ACTO DE CLAUSURA DE LOS CURSOS DE MAYORES
AÑO ACADÉMICO 2008/2009
AULA MAGNA, CAMPUS DE GETAFE

CONFERENCIA DE CLAUSURA:

# HISTORIAS Y LEYENDAS DE LA ESCRITURA SECRETA

Sra. Vicerrectora, Sr. Director General, Autoridades, queridos amigos y compañeros, señoras y señores.

Cuando hace unas semanas me ofrecieron impartir esta conferencia, de inmediato pensé en tratar algún tema de mi actividad académica, la seguridad de la información o, particularizando más, en la criptografía, disciplina íntimamente ligada a lo que antiguamente se conocía como escritura enigmática.

Sin embargo, cualquier disertación acerca de esta materia, la criptografía, comporta unos conocimientos previos nada desdeñables en temas tan difíciles como la teoría de números, la teoría de la complejidad algorítmica, la teoría de la información (establecida por Shannon en 1948) y la estadística. Por ello, y para no corresponder a su gentileza al invitarme mortificándoles sin misericordia, decidí exponer, de la manera más amena posible, el devenir de la escritura secreta a través de algunos episodios de su ancestral historia.

La escritura permite que ideas, opiniones o hechos perduren en el tiempo, bien para dejar constancia de los mismos a la posteridad, o bien para transmitirlos a distancia sin pérdida de integridad. Sea por

uno u otro motivo, muy pronto el hombre debió de sentir la necesidad de ocultar a los ajemos sus escritos, aunque permitiendo su lectura a los propios. En ese momento apareció la escritura secreta, cuya historia, por tanto, se extiende desde hace milenios.

Cuando los escritos eran de índole política o militar, los motivos de esta ocultación eran obvios: de su encubrimiento podía depender la victoria en una batalla o el derrocamiento de un rey. En otras ocasiones, las razones para velar informaciones eran religiosas. Así, para algunos textos sagrados los judíos usaron los sistemas de encubrimiento conocidos como el Atbash (que encontramos en Jeremías: 25:26, 51:41, 51:1), el Albam (que está presente en Isaías: 7:6) y el Atbah (usado a menudo en el Talmud). A veces los fines eran encubrir escarceos amorosos, como se constata en el popular Kamasutra de Vatsvâyâna, que entre las 64 artes cuyo conocimiento recomienda a las mujeres incluye dos (la 45 y la 46) en las que instruye acerca de la ocultación de escritos o conversaciones. Una última finalidad a citar, ha sido el afán de ocultar valiosos descubrimientos, como la fórmula de la Coca-Cola o supuestos tesoros, como es el caso Beale.

También es muy destacable la presencia de la escritura secreta en ciertas obras maestras de la literatura. Es este el caso de “El Escarabajo de Oro” de Edgar Alan Poe, o de la “Aventura de los Bailarines” de Sir Arthur Conan Doyle (conocido creador de Sherlock Holmes) o, más recientemente, de “El nombre de la Rosa” del semiólogo y novelista Umberto Eco.

Sea como fuere, los primeros precedentes de esta escritura se hallan en la XII dinastía del Antiguo Egipto (aproximadamente 2.000 años a. C.), durante el apogeo del Imperio Medio. Concretamente, el primero de tales escritos se halla en la tumba de de Khnumhotep, comarca del Faraón Amenemhet II (*c.a.* 1.900 a. C.). En dicha tumba se hallan numerosos epitafios epigramáticos con jeroglifos inusuales –pero legibles con un plus de atención–, cuyo propósito no está claro hoy en día. Podía ser despertar el interés del lector por lo escrito, o bien ensalzar la figura del difunto o quizás encumbrar al propio escriba, dueño de tal dominio de la lengua. Está misma tónica deliberada de confundir los jeroglifos se mantuvo desde entonces hasta el final del Imperio Egipcio.

A partir de entonces, los diversos modos de encubrimiento de la información se fueron reduciendo y sistematizando en dos grandes grupos: aquellos en los que se oculta el propio texto o aquellos que lo transforman (sin ocultarlo) para imposibilitar su interpretación.

