# Criptografía Tropical

Jessica Paola Barbosa Torres

## Prólogo

La cryptographie est un auxiliaire puissant de la tactique militaire.

Général Lewal, Études de guerre

Cuando uno menciona la palabra y explica que su objetivo es proteger la información transmitida entre dos actores para que nadie más que ellos entienda el mensaje, las personas inmediatamente piensan en cosas como o en la máquina durante la Segunda Guerra Mundial. En el imaginario colectivo, la criptografía está asociada solamente a secretos de Estado o a comunicación en tiempos de guerra. Sin embargo, el hecho de que muchos de los criptosistemas que conocemos hayan surgido en un contexto militar no significa que su uso a lo largo de los siglos haya estado limitado sólo a ese ámbito. El querer ocultar información de los demás es tan innato a los hombres como el mismo acto de buscar comunicarnos; en ocasiones es tan importante el transmitir un mensaje a otro como el que únicamente esa persona tenga conocimiento de él. Un ejemplo simple de esto son los alfabetos secretos que las niñas de 10 años inventan para intercambiar cartas o escribir diarios.

La historia de la criptografía es más larga de lo que podríamos suponer. Muestra de ello es su presencia en el Kama Sutra [**?**] como una de las 64 actividades que una buena esposa debe dominar. En la antigüedad, además de la criptografía, era común el uso de la , que busca esconder objetos dentro de otros. Un ejemplo de ello son las diversas técnicas para ocultar cartas dentro de las ropas de un mensajero o los tatuajes en el cuero cabelludo de esclavos rapados. Durante la Edad Media, no hubo grandes avances en materia de criptografía, pues, con tantas acusaciones de brujería, resultaba más riesgoso escribir textos ininteligibles que enviar cartas con algún sirviente de confianza y esperar que no fueran interceptadas. Fue hasta la época del Renacimiento que la criptografía fue reconocida y utilizada de manera abierta, principalmente como modo de comunicación entre gobernantes y militares. Por ejemplo, cuenta Kahn en [**?**] que tanto en tiempos del Cardenal Richelieu en el siglo XVII como de Napoleón Bonaparte un siglo después, existían academias militares en las que se enseñaba criptografía a los soldados franceses. Sin embargo, existen en la literatura algunos ejemplos aislados anteriores al siglo

XX que muestran que no sólo los gobernantes y militares hacían uso de métodos criptográficos[1].

A pesar de estos pocos ejemplos, durante muchos años, la mayoría de los métodos que se creaban y perfeccionaban surgían a partir de necesidades relacionadas con inteligencia militar. No fue sino hasta la década de 1960-1970 que se generalizó la necesidad de implementar criptosistemas para la seguridad del público en general. Con la proliferación de las computadoras surgió la necesidad de proteger la información digital que no sólo bancos y grandes empresas estaban generando, sino también personas comunes. Muestra de ello es el establecimiento en la década de los setenta por parte del gobierno de los Estados Unidos de un estándar de encriptación para información no clasificada. A partir de entonces, se han hecho muchos avances en materia tanto de criptografía como de criptoanálisis que se basan en la dificultad de resolver computacionalmente ciertos problemas. Algunos de ellos serán mencionados más adelante.

Definitivamente, el interés por preservar la seguridad de la información no es reciente. Sin embargo, hoy en día ha dejado de ser algo que interese sólo a los altos mandos militares. De hecho, también ha dejado de ser algo que incumba únicamente a quienes diseñan software. Empresas y gobiernos difunden campañas advirtiendo a la población sobre los riesgos de proporcionar contraseñas a extraños y cada día se establecen nuevas estrategias para que las transacciones de dinero por Internet sean más seguras. A diferencia de lo sucedido en décadas anteriores, los métodos que se implementan actualmente requieren cada vez más de usuarios responsables e informados que hagan un buen uso de ellos.

