“Crypto Go”: criptografía simétrica en tapete verde

Ana I. González-Tablas
COSEC Lab – Universidad Carlos III de Madrid
Avda. de la Universidad 30
28911 Leganés, Madrid
aigonzal@inf.uc3m.es

María Isabel González Vasco
MACIMTE – Universidad Rey Juan Carlos
C/ Tulipán, S/N
28933 Móstoles, Madrid
mariaisabel.vasco@urjc.es

Resumen- **En este documento describimos el diseño preliminar de un juego de mesa, “Crypto Go” cuyo planteamiento mimetiza el del conocido juego de cartas “Sushi Go”. El fin de nuestra propuesta es familiarizar al alumno de una manera lúdica con las principales herramientas de clave simétrica. Así, el objetivo de cada partida es llegar a construcciones robustas para conseguir los objetivos de confidencialidad, integridad y autenticación en la transmisión de mensajes. En esta aproximación inicial obviamos numerosos aspectos que pueden incorporarse para completar nuestra propuesta, como la consideración de tamaños de clave o la generación pseudoaleatoria de calidad. Nuestro diseño inicial, sin embargo, es suficiente para conseguir que el alumno afiance los conceptos básicos más relevantes adquiridos en un curso elemental de criptografía simétrica, conozca un gran número de herramientas de amplio uso en la actualidad y sepa identificar errores de planteamiento en construcciones reales.**

Index Terms- gamificación, criptografía simétrica, educación.

Tipo de contribución: *Formación e innovación educativa*

I. Introducción

En la actualidad existe una necesidad urgente de capacitar en ciberseguridad a un gran número de profesionales, así como de concienciar y formar de forma adecuada en esta área a los desarrolladores de sistemas que procesen información. Una de las disciplinas en las que se apoya la ciberseguridad es la criptografía. En este trabajo se propone un juego de mesa con el objetivo de afianzar los conceptos adquiridos en un curso básico de criptografía simétrica. Está, por tanto, enfocado a alumnos de grado.

En los últimos años, se han propuesto un número no desdeñable de juegos educativos que abordan alguna temática en ciberseguridad, arrojando resultados positivos en las evaluaciones a pequeña escala realizadas [1]. La tipología es variada, desde complejos desarrollos software que simulan mundos virtuales (e.g., *CyberCIEGE*) hasta sencillos juegos de cartas (e.g., *Elevation of Privilege*).

En este trabajo se propone un juego de cartas sencillo, de mecánica rápida y sistema de puntuaciones simple. El objetivo didáctico es que los jugadores sean capaces de reconocer cuáles son las primitivas y los esquemas criptográficos adecuados para cubrir ciertos objetivos de seguridad (siguiendo como referencia esencial las recomendaciones publicadas en [2]).

II. Diseño Preliminar de Crypto Go

Crypto Go se plantea como un juego de cartas, sin tablero, en el que los usuarios parten con una mano inicial y pretenden terminar con una selección de cartas que contenga lo que llamamos *Crypto-Kit.* Un *Crypto-Kit* contendrá suficientes herramientas criptográficas para implementar un sistema seguro de criptografía simétrica con garantías de confidencialidad, integridad y autenticación.

Fig. 1. Ejemplo de cartas: 2 anversos (SHA-3 y HMAC) y reverso.

A. Cartas criptográficas

Las cartas de la baraja Crypto Go representan herramientas criptográficas susceptibles de ser utilizadas para realizar un esquema de transmisión de información con ciertas garantías (ver sección B). Contemplamos, en esta versión inicial, la inclusión de dos tipos de cartas:

Cartas de primitivas. Cada una representa a una primitiva criptográfica fundamental para cualquier diseño simétrico. En concreto, se incluyen tres modalidades:

1. **BC** – Cifradores de bloque (AES, 3DES, DES,…).
2. **H** – Funciones resumen (MD5, SHA2, SHA3,…).
3. **SC** – Cifradores de flujo (HC-128, SALSA, RC4,…).

