Jugando a Descifrar...

Víctor Gatón Bustillo
Departamento de Matemática Aplicada, Universidad de Valladolid
vgaton@mac.uva.es

1. Introducción.

Un **serious game** (juego serio o juego formativo) es un juego diseñado con un objetivo principal distinto al mero entretenimiento [1]. El término "serio" representa el hecho de que el juego debe proporcionan algún mensaje a los participantes, ya sea en forma de conocimiento o de habilidad [2], dentro del contexto específico en el que se realiza el juego. Por lo tanto, un *serious game* debe combinar un verdadero elemento de entretenimiento y una dimensión práctica [3], centrada en los objetivos que buscan obtenerse con la realización del juego. Este tipo de juegos se han utilizado desde el siglo pasado [4], en ámbitos militares o de la salud, y actualmente juegan un papel de relevancia en las empresas, en las que los *serious games* se utilizan para la adquisición y desarrollo de habilidades directivas.

Los *serious games* también se han incorporado al entorno educativo, con el objetivo de ayudar a que los alumnos adquieran un mayor compromiso con su proceso de aprendizaje, al tiempo que adquieren las competencias o habilidades consideradas en el diseño del juego [5]. Este tipo de actividad formativa no sólo fomenta la motivación del alumno, sino que también ayuda a la comprensión de conceptos o materias, además de promover la construcción de conocimiento y el desarrollo de capacidades, a través de la exposición a diferentes situaciones, casos o problemas.

La metodología UVAGILE contempla el uso de *serious games* como método complementario a las clásicas clases magistrales o sesiones de prácticas de laboratorio. La finalidad de estos juegos es que los alumnos se diviertan aprendiendo y que adquieran un mayor compromiso con su proceso de aprendizaje. Por otro lado, estos juegos se realizan también con el objetivo de retroalimentar el aula ágil en la que se imparte la asignatura, sobre todo en lo relativo al trabajo en equipo: en este aspecto, los *serious games* se han mostrado como una herramienta efectiva para que los equipos Agile adquieran las habilidades necesarias para realizar su trabajo [6].

UVAGILE propone introducir *serious games* en el aula ágil para presentar o complementar la exposición de conceptos que, por su complejidad, son más difíciles de comprender para los alumnos. Para ello, el juego se diseñará como una metáfora del mundo real que presente los objetivos de aprendizaje de la actividad de tal forma que resulten fácilmente entendibles para los alumnos. Además, es importante que la realización del juego se lleve a cabo en un entorno de aprendizaje lúdico, que facilite que el alumno disfrute con el desarrollo de la actividad y adquiera las competencias deseadas utilizando el sentido común y otras habilidades de su vida cotidiana.

En este documento, se presenta una propuesta de *serious game* vinculada con Protocolos y Comunicaciones Seguras, asignatura optativa de 4º curso del Grado en Ingeniería Informática de Servicios y Aplicaciones. En el Apartado 2, se plantea el contexto del juego y los objetivos de aprendizaje que persigue. El Apartado 3 describe el juego en sí y cómo se lleva a cabo. Finalmente, el Apartado 4 presenta unas breves conclusiones sobre la experiencia de realización del juego durante el presente curso y las lecciones aprendidas de cara a su uso en el futuro.

2. Contexto del Juego

La **criptografía** [7] se define como el arte de escribir con clave secreta o de un modo enigmático. El uso de la criptografía se remonta a las primeras civilizaciones y su objetivo es el mismo que en la actualidad: garantizar la confidencialidad de los mensajes. La criptografía ha jugado un papel fundamental en una gran parte de los desarrollos tecnológicos de los últimos años y su uso es imprescindible en una sociedad tan interconectada como la actual.