La criptografía requiere en nuestros tiempos de la colaboración de investigadores de muchas áreas del conocimiento. La necesidad de tener dispositivos transmitiendo información entre sí ha hecho de ella algo más que el simple ocultar mensajes de posibles intrusos; también involucra, por ejemplo, protocolos de autentificación, para garantizar que las personas con quienes nos comunicamos sean quienes dicen ser. Así, nosotros como matemáticos, entre otras cosas, diseñamos junto con los ingenieros algoritmos que se basan en la dificultad computacional de resolver ciertos problemas, pero es importante tener en mente que en el momento de implementarlos están presentes, desde posibles ataques o errores en las computadoras, hasta aspectos legales, administrativos e incluso psicológicos.

El que la criptografía sea algo de uso tan generalizado en nuestros días permite que cada vez más personas se involucren en el diseño de métodos más seguros y eficientes. En general, se busca que el único modo de romper los métodos que se proponen sea probando todas las llaves posibles y que haya tantas de éstas que incluso las computadoras más poderosas tarden meses o incluso años en hacerlo.

En este trabajo estudiaremos un algoritmo de encriptación y otro de intercambio de llaves propuestos por Dima Grigoriev y Vladimir Shpilrain [**?**] que se basan en

[1] Algunos ejemplos son , de Honoré de Balzac; de Edgar Allan Poe y el gran cuento de Sir Arthur Connan Doyle, , entre otros.

*álgebras tropicales*. En el primer capítulo se da una introducción a las álgebras tropicales y se presentan conceptos sobre complejidad computacional, con base en [**?**], [**?**], [**?**], [**?**] y [**?**]. En el capítulo 2 se presenta un breve resumen histórico sobre el desarrollo de la criptografía, con base en [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**] y [**?**]. En los capítulos 3 y 4 se exponen los antecedentes matemáticos en que se basa la criptografía tropical a partir de las siguientes fuentes: [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**] y [**?**]. En el capítulo 5 se plantean los algoritmos estudiados y se discuten los resultados obtenidos al implementarlos en MATLAB y realizar algunas pruebas con MAPLE. El código utilizado para ello se incluye al final de este documento a modo de anexo al igual que definiciones básicas sobre expresiones booleanas, con base en [**?**]. Finalmente, se presentan algunas conclusiones respecto al trabajo realizado.

50


Akian, M., Gaubert, S. y Guterman, A. (2009) *Linear Independence Over Tropical Semirings and Beyond* en Proceedings of the International Conference on Tropical and Idempotent Mathematics. Volumen 495, pp. 1-38, Series in Contemporary Mathematics. AMS.

Berstel, J., Perrin, D. y Reutenauer, C. (2011) *Codes and Automata - Theory of Codes*. Volumen 129 de la Encyclopedia of Mathematics and its Applications. Cambridge Univ. Press.

Boneh, D. (1999) *Twenty Years of Attacks on the RSA Cryptosystem* en Notices of the American Mathematical Society, Volumen 46, No. 2, pp. 203-213. AMS. Butkovi, P. (2010) *Max-linear Systems: Theory and Algorithms*. Springer-Verlag. Cook, S. (1971) *The complexity of theorem proving procedures* en Proceedings of the Third Annual ACM Symposium on Theory of Computing, pp. 151-158. ACM. Cravioto, M. (2008) *Problemas $\mathcal{NP}$ − completos*. Tesis para obtener el título de Licenciada en Matemáticas Aplicadas. ITAM.

Develin, M., et al. (2005) *On the Rank of a Tropical Matrix*. Combinatorial and Computational Geometry, Vol. 52. MSRI Publications.

Fraleigh, J. (2002) *A First Course in Abstract Algebra*. Addison Wesley, 7ma. edición.

Gaubert, S, et al. (2011) *Tropical Lineal-Fractional Programming and Parametric Mean Payoff Games*. Preimpresión. Disponible en , consultado el 25 de agosto de 2011.

Grigg, N. y Manwaring, N. (2007) *An Elementary Proof of the Fundamental Theorem of Tropical Algebra*. Preimpresión. Disponible en , consultado el 25 de agosto de 2011.

Grigoriev, D. y Shpilrain, V. (2010) *Tropical Cryptography*. Preimpresión. Disponible en , consultado el 25 de agosto de 2011.