Ejemplos de aquellos (los que ocultan el texto) se encuentran con profusión en los escritos de los más notables historiadores griegos. Así, Herodoto (el padre de la Historia), Jenofonte o Tucidides nos han dejado numerosos testimonio de su uso. A modo de ejemplo, el primero de ellos cuenta en el VII libro de su obra “Los nueve libros de la Historia”, cómo los griegos fueron advertidos durante la II Guerra Médica de un inminente ataque del Rey de Reyes Persa Jerjes. En Susa (ciudad de Persia) vivía Demarato espartano exiliado, pero aun así amante de su patria, que enterado del propósito de Jerjes, resolvió avisar a sus compatriotas. En esta tesitura, el problema era cómo enviar un mensajero que cruzando el

Asia Menor y navegando por el Egeo llegase a Grecia sin que su mensaje fuese interceptado por los guardias persas. Para resolverlo, Demarato –en palabras prestadas por Herodoto–:

> "Tomó un cuadernillo de dos hojas o tablillas; rayó bien la cera que las cubría, y en la madera grabó con letras la resolución del rey. Hecho esto, volvió a cubrir con cera regular las letras grabadas, para que el portador del cuadernillo en blanco no fuera molestado por los guardas de los caminos" (fin de la cita).

No es superfluo advertir que estas tablillas de madera, recubiertas de cera por una cara, fueron muy usadas durante toda la Antigüedad como un soporte portátil y reutilizable de escritura. Una representación de estas tablillas se tiene en uno de los murales mejor conservados de Pompeya, donde se ve a una joven pareja cuya mujer porta una de estos instrumentos.

En todo caso, y siguiendo con nuestra historia, los griegos, advertidos de este modo, hicieron hacer frente a los persas en las mejores condiciones, venciéndoles en la famosa batalla naval de Salamina.

El mismo Herodoto nos relata, en esta ocasión en el libro V de la obra citada, otra peripecia similar, aunque anterior, con el griego Histaeio de protagonista. Deseando éste que Aristágoras, tirano de Mileto, se rebelase contra Dario I de Persia (padre del aludido Jerjes), rapó el pelo a un esclavo le tatuó en el cuero cabelludo un mensaje instando a Aristágoras a levantarse y, tras esperar a que le

creciese el pelo, le envió a su destino sin temor a que se descubriese el complot. Nuevamente en palabras de Herodoto:

> "[Histeio] había rasurado a navaja la cabeza del criado, habíale marcado en ella los puntos y letras, esperó después que le volviera a crecer el cabello y, crecido ya, habíalo despachado a Mileto sin más recado que decirle a [Aristágoras], cortándole a navaja el pelo, le mirara la cabeza" (fin de la cita).

Estos métodos que imposibilitaban la misma visión de los textos se han usado en todas las civilizaciones. Por ejemplo, los chinos solían escribir los mensajes secretos sobre un trozo de tela, que tras plegarse se envolvía en cera formando una pelotita que era engullida por el portador, tal y como hoy hacen –obviamente con otra finalidad– los camellos de la droga (aunque con la tranquilidad de no poder ser detectado el cargamento por unos rayos X inexistentes en aquel entonces). El procedimiento de descifrado, por escatológico, es preferible obviarlo.

Más cercano en el tiempo, se empiezan a usar las tintas simpáticas, aún usadas en la actualidad. Estas tintas son definidas en el diccionario de la RAE del siguiente modo:

> "Composición líquida que tiene la propiedad de que no se conozca lo escrito con ella hasta que se le aplica el reactivo conveniente".

Un ejemplo de este sistema fue ideado durante el Renacimiento por el napolitano Giovanni _ella Porta y usado en esta República durante el s. XVI: Se comienza cociendo un huevo, y a continuación

se disuelve piedra de alumbre (como la que todavía se usa para cortar pequeñas hemorragias, como las producidas al afeitarnos) en vinagre formando así una tinta con la que escribir un mensaje en la cáscara del huevo duro. Al ser esta cáscara porosa, absorbe el líquido sin quedar rastro del mismo. Basta con descascarillar el huevo para que en la clara aparezca el mensaje.