La asignatura "Protocolos y Comunicaciones Seguras", en la que se enmarca el presente juego, proporciona conocimientos sobre criptografía a los alumnos de 4º curso del Grado en Ingeniería Informática de Servicios y Aplicaciones. Más concretamente, se centra en el estudio de las técnicas matemáticas relacionadas con el cifrado de datos, el criptoanálisis y sus aplicaciones en la seguridad informática. A lo largo de la asignatura, se hace un repaso de las técnicas criptográficas usadas a lo largo de la historia, desde la más antigua registrada, la clave de "César", hasta las más modernas, como el RSA o el AES. Algunos de estos tipos de cifrado, y algunos de los ataques criptográficos expuestos en la asignatura, permiten que los alumnos hagan prácticas de forma colaborativa, facilitando que alcancen los objetivos de aprendizaje de forma más satisfactoria.

Cabe destacar que aunque las novelas y las películas han dado una visión un poco romántica del genio matemático que consigue romper o descifrar una clave con una "idea feliz", la realidad es que tanto la creación como el ataque a un sistema criptográfico suele requerir de un equipo de trabajo colaborativo. Por ejemplo, el descifrado de la máquina Enigma durante la segunda guerra mundial se atribuye a Alan Turing. Sin dejar de reconocer su increíble aportación con el diseño de la primera máquina computadora que permitió realizar miles de cálculos mucho más rápidamente, el descifrado en sí se realizó por todo un equipo de personas de varios países. Sin entrar en detalles, el problema de Enigma se dividió en varios problemas criptográficos más pequeños que se resolvieron por separado para, globalmente, poder descifrar los mensajes.

Por lo tanto, el objetivo de este juego es que los alumnos sean conscientes de que el trabajo colaborativo reduce significativamente el tiempo de resolución de un problema criptográfico. En este caso, elegimos el cifrado por sustitución, con el objetivo secundario de potenciar el uso del lenguaje y sus reglas sintácticas, y de que los alumnos apliquen una técnica de uso común en este campo: la búsqueda por diccionarios.

2.1. Cifrado por Sustitución

El **cifrado por sustitución** [7] es una técnica clásica que data del año 50 A.C. y cuyo uso original se atribuye al cifrado de mensajes militares en el imperio romano. En este juego, se abordará la variante de sustitución simple monoalfabética, que consiste en reemplazar cada letra del *alfabeto original* por una letra en el *alfabeto de sustitución*. Por lo tanto, este cifrado diferencia dos alfabetos (ambos con el mismo número de símbolos):

- El alfabeto original está compuesto por las letras minúsculas.
- El alfabeto de sustitución está compuesto por las letras mayúsculas.

El cifrado por sustitución se define, de forma sencilla, mediante la función que relaciona cada letra del alfabeto original con una letra en el alfabeto de sustitución. La Tabla 1 presenta un ejemplo de cifrado de sustitución.

Tabla 1. Cifrado por sustitución												
a	→	**H**	b	→	**I**	c	→	**J**	d	→	**K**	e	→	**L**
f	→	**M**	g	→	**N**	h	→	**Ñ**	i	→	**O**	j	→	**P**
k	→	**Q**	l	→	**R**	m	→	**S**	n	→	**T**	ñ	→	**U**
o	→	**V**	p	→	**W**	q	→	**X**	r	→	**Y**	s	→	**Z**
t	→	**A**	u	→	**B**	v	→	**C**	w	→	**D**	x	→	**E**
y	→	**F**	z	→	**G**									

De esta forma, para cifrar un mensaje *claro* simplemente se reemplaza cada letra (minúscula) por su correspondiente letra (mayúscula) en el alfabeto de sustitución, obteniendo así el mensaje *cifrado*:

`esto se puede leer` → **LZAV ZL WBLKL RLLY**

El procedimiento de descifrado procede de forma inversa. De esta forma, para obtener el mensaje *claro* a partir del mensaje *cifrado,* simplemente se reemplaza cada letra mayúscula por su correspondiente minúscula:

LZAV TV → `esto no`

2.2. Ataque al Cifrado

La fortaleza de este método de cifrado reside en que la tabla de sustitución sólo la conozcan el emisor y el receptor del mensaje. De esta forma, si un tercero interceptase el mensaje cifrado, debería probar todas las combinaciones posibles de tablas de sustitución hasta encontrar aquella que le permite obtener el mensaje *claro*. Esto supondría evaluar `28!` = `304.888.344.611.713.860.501.504.000.000` posibles tablas de sustitución, utilizando el método de fuerza bruta. Esta opción no es viable ni con la ayuda un ordenador, que requeriría un tiempo de cómputo elevado para obtener la tabla de sustitución correspondiente.

