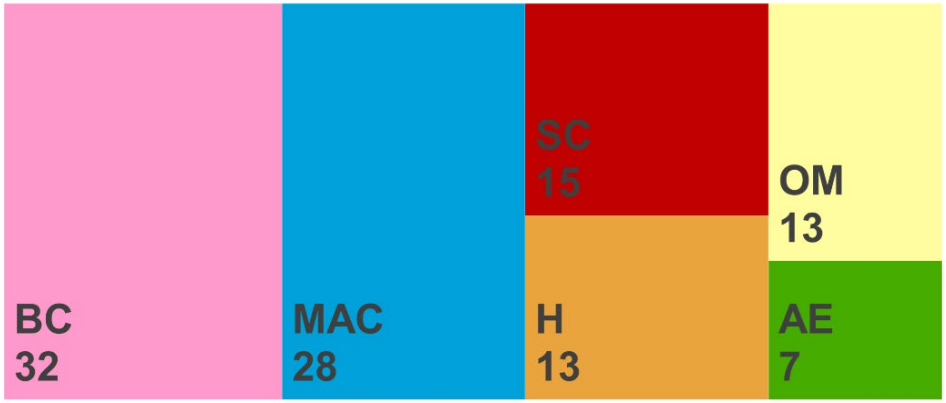
- **Crypto-Set**
  - CS1 (confidencialidad): (OM + BC) OR SC
  - CS2 (integridad + autenticación): MAC + (H OR BC)
  - CS3: (confidencialidad + integridad + autenticación): AE + BC
- **Crypto-Kit**: proporciona confidencialidad + autenticación
  - CK1: CS1 + CS2
  - CK2: CS3



# Mecánica del juego (1)

- Documento referencia contiene 54 primitivas y construcciones
- Baraja de 108 cartas + 16 cartas auxiliares
- Número de copias de cada algoritmo calculado según distribución de posibles construcciones de Crypto-Kits
- Hasta 8 jugadores
- Partidas de tres rondas

| Tipo de carta | BC | H | SC | OM | AE | MAC |
|---|---|---|---|---|---|---|
| Número de primitivas o construcciones en [2] | 7 | 10 | 15 | 8 | 7 | 7 |
| Copias de carta por primitiva o construcción en baraja | 4-5 | 1-2 | 1 | 1-2 | 1 | 4 |
| Número de cartas por tipo en baraja | 32 | 13 | 15 | 13 | 7 | 28 |



# Mecánica del juego (2)

- **Inicio de partida**: Se reparten a cada jugador 6 cartas. Resto boca abajo en mazo en el centro.
- **Ronda:** Cada jugador elige una carta de su mano y la "juega". Se pasa la mano al jugador siguiente, recibiendo otra.
- **Puntuando una ronda**: Solo puntúan las cartas que conforman un *Crypto-Kit*; con cierta "penalización" si hay cartas con seguridad media o baja
- **Fin de la partida y ganador(es) del juego**: Gana el jugador con mayor puntuación tras tres rondas.

Puntuación ajustada empíricamente para equilibrar posibilidades de ganar en varias rondas (se proponen tres)

# Uso del juego en contexto

- IMPORTANTE
- TONO, INTERACCIÓN Y CONTENIDO ADAPTADOS SEGÚN ASISTENTES

- REFUERZA
- MOTIVA

## Estructura del taller

- Presentación
- Charla
  - Conceptos necesarios
  - Explicación del juego Crypto Go
- Partida de Crypto Go

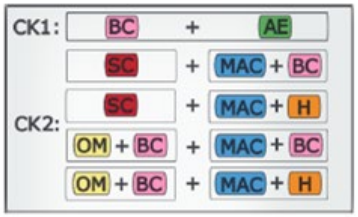
Necesidad de espacio con mobiliario móvil + medios de proyección
Recomendado un ponente por cada 15 estudiantes
Duración: 1 hora (más dependiendo de conocimientos previos) + explicación y tiempo de juego. Recomendado 2 horas - 2 horas y media.

# Charla

La criptografía se utiliza para hacer las comunicaciones "seguras", proporcionando CIA: Confidencialidad, Integridad, Autenticación


En criptografía simétrica los usuarios que se quieren comunicar de forma segura comparten una misma clave

Hay diferentes tipos de herramientas de criptografía simétrica, y diferentes herramientas concretas de cada tipo


Determinadas combinaciones de tipos de herramientas de criptografía simétrica consiguen las propiedades CIA


No todas las herramientas concretas son igual de seguras... de hecho, algunas son inseguras

**CIFRADORES DE FLUJO (STREAM CIPHERS)**
Toman un flujo continuo de datos y lo transforman en serie, mezclándose con una clave. El proceso puede revertirse... si se dispone de la clave.