En España, un libro muy ilustrativo es “Poligrafía o arte de escribir en cifra de diferentes modos”, del catedrático de Taquigrafía Francisco de Paula Martí Mora (Játiva, 1761 – Lisboa, 1827). Este setabense (que goza de una calle en el centro de Valencia y cuyo busto se erige en el madrileño Parque de El Retiro a 50 metros de la entrada por la puerta de América), expone multitud de exóticas composiciones de tintas secretas, que nos dan idea de los métodos usados por nuestros antepasados. Por ejemplo, se puede leer allí:

> “Se toma una agalla fina, se la quebranta, se pone en infusión por espacio de hora y media o dos horas en una xícara o vaso con un dedo de agua común; o si no, se escoge una agalla gorda y bien sólida, y se la hace un agujero o concavidad de quatro o cinco líneas de diámetro, y se llena de agua, dexándola en esta forma por el tiempo que queda dicho. Se corta una pluma nueva, y se moja en el agua de la agalla (que sirve de tintero), o en la infusión arriba dicha, para escribir lo que se quiera sobre un papel que tanga suficiente cola para no calarse.
>
> El papel escrito de este modo queda tan blanco, que apenas se seca nada se percibe en él, y quando se quiera que aparezca lo escrito, no se hace más que disolver en agua un poco de vitriolo común, mojar una espongita y pasarla por

encima del papel, y al instante se verán aparecer los caracteres tan negros como si se hubiesen escrito con tinta" (fin de la cita).

En todo caso, los métodos de ocultación más empleados hoy en día son los de cifrado (que no encriptado, como dicen algunos mientras patean el diccionario de nuestra Academia). Estos métodos son objeto de estudio en la criptografía (del griego kripto, oculto, y grafía, trazo) que es la disciplina que estudia los métodos de ocultar la información contenida en un mensaje. O bien, si se prefiere la definición del diccionario de la RAE:

"Arte de escribir con clave secreta o de un modo enigmático"

Nótese, que –a diferencia de los métodos tratados hasta ahora–, no se pretende encubrir un mensaje, sino su contenido, de modo que aunque se vea no se pueda entender lo que dice. Los especialistas en el cifrado se denominan criptógrafos y, al contrario, aquellos que estudian los modos de descifrar un texto sin estar en el secreto de ninguna otra información adicional, criptoanalistas.

Los espartanos (también conocidos por lacedemonios) fueron los primeros en usar sistemáticamente un dispositivo de cifrado (*c.a* 400 a. C.), según cuenta el historiador griego Plutarco en sus "Vidas Paralelas: Lisandro-Sila". El dispositivo, conocido como escítala lacedemonia, consistía en un bastón de determinado diámetro a todo lo largo del cual se enrollaba (a modo de venda) una estrecha tira de papiro, sobre la que se escribía un mensaje siguiendo el sentido longitudinal del bastón así vendado. Tras ello, bastaba con desenrollar la tira para que las letras quedasen desordenadas,

haciendo el mensaje ilegible, o sea, indescifrable. Sólo si el receptor poseía un bastón del mismo grosor podía volver a enrollar la tira y recuperar el mensaje. Como curiosidad, parece que éste es el origen del llamado bastón de mando de los generales.

Pero debemos esperar aún tres siglos para que Julio César (s. I a. C.) nos legue el método de cifrado con el que, todavía hoy en día, se comienzan las asignaturas de criptografía en las universidades. El método, como explica el historiador Suetonio (s. I d. C.), consistía en la sustitución de cada letra del mensaje por aquella otra situada tres posiciones por delante de ella en el alfabeto (es decir, sustituir A por D, B por E y sucesivamente hasta las tres últimas X, Y y Z cambiadas respectivamente por las tres primeras, A, B y C). Aunque el procedimiento parezca hoy de una trivialidad casi infantil, en el siglo I a. C. –con la mayor parte de la población analfabeta–, era prácticamente ilegible. Obviamente, el método se podía generalizar simplemente intercambiando cada letra por otra aleatoriamente escogida (naturalmente evitando sustituir dos letras distintas por la misma), sin seguir ningún patrón uniforme como el del método César.

Es interesante destacar que estos métodos –denominados genéricamente de sustitución– tuvieron una larga vida, pues no fue sino hasta el siglo VIII cuando las escuelas coránicas de Bagdad descubrieron que todas las lenguas tienen una frecuencia característica de aparición de las letras de su alfabeto. Así, por ejemplo, la “e” es la letra más frecuente en español (en un texto suficientemente largo, en torno al 12% de letras son “e”), por lo que bastaba con poseer una tabla con estas frecuencias para poder

identificar cada letra de un texto, aunque se presentase con un aspecto distinto. Por ejemplo, usado el citado método César una “e” se presenta como una “h”, pero eso no evitará que sean “h” doce letras de cada 100, lo que indicará que realmente nos encontramos frente a una “e”. Obviamente conociendo esta tabla de frecuencias para cada idioma es elemental romper este tipo de cifrados.