No obstante, el procedimiento para atacar y poder descifrar este tipo de mensajes data del año 1200 D.C., mucho antes de la invención del ordenador. La técnica se basa en un fenómeno conocido como *frecuencia del idioma*, que indica la probabilidad de ocurrencia de cada letra dentro del mensaje claro depende de las características particulares del idioma utilizado para escribirlo. Es decir, algunas letras tienen una probabilidad de ocurrencia mucho mayor que otras. Por ejemplo, en castellano, las letras `'e'`, `'a'`, `'l'`, y `'s'` aparecen con mayor frecuencia que `'u'`, `'x'`, `'w'` o `'y'`. En el caso del inglés, la `'y'` presenta una frecuencia de aparición mucho mayor.

Es un fenómeno común que, fijado un idioma, las frecuencias de las letras se mantenga en cualquier texto escrito de acuerdo con su gramática. Evidentemente, se requiere que el texto sea suficientemente largo, aunque incluso en ejemplos cortos puede observarse este fenómeno.

Retomando el ejemplo anterior: `LZAV ZL WBLKL RLLY`, se puede observar que la letra `'L'` es la más frecuente. Asumiendo que el texto está escrito en castellano, podemos reemplazar todas las apariciones de `'L'` por `'e'`, dado que la `'e'` es la letra más frecuente en el idioma castellano. Así podría continuarse con las diferentes letras del mensaje cifrado, aunque en algunos casos nos encontraríamos con que varias letras ocurren el mismo número de veces. Esto puede suceder por múltiples motivos, pero el más general es que hay letras que tienen una frecuencia muy similar dentro de un idioma. Por lo tanto, el método para atacar el cifrado por sustitución debe ser un poco más elaborado. Concretamente, seguirá los siguientes pasos:

1. Obtener la frecuencia del idioma utilizado para escribir el mensaje claro. Esto puede obtenerse fácilmente a través de la web.
2. Calcular la frecuencia de cada símbolo presente en el mensaje cifrado.
3. Sustituir el símbolo más frecuente en el mensaje cifrado, por la letra más frecuente en el idioma considerado.
4. Sustituir el segundo símbolo más frecuente en el mensaje cifrado, por la segunda letra más frecuente en el idioma considerado.

El paso 5 podría imitar a los pasos 3 y 4, y reemplazar las ocurrencias del tercer símbolo más frecuente por la letra correspondiente. El procedimiento podría continuar con el cuarto símbolo más frecuente, quinto… pero podríamos encontrarnos con el problema indicado anteriormente, que varios símbolos presenten la misma frecuencia. Por este motivo, se suele utilizar también una **búsqueda por diccionarios** para tomar decisiones más fiables a la hora de seguir sustituyendo símbolos.

Después de haber reemplazado el símbolo más frecuente en el mensaje cifrado de nuestro ejemplo, obtenemos lo siguiente: `eZAV Ze WBeKe ReeY`. Si nos fijamos en la última palabra, `ReeY`, podemos observar que tiene sólo cuatro letras y que las dos letras centrales son sendas `'e'`. Una búsqueda por diccionarios consistiría en localizar todas aquellas palabras de 4 letras, en castellano, que contienen la letra `'e'` en la segunda y tercera posición. El número de palabras que satisfacen estas restricciones no es muy elevado, por lo que se podría hacer una evaluación relativamente rápida que nos permitiese deducir las letras (minúsculas) que se cifran mediante `'R'` e `'Y'`. Supongamos que elegimos la palabra `"leer"`. Esto significaría que `'R'` cifra `'l'` e `'Y'` cifra `'r'`.

