JARDINERÍA CRIPTOGRÁFICA: RETOS CRIPTOGRÁFICOS DISTRIBUIDOS

Usando las plataformas *wiki* para coordinar un ataque adaptativo y distribuido basado en el criptoanálisis de la máquina Enigma de la segunda guerra mundial

• Borrego Iglesias, Carlos
Universitat Autònoma de Barcelona
Departament d'Enginyeria de la Informació i les Comunicacions (dEIC)
Escola Tècnica Superior d'Enginyeries
Edifici Q. 08193 Bellaterra, Barcelona – España.
carlos.borrego@uab.cat

1. **RESUMEN:** El criptoanálisis es la ciencia que estudia los mecanismos para romper los algoritmos criptográficos de ocultamiento de la información. En un criptoanálisis adaptativo sus atacantes pueden elegir progresivamente varios textos y obtener sus textos cifrados correspondientes. En esta comunicación presento la experiencia de seis años de una actividad en la que estudiantes de criptografía han participado en un reto criptográfico adaptativo grupal basado en la *siembra* de minas de la segunda guerra mundial.

2. **ABSTRACT:** Cryptanalysis is the science that studies the mechanisms to break cryptographic algorithms. In an adaptive cryptanalysis, attackers have the privilege of choosing various texts and gradually obtain their corresponding ciphertexts. In this communication, I present the six-year experience of an activity in which students of the cryptography course have participated in a group adaptive cryptographic challenge based on planting mines during the Second World War.

3. **PALABRAS CLAVE:** reto criptográfico, jardinería, máquina Enigma, segunda guerra mundial, criptoanálisis / **KEYWORDS:** cryptographic challenge, gardening, Enigma machine, Second World War, cryptanalysis.

4. DESARROLLO:

Durante la segunda guerra mundial los aliados mantuvieron una lucha incansable para poder descifrar los contenidos de los mensajes cifrados con la máquina Enigma [1], un dispositivo electromecánico de cifrado con el que los alemanes cifraban sus comunicaciones. Los textos cifrados incautados por Bletchey Park, el centro militar encargado de criptoanalizar la máquina Enigma, no eran suficientes para atacar criptográficamente y romper su seguridad. Por este motivo, los aliados entendieron que la única manera de lograr este ataque era por medio de forzar a los alemanes a enviar determinados mensajes, de tal modo que si los aliados consiguiesen incautar estos mensajes cifrados, dispondrían también de sus textos en claro correspondientes, o al menos alguna parte de ellos.

Para realizar semejante reto, los aliados *sembraban* con minas una determinada zona esperando que los alemanes informasen de ello usando mensajes cifrados con la máquina Enigma con la posición de las minas. A esta acción los aliados la denominaban jardinería, del inglés *gardening*.

a) Objetivos

El criptoanálisis es la ciencia que estudia los mecanismos para romper o revelar los métodos criptográficos de ocultamiento de la información. En un criptoanálisis adaptativo de texto claro conocido los atacantes tienen el privilegio de poder elegir o imponer progresivamente varios textos y obtener sus textos cifrados correspondientes.

El objetivo principal de la actividad descrita en esta comunicación es realizar un criptoanálisis adaptativo de texto claro conocido distribuido entre todos los miembros de una clase[1]. Los estudiantes son retados a resolver un algoritmo de cifra propuesto por el profesor simulando los trabajos de *jardinería* realizados por los aliados durante la segunda

[1] Asignatura Criptografia I seguretat en Xarxes del quinto curso de la Ingeniería de Telecomunicaciones de la Escuela de Ingeniería, Universidad Autónoma de Barcelona. Más información sobre el curso: http://deic.uab.cat/curt/csx

guerra mundial. Así mismo, con esta actividad también se persigue estimular el paradigma de cooperación [2] entre los estudiantes en contraposición al clásico paradigma de competición, de tal manera que se fomente el trabajo grupal y colaborativo.