Tras esta introducción, es hora ya de tratar varios episodios muy significativos de la historia de la criptografía.

El primero de ellos nos lleva al s. XVI, cuando las tensiones entre Inglaterra y Escocia, los dos grandes reinos que componían la actual Gran Bretaña, se habían exacerbado, pues a las tradicionales disputas territoriales se había añadido las religiosas, consecuencia de la conversión de Inglaterra al protestantismo. En la segunda mitad de dicho siglo, los enfrentamientos tenían como protagonistas a dos primas hermanas: Isabel Tudor, Reina de Inglaterra y María Estuardo, Reina de Escocia. Tras años de luchas contra Inglaterra e intrigas palaciegas en Escocia, la bella, encantadora y desdichada María huyendo de los enemigos que tenía en su propio reino penetró en Inglaterra donde fue prendida por su prima Isabel y encerrada durante años en el castillo de Sheffield, durante los que fue sometida a un durísimo régimen.

Sin embargo, los católicos ingleses vieron a María como una oportunidad para la reconversión de su país al catolicismo. En efecto, no estando casada Isabel (es conocida como la Reina Virgen, por su resistencia al matrimonio) y careciendo la dinastía Tudor de candidatos con mejor derecho, caso de morir Isabel, sería

María la heredera del trono inglés, además del escocés que ya le pertenecía.

Dirigiendo a los conspiradores católicos, David Babbington, diseñó un plan para asesinar a Isabel y simultáneamente liberar a María. Para comunicarse con ésta Babbington creo una cifra aparentemente muy robusta, con la que escribía sus notas que eran confiadas a un mensajero llamado Gilbert Gifford. Lamentablemente para los conspiradores Gifford era un agente al servicio del secretario de la Reina Virgen, el poderoso y cruel Francis Walshingan, para quien trabajaba uno de los más conspicuos criptoanalistas del siglo, Thomas Phelippes, quien logró descifrar todas las misivas.

Llevada a juicio la Reina María bajo el cargo de rebelión, las pruebas fueron concluyentes, siendo condenada a morir decapitada. Así, en 1587, a los 45 años, y tras casi veinte de indigno encarcelamiento, fue conducida al cadalso, donde la desdichada Reina mantuvo hasta el último momento una admirable dignidad, de la han dado testimonio los historiadores.

Para el siguiente acontecimiento, muy arraigado en las leyendas populares, es preciso trasladarnos a la Francia de un siglo más tarde, el XVII, donde tiene lugar un suceso intrigante, objeto de innumerables hipótesis y fabulaciones. Me refiero al confinamiento en la fortaleza de Pignerole (Pinerolo) de la región de Saboya y posterior traslado a la Bastilla (en 1698) de un anónimo personaje cuyo rostro se ocultaba bajo una cruel máscara de hierro, aunque según otros era simplemente de tela. El enigmático personaje salía

unas pocas horas para pasear totalmente aislado por el adarve de Pinerolo y ni eso desde que fue encarcelado en la Bastilla. Naturalmente tan insólito hecho despertó la curiosidad y las habladurías de los más, según los cuales el misterioso individuo sería el hermano gemelo segundogénito de Luis XIV, el todo poderoso Rey Sol, exponente máximo del absolutismo.

El caso seguía dando que hablar casi un siglo después, hasta el extremo de que el gran Víctor Hugo comenzó a escribir una obra de teatro, de nombre Gemelos, que abandonó al conocer que Alejandro Dumas –ya escritor de éxito por su Conde de Montecristo– había tratado ya el tema del supuesto gemelo –bien es verdad que tangencialmente–, en la tercera parte de su trilogía “Los tres mosqueteros”. Además, y como es sabido, el morbo del tema también ha interesado la industria cinematográfica que ha producido seis películas con este argumento, la última, en 1998, de título “El hombre de la Máscara de Hierro”, protagonizada, entre otros, por Leonardo DiCaprio y Gerard Depardieu.