Con un poco de práctica y una buena dosis de paciencia, esta técnica permite descifrar cualquier mensaje en un tiempo razonable.

3. El Juego

El juego se plantea como una sencilla actividad centrada en que los equipos de alumnos sean capaces de obtener mensajes claros a partir de los mensajes cifrados que se le entregan. Por lo tanto, lo que se busca es que los alumnos alcancen el objetivo de aprendizaje de “aprender a cifrar y descifrar un mensaje utilizando el método de cifrado por sustitución”. Además, se busca que este juego ayude a que los alumnos comprendan la necesidad de “colaborar en sus equipos de trabajo” y, con ello, poder resolver sus tareas de manera más eficiente. Para ello, el juego se desarrollará en tres etapas. En cada una de ellas, el tamaño del equipo se irá incrementando en una persona, de tal forma que el primer mensaje se descifrará de forma individual, el segundo por parejas y el tercero en equipos de 3 alumnos.

En primer lugar, se introducirán los fundamentos del cifrado por sustitución y se explicarán los pasos que han de llevarse a cabo para atacarlo. Asimismo, se proporcionarán varias utilidades software para que puedan obtener eficientemente la distribución de frecuencias de símbolos en el mensaje cifrado y el reemplazo de los símbolos cifrados por los símbolos en claro correspondientes, de acuerdo con las decisiones que se vayan tomando. Finalmente, se les entregarán a los alumnos un par de mensajes cifrados, para que puedan familiarizarse con las herramientas y el procedimiento de descifrado, antes de comenzar el juego de forma efectiva.

Como se indicaba anteriormente, el juego se llevará a cabo en tres etapas, en las que los alumnos tendrán que descifrar mensajes de la misma longitud. El responsable del juego registrará el

tiempo que requiere cada equipo para descifrar el mensaje en cada una de las etapas del juego, de cara a obtener una estadística que muestre el efecto positivo de trabajar en equipo. Esta información se presentará al final del juego, realizando una retrospectiva sobre los resultados, en la que los alumnos reflexionen sobre su aprendizaje y las dificultades que se han encontrado en el juego, además de explicar cómo esperan utilizar el aprendizaje adquirido durante el desarrollo de la asignatura.

4. Evaluación y Conclusiones

La evaluación del presente juego se ha realizado fuera del periodo de clases de la asignatura "Plataformas y Comunicaciones Seguras" y se ha invitado a alumnos de primer curso, que obviamente no han cursado aún la asignatura. Además, se ha mantenido un pequeño grupo de control de alumnos (de cuarto curso) que ya han superado la asignatura. Esta decisión tiene una doble motivación:

- Invitar a alumnos de primer curso es una forma de acercar UVAGILE y el concepto de *serious game,* a un conjunto de alumnos que aún no han tenido oportunidad de experimentar con la metodología. De esta forma, conseguimos ampliar la base de estudiantes que ya conocen UVAGILE, facilitando con ello la implantación de un mayor número de aulas ágiles durante el próximo curso.
- Además, poder formar grupos de alumnos de primer y último curso nos permite mostrarles de forma práctica, que los beneficios del trabajo en equipo no dependen de los conocimientos de sus miembros, si no de su capacidad de colaborar.

El juego contó con la participación de 16 alumnos, la gran mayoría pertenecientes a primer curso del Grado en Ingeniería Informática de Servicios y Aplicaciones. Todos ellos realizaron el juego de acuerdo con lo indicado en el apartado anterior y en cada etapa descifraron mensajes de 500 símbolos.

