# Educación en Tecnología y Matemática en Criptografía. Puntos de Encuentro

**Juan Carlos Canavelli, María Magdalena Añino,**
Departamento de Matemática. Facultad de Ingeniería (Bioingeniería).
Universidad Nacional de Entre Ríos.
Ruta Prov. Nº 11-Km. 10- ORO VERDE, Dpto. Paraná
Dirección Postal: C.C. 47 Suc.3 (3100)
e-mail: marjuan@arnet.com.ar
e-mail: maena@gigared.com,

## Resumen

En este artículo narramos la experiencia vivida, trabajando en la búsqueda de puntos de encuentro entre la Matemática y la Informática que permitan articular a su vez la Escuela Media con la Universidad. Las actividades se desarrollaron en el marco del Proyecto denominado "Universidad-Escuela Media: una complejidad para compartir II", implementado por la Secretaría Académica de la Universidad Nacional de Entre Ríos junto con el Consejo General de Educación de dicha provincia, durante el año 2004.
Se puso el énfasis en la "Teoría Elemental de Números". Temas básicos de esta parte de la Matemática son los siguientes: Divisibilidad. Sistemas de numeración. Máximo común divisor. Algoritmo de Euclides. Números Primos. Teorema fundamental de la Aritmética. Congruencias. Congruencias con incógnitas. El teorema chino del resto. El pequeño teorema de Fermat. El teorema de Euler-Fermat. Estos temas no siempre reciben en la Escuela la atención que merecen. Nos referimos a los niveles tanto elemental como medio. Esta situación debe corregirse, pues la Aritmética posee una extensa tradición histórica y es hoy una herramienta fundamental en el dinámico campo de las Tecnologías de la Información (podemos decir que todos los temas enunciados precedentemente intervienen para explicar uno de los sistemas más utilizados hoy para cifrar mensajes, el llamado sistema RSA en honor a sus creadores: Rivest, Shamir y Adleman).

*Palabras clave*:
Educación Matemática, Criptografía, Articulación Universidad - Escuela Media, Nuevas Tecnologías.

## 1. Introducción

Una realidad compleja y contrastante se percibe hoy en cuanto a la inserción de las nuevas tecnologías en las diferentes áreas de nuestra sociedad. Por un lado la Informática se ha instalado en la vida cotidiana, desde el supermercado, al pago de servicios, hasta las comunicaciones. INTERNET y el correo electrónico son ampliamente usadas por un basto sector de la sociedad y en especial por los jóvenes. "El locutorio ha pasado a ser la plaza del siglo XXI", expresó al respecto el Sociólogo y docente de la Universidad de Buenos Aires Luis Alberto Quevedo, quién además agregó, el celular se instaló en la escuela, desafiando a esta institución, quien deberá encontrar la forma de administrar y usar provechosamente estas nuevas tecnologías, valiéndose de la inclinación y curiosidad manifiesta por los alumnos hacia ellas. Por otro lado la Matemática ciencia que ha estado medularmente vinculada a Informática desde sus orígenes no goza de la misma popularidad. En todos los niveles educativos, la Matemática es una de las disciplinas más temida por la mayoría de los alumnos y en muchos casos es el factor determinante en la elección de una carrera o de la deserción de los estudios en los primeros años de la Universidad. Al respecto

son numerosos los estudios realizados por las Universidades Nacionales referidos a la problemática del ingresante. En este sentido la Facultad de Bioingeniería de la Universidad Nacional de Entre Ríos ha venido desarrollando un análisis de los diferentes aspectos del problema. Si bien se ha detectado que las causas del abandono durante el primer año pueden responder a múltiples factores, podríamos categorizarlos en dos tipos: los relacionados con el contexto personal (económicos, desarraigo, falta o inadecuada orientación vocacional,.....), y aquellos institucionales que involucran tanto a la Escuela Media como a la Universidad y que tienen que ver, entre otros, con la forma en que se articulan ambos niveles de enseñanza. Esta situación está caracterizada por: la dificultad en el cursado y aprobación de materias básicas, el insuficiente nivel de formación de los ingresantes, como así también la falta de entrenamiento para desarrollar actividades basadas en el razonamiento [1].
Por lo tanto, esta circunstancia nos demanda, como docentes de Matemática en los primeros años de la formación universitaria, no sólo repensar nuestras estrategias y prácticas sino explorar nuevos puntos de articulación entre los diferentes niveles de la enseñanza que contemplen los cambios culturales y tecnológicos en los cuales estamos inmersos.