Pero volviendo a nuestro relato, la realidad del mismo es mucho más prosaica y sólo se conoció al romperse el cifrado conocido como la Gran Cifra. Ésta fue desarrollada por dos eminentes criptógrafos Antoine y Bonaventure Rossignol (padre e hijo respectivamente) que trabajaron al servicio de Luis XIII y Luis XIV. El sistema de cifrado consistía en sustituir cada sílaba por un número dado de entre miles. No obstante su gran seguridad, a la muerte de sus creadores esta cifra cayó en el olvido, hasta el punto de que importantes textos del absolutismo permanecieron vedados para los estudiosos durante más de siglo y medio.

Afortunadamente para la Historia, en 1890 aparecieron un gran número de cartas así cifradas, que aparentemente eran un galimatías de miles y miles de números, de los cuales sólo 587 eran distintos. Entregada esta correspondencia al criptoanalista Etienne de Bezeries, consiguió romper la cifra tras tres años de ininterrumpidos esfuerzos. Entre estas cartas cifradas se hallaba una de Francois de Louvois, Ministro de la Guerra, dirigida al Rey Sol, en la que relataba la deserción del general Vivian de Bulonde dejando a sus tropas abandonadas en el sitio de Cuneo (en el Piamonte), durante la guerra de sucesión austríaca. El Ministro concluía su carta rogando al Monarca el arresto del general para ser conducido “a la fortaleza de Pinerole, donde le encerrarán en una celda guardada por la noche, permitiéndosele caminar por las almenas durante el día cubierto con una máscara”. Con ello, y aunque algunos mantienen un cierto escepticismo, el caso del hombre de la máscara de hierro parece estar concluido.

Nuestro siguiente caso nos desplaza nuevamente a un siglo más tarde y sucede en EE UU.

Allí se publica una de las cifras más enigmáticas y que más ha fascinado y ocupado a criptógrafos tanto profesionales como aficionados en los últimos 120 años: Es la conocida como Beale. Sucintamente contada, la leyenda comienza en 1822 cuando un misterioso vaquero, Thomas J. Beale deposita en un hotel de Lynchburg, Virginia, un cofre cerrado. Meses más tarde el dueño del hotel, Robert Morriss recibe una misiva del tal Beale comunicándole que diez años más tarde recibiría una carta con instrucciones de

abrir el cofre y de como leer su contenido. Sobrepasado ampliamente el plazo sin recibir dicha carta, en 1845 Morriss se decide a abrir el cofre, hallando una nota en inglés corriente y tres folios de texto cifrado constituidos íntegramente por multitud de números de uno, dos o tres dígitos. Estos folios son conocidos como primera, segunda y tercera cifra Beale y, según la nota, contenían respectivamente la ubicación de un tesoro, su descripción y una lista de allegados a los que hacérselo llegar. Tras casi 20 años de infructuosos intentos, Morriss contó los hechos a un amigo, de identidad desconocida, que tras otros 20 años logró desvelar el segundo cifrado –que como se recordará describía la fortuna–, siendo vanos sus esfuerzos para descubrir su posición geográfica. Finalmente, en 1885, publicó, manteniendo el anonimato, un folleto de 23 páginas que narraba pormenorizadamente los sucesos desde la primera llegada a Virginia de Beale. Desde aquél 1885 han sido multitud los criptógrafos, profesionales y aficionados, que han velado tratando de quebrar los enigmáticos folios primero y tercero. Incluso existe una sociedad norteamericana cuyos miembros son devotos analistas de dichos cifrados Además, como el segundo texto señalaba que la fabulosa fortuna se hallaba enterrada en el condado de Badford a 4 millas de Bufford no es de asombroso que miles de aventureros se lanzasen a su búsqueda horadando desde hace 120 años – hasta dejarlo cual un queso de Gruyere – el terreno circundante a Bufford.

Aunque se puede pensar que los cifrados primero y tercero son una impostura –y así lo creen muchos estudiosos–, otros indicios científicos –basados en análisis de frecuencias y la aleatoriedad de

ambos textos– apuntan a la veracidad de la historia contada por Beale.