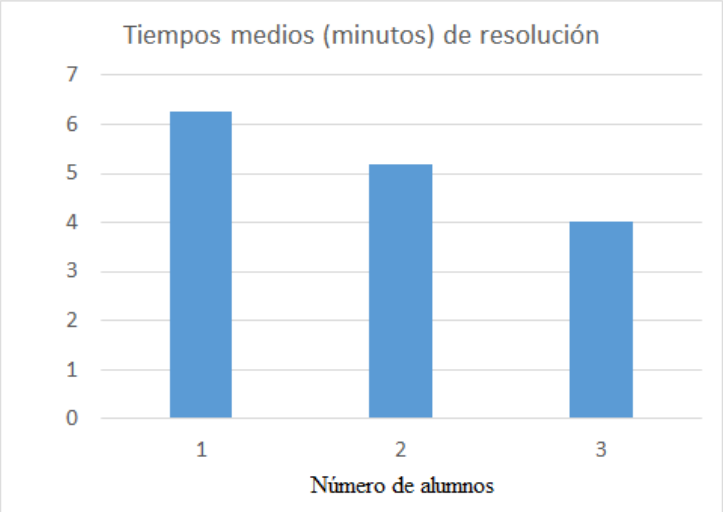

Figura 1 | Tiempo medio de resolución por número de alumnos en el grupo

La Figura 1 muestra el tiempo medio (en minutos) que les costó descifrar el mensaje proporcionado en cada etapa, trabajando en equipos de 1, 2 y 3 alumnos, respectivamente. Como puede observarse, el tiempo se redujo paulatinamente desde la primera a la última etapa. Este resultado viene a demostrar el beneficio del trabajo colaborativo que, en este caso, permitió que los alumnos pudiesen encontrasen más similitudes, y más deprisa, en los

diccionarios, acelerando con ello el proceso de descifrado ("cuatro ojos, ven más que dos"). No obstante, no debe despreciarse tampoco el efecto de la experiencia de los alumnos en etapas sucesivas. Obviamente, en la tercera etapa, los alumnos habían asimilado más el procedimiento de descifrado, tomando mejores decisiones, de forma más eficiente. Por lo tanto, se puede concluir que el juego permitió que los alumnos alcanzasen de forma satisfactoria sus dos objetivos de aprendizaje, el relacionado con aprender a cifrar y descifrar utilizando el método de sustitución, y el del fomento del trabajo en equipo. Respecto a este último, cabe destacar que no se encontraron diferencias significativas entre el rendimiento de los alumnos de primer y cuarto curso.

Durante la retrospectiva de finalización del juego, los alumnos de primer curso mostraron su interés en seguir aprendiendo Criptografía y, por consiguiente, en cursar la asignatura "Protocolos y Comunicaciones Seguras" en un futuro. Además, como los alumnos ya tenían cierta experiencia de programación, se plantearon diferentes cuestiones relativas a cómo construir, por ellos mismos, las utilidades proporcionadas para la realización del ejercicio.

En definitiva, la experiencia resultó muy positiva para todos y los resultados obtenidos avalan el interés del juego y, sobre todo, el valor que tienen este tipo de actividades docentes dentro de un aula ágil.

Bibliografía

[1] D. R. Michael y S. L. Chen. *Serious Games: Games That Educate, Train, and Inform*. Muska & Lipman/Premier-Trade. 2005.

[2] F. Laamart, M. Eid y A. El Saddik. *An Overview of Serious Games*. International Journal of Computer Games Technology. Article 358152. 2014.

[3] J. Álvarez and L. Michaud. *Serious Games: Advergaming, Edu-gaming, Training, and More.* IDATE. 2008.

[4] C. Abt. *Serious Games*. New York: The Viking Press. 1970.

[5] M. Dankbaar. *Serious Games and Blended Learning; Effects on Performance and Motivation in Medical Education*. Perspectives on Medical education, 6(1): pp- 58–60. 2017.

[6] C.J. Stettina, T. Offerman, B. De Mooij e I. Sidhu. *Gaming for Agility: Using Serious Games to Enable Agile Project & Portfolio Management Capabilities in Practice*. IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). 2018.

[7] A. Fúster Sabater, D. de la Guía Martínez, L. Hernández Encinas y F. Montoya Vitini. *Técnicas Criptográficas de Protección de Datos*. Ra-Ma. 2004.