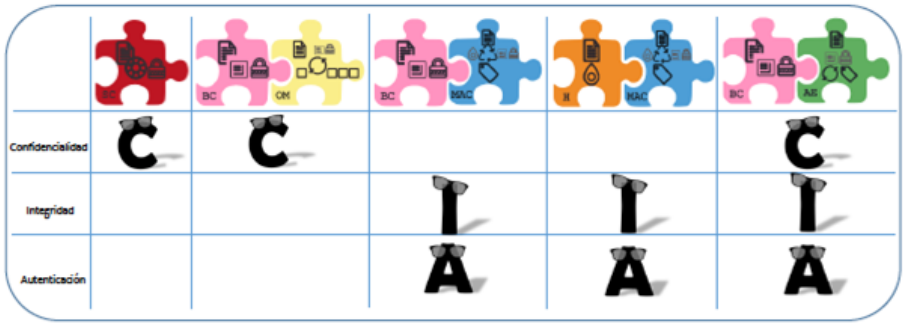
**CIFRADORES DE BLOQUE (BLOCK CIPHERS)**
Parten el mensaje en trocitos (bloques), que se transforman uno a uno, mezclándose con la clave. Se pueden "invertir" para, usando la clave, recuperar los bloques de partida.

**FUNCIONES RESUMEN (HASH FUNCTIONS)**
Toman un mensaje y lo resumen (condensan, comprimen, extraen su esencia...). Su acción es, en principio, irreversible...

**MODOS DE OPERACIÓN (OPERATION MODES)**
Un OM te dice cómo cifrar un mensaje largo con un BC (que transforma bloques "pequeñitos"). El mismo BC puede ser muy seguro o totalmente inseguro, dependiendo del OM con el que se implemente.

**CIFRADO AUTENTICADO (AUTHENTICATED ENCRYPTION)**
Modos de operación especiales, que además proporcionan autenticación e integridad cuando implementas un BC según sus normas.

**CÓDIGOS DE AUTENTICACIÓN DE MENSAJES (MESSAGE AUTHENTICATION CODES)**
Mecanismos que sirven para añadir autenticación e integridad a un mensaje, utilizando una clave. Llevan casi siempre una H o un BC asociados.



# Juego

**Objetivos didácticos:**

– Distinguir las tres propiedades CIA como elementos independientes y complementarios

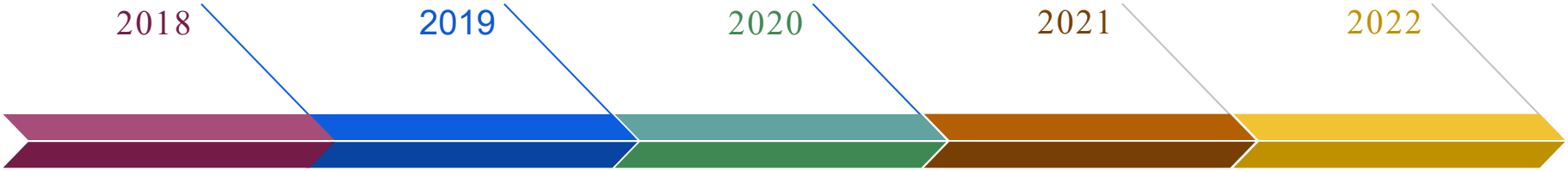
– Conocer qué tipo de herramientas criptográficas proporcionan las propiedades CIA, solas o en combinación

– Recordar que no todas las herramientas ofrecen el mismo nivel de seguridad; especialmente, recordar ejemplos de algoritmos “malos” y “buenos”

– Comprender la relevancia de los tamaños de las claves y los rangos de las funciones resumen desde el punto de vista de la seguridad

– Percibir como más ventajosas las herramientas de cifrado autenticado en comparación con las soluciones que combinan cifrado y autenticación de forma independiente

# Uso del juego en actividades de divulgación y refuerzo académico (1)




**–Concepción, diseño y creación del juego**

–2 comunicaciones cortas (JNIC 2018, IJIDOCEIN 2018)

–Talleres eventos públicos (HoneyCON, Semana de la Ciencia y la Innovación, CyberCamp)

–Talleres privados (IES)

–Talleres en eventos públicos (HackOn, STEM for Girls UC3M, Viernes tecnológicos UC3M, T3chFest [familias y público general], Feria Madrid por la Ciencia y la Innovación, Hack&Kids de CONPilar, Semana de la Ciencia y la Innovación)

–Talleres privados (IES, UC3M)

–Artículo Mathematics (MDPI), evaluación del juego y resultados talleres Nov2018 - Feb2019

–Talleres en eventos públicos (HackOn, Viernes tecnológicos [suspendida], Semana de la Ciencia y la Innovación [escape room online], c0r0n4con diciembre [escape room online])