En cualquier caso, merece la pena comentar el método de encubrimiento de la segunda cifra, ya que muestra el ingenio del amigo anónimo de Morriss, que descubrió que la clave de descifrado se encontraba en la “Declaración de Independencia de los EE UU”. Recordando que los cifrados Beale están constituidos por números, y numerando las 1322 palabras de que consta la Declaración, para hallar la letra que corresponde a un número cualquiera basta con contar hasta llegar a la palabra cuyo número coincide con aquel y extraer su primera letra que será la buscada.

Lamentablemente búsquedas similares con otros documentos no han tenido éxito, aunque pudiera ser que Beale hubiese efectuado u doble cifrado transformando dos veces el texto hasta ahora secreto. Aún peor, podría haber redactado un documento y tomado con clave para obtener los textos aún vírgenes. Quizás nunca sepamos la verdad de lo que hoy es una leyenda, la del cifrado Beale.

Para concluir con estas historias debemos irnos al Océano Pacífico, durante la II Guerra Mundial, para tratar un suceso que ilustra las numerosas variaciones de los procedimientos de cifrado, alguno de los cuales, como el que vamos a comentar, muestra como se puede cifrar sin conocer ninguna técnica especial para ello.

En el año 2002 se estrenó la película “The Windtalkers”, que narra el papel de los indios navajos en la Guerra del Pacifico, que durante la II Guerra Mundial enfrentó a las tropas aliadas y al Imperio del

Sol Naciente. La narración comienza el 7 de diciembre de 1941, con el devastador ataque nipón a la base de Pearl Harbour. En pocas semanas las fuerzas imperiales habían conquistado Guam, Guadalcanal, parte del archipiélago de Salomón, Hong-Kong y las islas Filipinas. Cuando los EE UU reaccionaron y comenzaron su ofensiva se hallaron en un escenario muy diferente del europeo en el que ya combatían. En las batallas, más que divisiones enteras, luchaban compañías en frentes cambiantes en los cuales los equipos de cifrado, voluminosos y pesados, eran inoperantes. Además, el proceso de cifrado era laborioso: el auxiliar de cifrado debía teclear el mensaje, anotar la salida y pasársela al operador de radio para que la transmitiera a su interlocutor, quien iniciaba el proceso inverso.

Afortunadamente para los aliados, los estadounidenses retomaron una idea experimentada en pequeña escala durante la I Guerra Mundial. Escogerían una lengua hablada por unos pocos individuos y la usarían directamente traduciendo cualquier mensaje a ella. Naturalmente, cualquier escucha desconocedor de dicha lengua, pensaría que se encontraba ante un cifrado con las consiguientes dificultades de traducción. En EE UU las únicas lenguas escasamente habladas eran las de los indios navajos, de los sioux, de los chippewas y de los primo-papagos. De todas eligieron el navajo, pues eran la única que no había sido investigada por estudiantes alemanes de antropología entre la I y la II Guerra Mundial, quizás advertidos del uso de estas lenguas durante la Gran Guerra.

De este modo, a finales de 1942 eran más de cien los indios navajos que estaban desplegados por todos los frentes, siempre protegidos por otro compañero con la misión de evitar que cayesen prisioneros del enemigo y, con toda probabilidad, con la consigna de ejecutarlos antes de que tal ocurriese.

Para el ajeno al mundo de la seguridad de la información resulta curioso que a pesar de los enormes servicios prestados por estos ejemplares soldados, su misión fue sigilosamente preservada hasta 1968. Años después, en su honor los EE UU declararon el 14 de agosto “Día de los mensajes en código navajo”. Se debe resaltar que esto no es inusual, y que a menudo, en la escritura secreta, más enigmáticos que la misma lo son sus profesionales.

Para concluir esta lección es imprescindible citar que estar técnicas ancestrales, y en particular el cifrado, es hoy en día una práctica cotidiana. Cada vez que mantenemos una conversación a través de un teléfono móvil, pagamos con una tarjeta de crédito o débito, nos conectamos a nuestro banco para realizar una operación en nuestra cuenta, compramos en un servidor de los llamados seguros, introducimos nuestra contraseña en un ordenador, etc. estamos cifrando, eso sí, muy a menudo inadvertidamente. Además, esta técnica adicionalmente a proteger nuestro dinero, es insustituible para mantener nuestra intimidad –tan amenazada– a cubierto de ojos extraños y a menudo maliciosos.

Arturo Ribagorda Garnacho

Getafe 28 de mayo de 2009