## 1.1 Reorientando la enseñanza de la Matemática.

Para que el aprendizaje de la Matemática contribuya efectivamente a la comprensión e interpretación de la realidad y al desarrollo del pensamiento crítico y autónomo, es necesario reorientar su enseñanza en los diferentes niveles. Hay dos aspectos interconectados a considerar: las estrategias didácticas y los contenidos.

La vertiente teórica de la "Cognición Situada" retoma de Vygostsky la idea de que el aprendizaje es inherentemente social y está enclavado en un entorno cultural particular. Algunos de los representantes de esta teoría, como Brown, A. Collins y Duguid sostienen que es importante vincular lo que se aprende con el uso que se le da en la realidad, "*parten de la premisa de que el conocimiento es situado, es parte y producto de la actividad, el contexto y la cultura en que se desarrolla y utiliz*a" [2]. Desde esta visión, las actividades planificadas deben permitir al alumno interactuar con situaciones reales, resolver problemas relevantes, aprender a tomar decisiones en situaciones que proponen un reto o plantean un conflicto que obliga a tomar decisiones, es decir, adquirir los saberes y habilidades propios de la comunidad de práctica social o profesional a la que se pretende integrar. Hay numerosos escritos al respecto y no centraremos en este aspecto nuestro trabajo sino en la selección de contenidos, sin perder de vista este marco. Desde los contenidos, entonces, el esfuerzo que debemos realizar como docentes universitarios es el de indagar cuáles son los temas de Matemática relacionados con la Informática, que admiten ser tratados con diferente profundidad en distintos niveles educativos y que resulten de interés para los jóvenes; de manera que motiven sus ganas de aprender más sobre la Matemática oculta en la tecnología que usan [3].

Si de buscar puntos de encuentro entre Matemática e Informática se trata, debemos recurrir a la Matemática Discreta la cual unifica diversas áreas: Combinatoria, Probabilidad, Teoría elemental de números, Grafos, las cuales ofrecen herramientas para la modelización de problemas propios tanto del campo informático como de las telecomunicaciones. Dentro de este amplio espectro los aspectos básicos de la Teoría elemental de números, como son la división en el conjunto de los enteros, números primos, el algoritmo de Euclides entre otros, figuran en los programas y libros de texto correspondientes a la educación general básica, sin embargo en muchos casos se

desconoce su relación con un tema de gran actualidad: la Seguridad Informática.

## 1.2 Seguridad Informática

El uso de INTERNET y del correo electrónico se ha extendido a casi todas las áreas: comercio, educación, salud, entre otras, pero paralelamente ha crecido la necesidad de resolver los problemas de seguridad presentes en este medio. Un esfuerzo especial se ha puesto en todo lo concerniente a la ***Confidencialidad*** en la transmisión de la información, es decir, la seguridad con que una información que se transmite por una red abierta como INTERNET no pueda ser utilizada por algún intruso que la intercepte, y al mismo tiempo que el legítimo destinatario pueda leerla sin dificultad. La ***Integridad*** en la transmisión y almacenamiento de la información, es otro aspecto a considerar. Sabemos que la información puede distorsionarse por ruido en el canal de transmisión o por imperfecciones en el material de almacenamiento, surge así la necesidad de recuperación sin error de la misma.

La ***Criptografía*** en particular estudia la construcción de sistemas para modificar mensajes de tal forma que sean incomprensibles para cualquiera que los intercepte. Durante mucho tiempo estas técnicas interesaban sólo a militares y diplomáticos, pero la difusión del uso de redes abiertas hace imprescindible hoy a diversos usuarios (comerciantes, empresarios, instituciones financieras, médicas, etc.) la utilización de sistema criptográficos [4]. Para entender como funcionan supongamos que Alicia quiere mandarle un mensaje a Benito de tal forma que si alguien intercepta la comunicación sea incapaz de entenderlo. A tal fin Alicia transforma, el texto del mensaje, mediante un proceso de cifrado, utilizando una clave.

Tenemos entonces:

- El *texto llano*, que es el mensaje que Alicia quiere enviar.