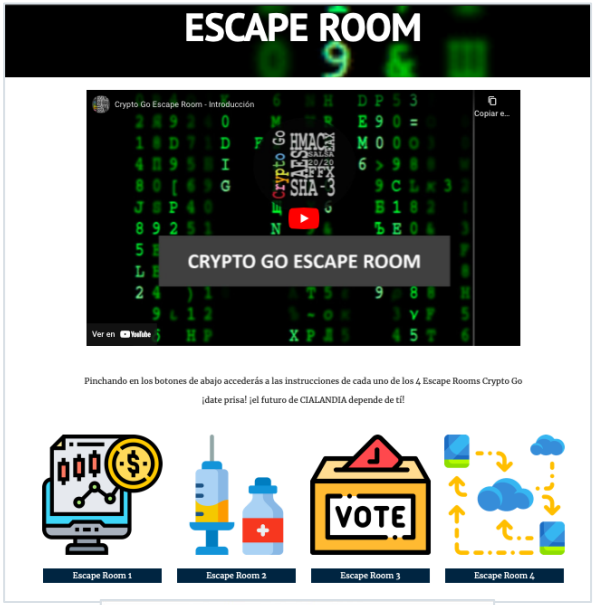
–Talleres privados (IES)

–Talleres en eventos públicos (Viernes tecnológicos [escape room online], STEM for Girls UC3M [escape room online])

–Talleres en eventos públicos (Día de la Mujer y la Niña en la Ciencia, STEM for Girls UC3M, Feria Madrid es Ciencia, URJC, Viernes Tecnológicos, C1b3rWall, Tecnocamp, UNICAN)

–Talleres privados (IES)

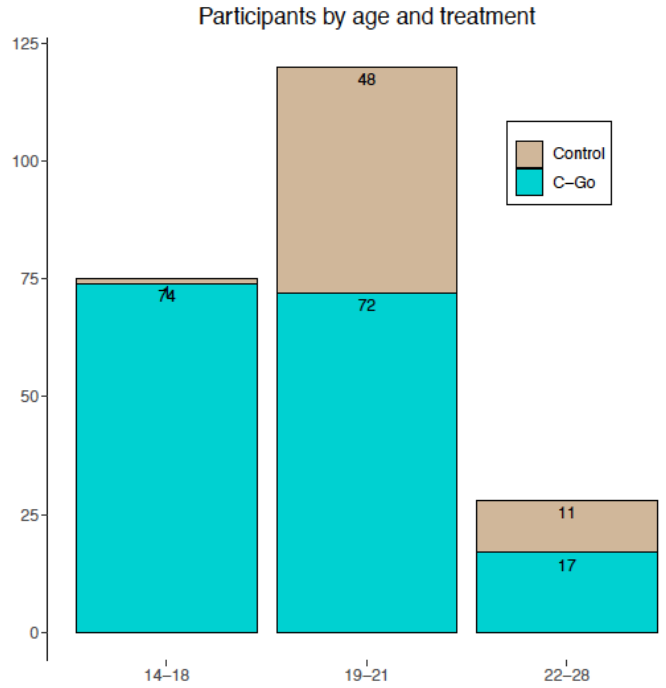
# Uso del juego en actividades de divulgación y refuerzo académico (2)

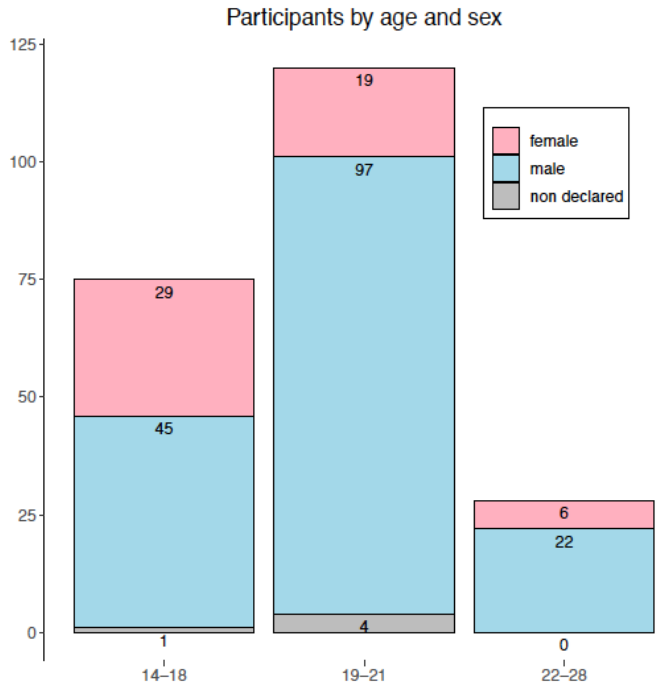






# Resultados de la evaluación del juego (1)

- 200 participantes (talleres Nov2018-Feb2019)
- Grupo Crypto Go y de control (actividad sustitutiva)
- MEEGA (Model to Evaluate Quality of Educational Games)