Cartas para construcciones combinadas. Representan distintos esquemas que pueden determinar una implementación efectiva de las herramientas representadas por las cartas de primitivas (aisladas o en combinación). Contemplamos, en principio, las siguientes modalidades:

1. **OM –** Modos de operación (EME, FFX, OFB, CTR, CBC, ECB,…), para ser combinados con un cifrador de bloque explicitado por una carta BC.
2. **AE** – Métodos de cifrado autenticado (OCB, EAX, CCM, CWC…), que se construyen a partir de un cifrador de bloque. En su mayoría, estos métodos son implementados mediante la combinación de un modo de operación con un MAC que verifique ciertos requisitos, aunque en el juego simplemente se explicita que dependen de un cifrador en bloque.
3. **MAC** – Códigos de autenticación de mensaje (CMAC, EMAC, AMAC, HMAC,…), construidos con distintas primitivas (cifradores de bloque o funciones hash).

En la *Fig. 1* se ilustra el diseño de las cartas correspondientes a la función resumen SHA-3 y la función de generación de códigos de autenticación de mensajes HMAC. El anverso de cada carta identificará la herramienta criptográfica a la que representa (e.g., SHA-3 y HMAC), identificándose cada tipo de herramienta con un color diferente

(e.g., naranja para las cartas H y azul claro para las MAC). Además, se incluirá una breve reseña de la herramienta representada, sin desvelar su nivel de seguridad. El reverso de todas las cartas ha de ser idéntico para no revelar ni su tipología ni la herramienta concreta que representan.

B. Objetivo del juego

Crypto-Sets y Crypto-Kits. Comenzamos por definir los siguientes conjuntos especiales de cartas o *Crypto-Sets*:

- **Crypto-Set CS1** (Confidencialidad): a partir de una carta OM combinada con una carta BC, o con una carta SC.
- **Crypto-Set CS2** (Integridad + Autenticación): a partir de una carta MAC combinada con una carta H o BC, dependiendo del tipo de MAC.
- **Crypto-Set CS3** (Confidencialidad + Integridad + Autenticación): a partir de una carta AE combinada con una carta BC.

El objetivo del juego es conseguir un conjunto de cartas que permitan cubrir los tres objetivos de seguridad considerados, denominando dicho conjunto de cartas como *Crypto-Kit*. Con los *Crypto-Sets* recién definidos hay dos maneras de alcanzar dicho objetivo:

- **Crypto-Kit CK1**: Combinando dos *Crypto-Sets*, uno del tipo CS1 y otro del tipo CS2.
- **Crypto-Kit CK2**: Consiguiendo un *Crypto-Set* CS3.

Nótese que éste es un escenario muy simplificado, pues en esta versión inicial tomaremos dos hipótesis que no se corresponden al cien por cien con la práctica criptográfica real. Concretamente, consideraremos que:

- cualquier cifrador en bloque es válido para construir cualquiera de los *Crypto-Set* de tipo CS3.
- las cartas tipo MAC pueden combinarse con cualquier cifrador en bloque, a excepción de la carta HMAC que deberá combinarse con una carta de tipo H para poder completar un *Crypto-Set* de tipo CS2.

Completar un Crypto-Kit robusto. El objetivo de cada jugador será conseguir un *Crypto-Kit* robusto, es decir, una combinación de cartas que posibilite la construcción de un diseño criptográfico seguro, según las premisas descritas en las instrucciones del juego. Dicho *Crypto-Kit* puede formarse con distinto tipo y número de cartas, y no todos los diseños, siendo válidos, darán al jugador la misma puntuación.