b) Descripción del trabajo

El profesor a principio de curso idea un algoritmo de cifra de tipo clásico: algoritmos de transposición y sustitución con un componente de computación bajo, es decir, los algoritmos de cifra elegidos deben ser métodos sencillos cuya resolución sea accesible a través de un ataque adaptativo de texto claro conocido. Cada año el algoritmo cambia para evitar posibles copias. Los algoritmos de cifra que se han propuesto hasta el momento son variaciones de algoritmos clásicos como la cifra del César [3], la cifra de Vigenère [4] o el método de cifra del libro [5] con la particularidad que la llave del método era el mismo enunciado del reto. La totalidad de estos algoritmos han sido programados por el profesor usando todo tipo de lenguajes de programación como *C++*, *perl*, *bash programming* o *python*.

Por otro lado, el profesor prepara un espacio común usando una plataforma *wiki* [6] en el que todos los participantes del reto pueden leer y escribir. Adicionalmente, el profesor crea un espacio individual privado para que cada estudiante pueda escribir el desarrollo de la resolución del reto. En el espacio común los alumnos proponen ordenadamente diferentes textos cualesquiera o *siembras.* Es decir, los participantes del reto criptográfico para su resolución no parten de textos cifrados simplemente sino que proponen textos de modo adaptativo al estilo de la *siembra* de minas ideadas por los aliados durante la segunda guerra mundial.

Posteriormente, el profesor cifra cada uno de estos textos o *siembras* siguiendo el algoritmo de cifra ideado. No se admiten textos nuevos por parte de los alumnos hasta que el profesor no haya cifrado el último propuesto con el fin de asegurar el proceso adaptativo del reto. En función de los textos propuestos por los alumnos y sus correspondientes textos cifrados los alumnos van proponiendo textos adicionales hasta dar con la solución del tipo de cifra. La

resolución del reto puede llegar pasados varios meses. En la Figura 1 se ilustra un ejemplo de dos textos *siembras* con sus correspondientes textos cifrados (*Siembra* y *Cifra* en la figura).

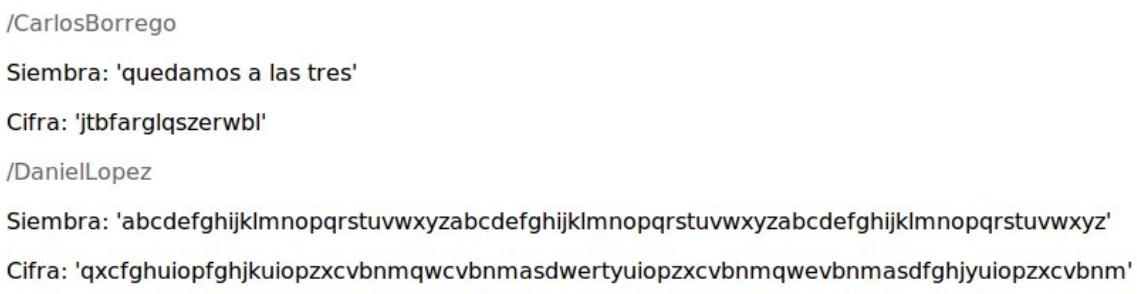

Figura 1: Extracto de la wiki común con dos entradas de texto en claro y sus correspondientes textos cifrados.

En el momento que el primer alumno resuelve el reto criptográfico se le entrega un diploma de resolución a todos aquellos alumnos que hayan propuesto una *siembra* hasta el momento. De esta manera los alumnos entienden que la solución al reto ha sido un proceso colaborativo y no competitivo fruto de un trabajo grupal. A modo de diversión, el texto del diploma de resolución está cifrado con el algoritmo de cifra propuesto. Los alumnos reciben este momento con sorpresa y diversión.

Al final del periodo de resolución del reto criptográfico, que aproximadamente son tres meses dependiendo de la evolución del temario de la asignatura, los alumnos tienen que justificar los textos propuestos usando su espacio de *wiki* privado. Así mismo, independientemente de que los alumnos hayan conseguido resolver completamente el reto criptográfico o no, deberán clasificar el algoritmo de cifra siguiendo la clasificación propuesta en [7] e ilustrada en la Figura 2.