Haase, C., Musiker, G y Yo, J. (2011) *Linear Systems on Tropical Curves*. Disponible en , consultado el 25 de agosto de 2011.

Hogg, T. (1999) *Solving Highly Constrained Search Problems with Quantum Computers* en Journal of Artificial Intelligence Research, Volumen 10, pp. 39-66. AAAI Press. Johnson, M. y Kambites, M. (2009) *Multiplicative Structure of* $2 \times 2$ *Tropical Matrices*. Reporte técnico disponible en , consultado el 25 de agosto de 2011.

Kahn, D. (1996) *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 2da. edición.

Kammer, R. (1999) *Data Encryption Standard (DES)*, FIPS-Pub.46-3. U.S. Department of Commerce. National Institute of Standards and Technology Kato, T. (2011) *An Asymptotic Comparison of Differentiable Dynamics and Tropical Geometry*. Mathematical Physics, Analysis and Geometry. Volumen 14, No.1, pp.39-82. Springer

Kerckhoffs, A. (1883) *La Cryptographie Militaire*. Journal des sciences militaires, Volumen IX, pp. 5-38, disponible en , consultado el 11 de mayo de 2012.

Kelly, T.(1998) *The Myth of the Skytale* en Cryptologia, Volumen 22, No. 3, pp. 244-260. Taylor & Francis. Lewal, J. (1881) *Études De Guerre. Tactique Des Renseignement*. Disponible en , consultado el 11 de mayo de 2012.

Litvinov, G. (2007) *The Maslov Dequantization, Idempotent and Tropical Mathematics: A brief introduction* en Journal of Mathematical sciences. Volumen 140, No. 3, pp. 426-444. Springer.

Maclagan, D. y Sturmfels, B. (2009) *Tropical Geometry*. Preimpresión. Disponible en: , consultado el 25 de agosto de 2011.

Menezes,A., Van Oorschot, P. y Vanstone, S. (2001) *Handbook of Applied Cryptography*. CRC Press, 5a. reimpresión.

Mikhalkin, G. (2006) *Tropical Geometry and its Applications*. Disponible en: , consultado el 25 de agosto de 2011.

Pachter, L. y Sturmfels, B. (2004) *Tropical Geometry of Statistical Models*. Proceedings of the National Academy of Sciences of the USA. Volumen 101, No. 46, pp. 16132-16137. PNAS.

Pin, J.-E. (1994) *Tropical semirings* en Idempotency, Volumen 11 de Publ. Newton Inst., pp. 50-69. Cambridge Univ. Press.

Pommerening, K. (2006) *Kasiski's Test: Couldn't the Repetitions be by Accident?* en Cryptologia, Volumen 30, No. 4, pp. 346-352. Taylor & Francis. Puente, M. J. (2010) *Tropical Linear Maps on the Plane*. Preimpresión Disponible en: , consultado el 25 de agosto de 2011.

Rajaraman, A., Leskovec, J. y Ullman, J. (2012) *Mining of Massive Datasets*. Disponible en: , consultado el 26 de agosto de 2012.

Richter-Gebert,J., Sturmfels, B. y Theobald, T. (2003) *First Steps in Tropical Geometry*. Disponible en: , consultado el 25 de agosto de 2011.

Simon, I. (1998) *Recognizable Sets With Multiplicities in the Tropical Semiring* en Lecture Notes in Computer Science. Volumen 324, pp. 107-120. Springer.

Speyer, D. y Sturmfels, B. (2004) *Tropical Mathematics.* Notas sobre una conferencia dictada por Sturmfels en el Clay Mathematics Institute. Disponible en: , consultado el 25 de agosto de 2011.

Stickel, E. (2005) *A New Method for Exchanging Secret Keys* en las memorias de la Third International Conference on Information Technology and Appplications (ICITA05), Volumen 2, pp. 426-430. IEEE Computer Society. Suetonio, C. (¿119-122?) *Vidas de los Césares.* Ediciones Catedra, 3a. edición. Vatsayana. (2011) *The Kama Sutra of Vatsyayana.* Empire Books. Pág. 7.

Whitesitt, J. (2010) *Boolean Algebra and its Applications.* Dover Publications.