Nivel de seguridad de las herramientas. El juego incluirá una tabla que asignará a cada herramienta criptográfica un color indicando su robustez. Así, las cartas a las que se les asigne el color verde serán las que representen herramientas cuya seguridad se considera elevada, el naranja será para las que alcanzan una seguridad media y reservaremos el rojo para aquellas cuya seguridad es altamente cuestionable. La asignación de colores a cada herramienta se realizará a partir de las recomendaciones de [2], identificando con color verde las herramientas etiquetadas con nivel de seguridad "Future" y con naranja las etiquetadas como "Legacy". Las cartas rojas serán aquellas cuya seguridad se considera en entredicho de manera aplastante, como la función resumen MD5, o el cifrador de flujo RC4. El uso de esta tabla en el juego permitirá que los jugadores interioricen el nivel de seguridad de las herramientas involucradas.

C. Mecánica del juego

El juego se articulará en rondas (considerando en un principio partidas de tres rondas) y ganará aquel jugador que haya obtenido mayor puntuación acumulando los puntos de cada ronda. Planteamos el juego con un máximo de 8 jugadores y una baraja de 108 cartas. De esta forma puede garantizarse la variabilidad en el juego, así como la aparición en cada partida de un amplio abanico de cartas distintas (véase Tabla I).

Tabla I: Número de copias de cada carta

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

Inicio de partida: Se baraja el mazo y se reparten a cada jugador 6 cartas. El resto se disponen boca abajo en un mazo en el centro.

Ronda: En cada turno normal cada jugador debe elegir una carta de su mano y la deja boca abajo en la mesa. A continuación, todos revelan la carta elegida simultáneamente y la colocan enfrente de cada jugador con el anverso a la vista (junto con las otras cartas seleccionadas). A continuación, cada jugador pasa al jugador sentado a su izquierda las cartas restantes de su mano boca abajo. De este modo, en el siguiente turno cada jugador empieza con una carta menos y una mano nueva. Este proceso se repite hasta que cada jugador recibe un mazo con una sola carta.

Entonces cada jugador tomará 2 cartas del mazo central y los incorporará a la mano. En este momento, además de seleccionar una carta como en los turnos normales, el jugador podrá sustituir hasta 2 de sus cartas ya jugadas, descartando las que sustituya en un mazo de descartes. Antes de pasar el mazo al siguiente jugador, por cada carta sustituida, se tomará otra carta del mazo central. Cuando se han jugado todas las cartas, la ronda se da por finalizada y se procede a calcular públicamente las puntuaciones de cada jugador.

Puntuando una ronda: Solo puntúan las cartas que conforman un *Crypto-Kit*. Por cada *Crypto-Kit*, el jugador acumula 10 puntos de los que se restan 1 punto por cada carta con clasificación naranja y 2 puntos por cada carta con clasificación roja de las incluidas en sus *Crypto-Kits*.

Fin de la partida y ganador(es) del juego: Gana el jugador con mayor puntuación tras tres rondas.

III. Trabajos Futuros y Conclusiones

Este diseño inicial de Crypto Go es muy útil para ayudar al alumno a afianzar los conocimientos básicos de criptografía simétrica impartidos en un curso de grado. Por supuesto, un primer paso a dar de cara a la validación de esta idea es hacer un prototipo sencillo y analizar la experiencia de varios grupos de alumnos al jugar. Entre nuestros planes está además el realizar una versión extendida en la que se puedan añadir cartas para, por un lado, incorporar nociones y destrezas relacionadas con la correcta gestión de claves en este ámbito y, por otro, afianzar conocimientos directamente relacionados con ataques concretos a las herramientas consideradas. Nuestra idea es que esta versión extendida, enfocada a alumnos de postgrado, sea compatible con la aquí presentada.

IV. Referencias

[1] Hendrix, M., Al-Sherbaz, A. & Victoria, B.: "Game based cyber security training: are serious games suitable for cyber security training?", en *International Journal of Serious Games*, vol. 3, n. 1, pp. 53-61, 2016.

[2] ECRYPT CSA: "D5.2 algorithms, key size and protocols report", *informe del proyecto 645421 (H2020-ICT-2014)*, 2016.