La plataforma wiki elegida para el intercambio de mensajes es MoinMoin [8]. Esta plataforma es de código libre y está distribuida bajo los términos de la licencia GNU General Public License (GPL). La edición de las entradas wiki es altamente intuitiva permitiendo incluso un modo gráfico de fácil edición. Sus listas de control de acceso permiten gestionar detalladamente los permisos de las distintas entradas de forma sencilla

tanto a nivel de usuario individual para las memoria final de cada uno de los participantes del reto criptográfico, como a nivel de grupo de usuarios para disponer de un espacio para el ataque conjunto.

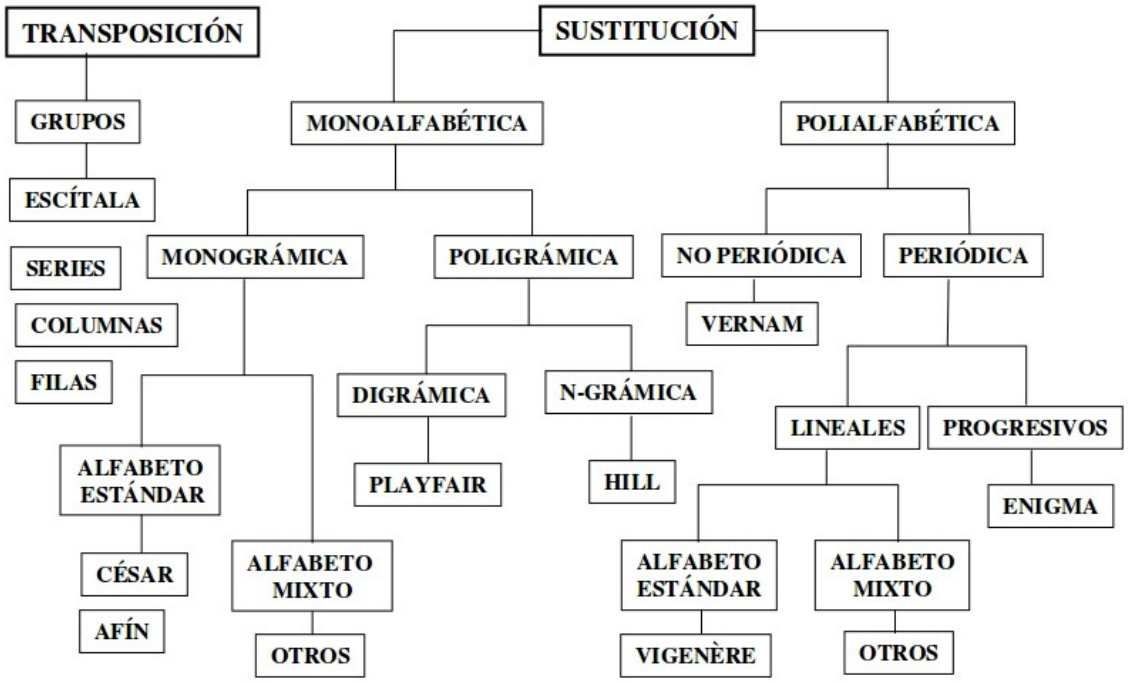

Figura 2: Clasificación de los criptosistemas clásicos.

c) Resultados, conclusiones y líneas futuras.

En esta comunicación se presenta la experiencia de seis años de una actividad propuesta a los alumnos de criptografía basada en el criptoanálisis de la máquina Enigma durante la segunda guerra mundial. La experiencia ha sido extremadamente positiva en cuanto al aprendizaje y todo un reto intelectual, divulgativo y académico, tanto para el profesor como para los alumnos.