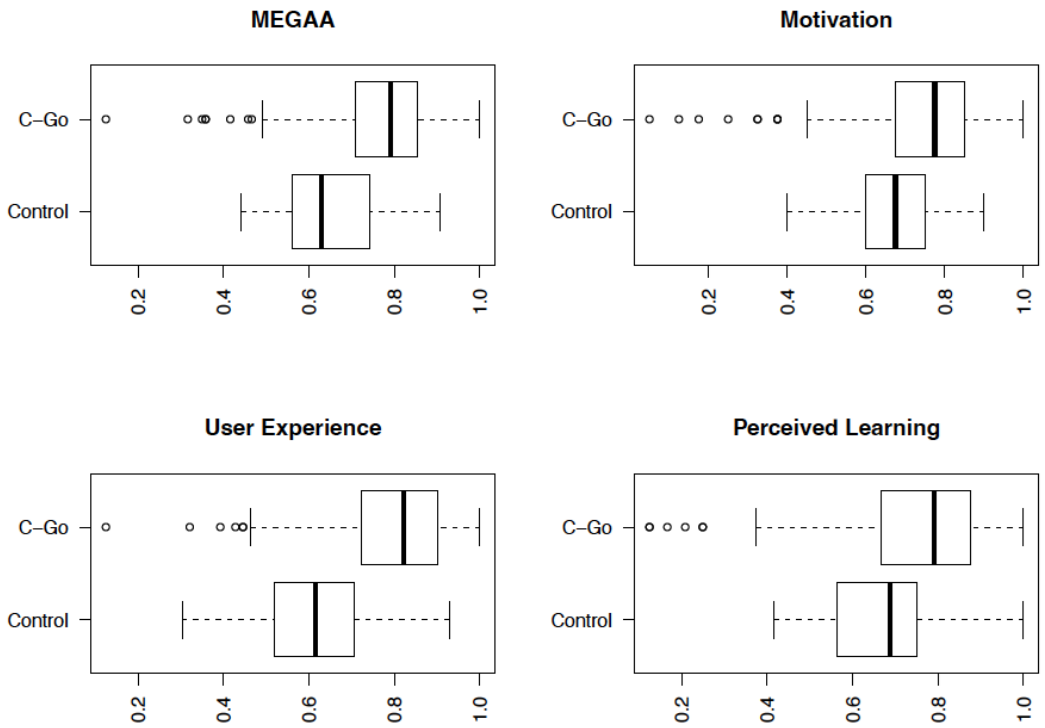
- González - Tablas, A.I.; González Vasco, M.I.; Cascos, I.; Planet Palomino, Á. **Shuffle, Cut, and Learn: Crypto Go, A Card Game for Teaching Cryptography** . *Mathematics* **2020** , *8*, 1993. URI: https://www.mdpi.com/2227-7390/8/11/1993

# Resultados de la evaluación del juego (2)

– **H1** : Participantes perciben Crypto Go como un juego educativo de calidad [✓ ]

– **H2** : Participantes perciben Crypto Go como un juego educativo de calidad superior que una actividad equivalente no lúdica [✓ ]

– **H3** : La efectividad de Crypto Go está influenciada por el género o la frecuencia de uso de juegos [ X ]





- González - Tablas, A.I.; González Vasco, M.I.; Cascos, I.; Planet Palomino, Á. **Shuffle, Cut, and Learn: Crypto Go, A Card Game for Teaching Cryptography** . *Mathematics* **2020** , *8*, 1993. URI: https://www.mdpi.com/2227-7390/8/11/1993

# Conclusiones

- Crypto Go:
  - juego de cartas útil para introducir, divulgar, reforzar conocimientos básicos de criptografía simétrica y de ciberseguridad
  - también permite para públicos más avanzados introducir TLS
  - muy flexible por su fácil adaptación para públicos diversos (juego por colores vs. algoritmos del estado del arte)
- Nuestra experiencia:
  - útil como complemento (motivación, experiencia de usuario) pero haría falta un uso continuado (o al menos mayor que una única vez) para obtener mayores beneficios en el aprendizaje
  - estupendo como gancho para captar público y divulgar criptografía
- Trabajo Futuro
  - Versión online (ya tanteado en pandemia)
  - Otras primitivas (clave pública)

# MUCHAS GRACIAS POR VUESTRA ATENCIÓN

**Hemos traído algunas barajas ;D**

**¿Alguien quiere probarlo?**