Durante los seis cursos en los que se ha impartido la actividad el número de alumnos que lo ha resuelto está en torno al 5%. El hecho que sea un número tan bajo indica que el reto es suficientemente difícil para motivar a los alumnos sin llegar a ser evidente. A pesar de que el objetivo no es resolverlo sino participar en el ataque conjunto y cooperativo, al menos

una persona lo ha resuelto cada año. Además, del 95% restante la mayoría ha demostrado interés en el reto y ha disfrutado de su experiencia. El tiempo de resolución ha sido similar entre todos los cursos y oscila entre los 72 y 90 días. El número de *siembras* necesarias para resolver el reto ha variado entre 22 y 45.

Por otro lado, el reto criptográfico ha sido la actividad mejor valorada por los estudiantes según las encuestas realizadas al 97%[2] de los alumnos y la retroalimentación directa ofrecida por los alumnos al profesor sobre la asignatura. A pesar de que solo una minoría ha sido capaz de resolver el reto criptográfico en su totalidad, los alumnos han disfrutado enormemente del proceso colaborativo.

Como conclusiones se puede destacar, por un lado, que la wiki es una buena plataforma para la coordinación del criptoanálisis distribuido. Permite el trabajo en equipo, así como el trabajo personal, facilita mediante avisos de cambios a los participantes del reto y al profesor y visualiza de manera clara la evolución del ataque. La elección de la plataforma MoinMoin ha sido muy acertada ya que ha proporcionado todas las funcionalidades necesarias para desarrollar el reto criptográfico.

Por otro lado, el reto de encontrar la solución al ataque como actividad grupal ha sido un buen detonante para que los estudiantes reflexionen sobre las ventajas del principio de cooperación frente al paradigma de competición. Debido a estas reflexiones, interesantes conceptos han surgido en clase en torno a este tema y otros muy relacionados como la teoría de la evolución de las especies, la teoría de juegos o la economía basados en los estudios de autores como Richard Dawkings, John Forbes Nash y Lynn Margulis. En consecuencia, los estudiantes han demostrado una alta motivación ante el reto criptográfico.

Actualmente la siembra se realiza de modo colaborativo mientras que su resolución es individual. Como líneas futuras de investigación se quiere hacer que el reto sea en su totalidad colaborativo, incluso su resolución. Actualmente para evaluar al alumno se

[2] El alto porcentaje de participación en las encuestas se debe al hecho de que laasistencia a clase exime del examen final.

ISSN: 2385-6203

estudia el trabajo de resolución realizado en su espacio de wiki privado. Una evolución del reto podría ser que tanto las siembras como la resolución del resto fuesen procesos colaborativos. Los alumnos a través de foros de discusión sugerirían siembras para ser propuestas. Se necesitaría un foro que la wiki utilizada no dispone, pero existen muchas soluciones con licencias GNU disponibles[3]. De esta manera todos los participantes obtendrían la misma nota y la experiencia será puramente colaborativa sin competición alguna. Esta opción es altamente más compleja desde el punto de vista de la evaluación por parte del profesor pero realmente interesante a efectos de retos de innovación docente.

Por último, señalar el éxito aportado al desarrollo de la actividad gracias al hecho de contextualizar el reto criptográfico en el marco de un episodio de interés histórico. Los alumnos lo han acogido muy positivamente y ha afectado enormemente a su motivación.

5. REFERENCIAS BIBLIOGRÁFICAS

1: Turing, AM, Mathematical theory of enigma machine, 1940

2: Bruffee, Kenneth A., Collaborative learning: Higher education, interdependence, and the authority of knowledge, 1999

3: Moore, Dan Tyler y Waller, Martha Stifler, Cloak and cipher, 1962

4: Stinson, DR, Cryptography: Theory and Practice, 2002

5: Anderson, Ross, Stretching the limits of steganography, 1996

6: Klobas, Jane E , Wikis: tools for information work and collaboration, 2006

7: Ramió, Jorge, Libro electrónico de seguridad informática y criptografía, 2006

8: Xiao, WenPeng, ChangYan Chi y Min Yang, On-line collaborative software development via wiki." Proceedings of the 2007 international symposium on Wikis, 2007

[3] En http://es.wikipedia.org/wiki/Anexo:Softwares_de_foros_de_internet se puede encontrar un estudio comparativo de software de foros disponibles.