- El *texto cifrado*, que es el mensaje que efectivamente envía.

- La *clave*, que especifica cómo convertir el texto llano en texto cifrado, y recíprocamente.

En **términos matemáticos**, sea P el conjunto de todos los posibles textos llanos, sea C el conjunto de todos los posibles textos cifrados y sea K la clave que determina la función $f_K$:P→C que Alicia usa para cifrar el mensaje. Benito debe usar entonces la función inversa $f_K^{-1}$ para descifrarlo. Esta quíntupla (P, C, K, $f_K$ , $f_K^{-1}$), suele denominarse *criptosistema*.

# 2 Puntos de encuentro entre Matemática e Informática

## 2.1 Aritmética y Criptografía.

Si buscamos construcciones criptográficas basadas en ideas matemáticas debemos remontarnos a la época de Julio César (100 – 44 a. C.), quien para cifrar mensajes en sus campañas militares simplemente transformaba el alfabeto llano en un alfabeto cifrado desplazando las letras un número de lugares a la derecha dado por la clave, y luego se modifica el texto llano letra por letra de acuerdo a lo indicado por la transformación del alfabeto. Para ejemplificar el procedimiento usaremos un alfabeto de 26 letras, y tomaremos como clave el valor 3 (que precisamente fue el utilizado por Julio César). Resulta entonces:

*Alfabeto llano*: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

*Alfabeto cifrado*: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Naturalmente, cuando en el alfabeto cifrado llegamos a la Z, continuamos con las primeras letras A, B, .....Si ahora tenemos el
Texto llano: E D U C A C I Ó N;
Benito lo transforma en
Texto cifrado: H G X F D F L R Q
La tarea de Alicia es ahora, a partir de este texto cifrado reemplazar las letras (son todas consonantes!) de acuerdo a lo indicado por la tabla de transformación de alfabetos, o bien directamente reemplaza cada letra por la que está situada 3 lugares a la izquierda en el alfabeto
En la búsqueda de puntos de encuentros asignando números a las letras del alfabeto. Además esto nos permitirá reducir el cifrado a la realización de simples operaciones aritméticas.
Resulta entonces la correspondencia (biunívoca): (A, 0), (B, 1), (C, 2), (D, 3), (E, 4),…., (Z, 25) de esta manera las 26 letras se representan con números del 0 al 25.
Es el momento de recordar conceptos de *Aritmética Modular* y representamos por: *a mod n* el resto de la división en los enteros de *a* por *n*, es decir *15 mod 6* = 3.
Si P es un texto llano y C el correspondiente texto transformado, el Cifrado de César se expresa en forma compacta mediante las fórmulas:
$C = (P + 3) \bmod 26$ y $P = (C - 3) \bmod 26$.
Si el *texto cifrado* que recibe Benito es:
H A L W R $\rightarrow$ 7 0 11 22 17,
tiene que restar, módulo 26, el número 3 a cada uno de los números anteriores, obteniendo: 4 23 8 19 14, de aquí resulta el *Texto llano:* E X I T O.
Técnicamente, podemos decir que estamos trabajando en el anillo de los enteros módulo 26, representado por $Z_{26}$.
Tomando un texto suficientemente extenso en castellano, se observa que las letras más usadas son la E (aproximadamente el 17%) y la A (aproximadamente el 12%). Siguen la O, L, S, N, D pero con frecuencias relativas bastante menores. Estos valores están tabulados. Si un intruso interceptó el mensaje pudo consultar una tabla, o bien pudo construirla el mismo, descifrando el texto.

Evidentemente el cifrado de Julio César a esta altura de los tiempos resulta muy ingenuo. Técnicamente se trata de una sustitución monoalfabética (cada letra del alfabeto se sustituye por otra)
El Criptoanálisis estudia las formas de romper los sistemas criptográficos obteniendo de manera ilegítima información confidencial.
La Historia muestra la permanente lucha entre criptógrafos y criptoanalistas. Con la victoria de estos últimos sobre el cifrado monoalfabético a través del análisis de frecuencias, se imponía el desarrollo de un nuevo método de cifrado. Se atribuye al diplomático francés Blaise de Vigenère (1523-1596) la idea de tomar como clave no una letra, sino una palabra. Esta palabra se repite tantas veces como sea necesario para obtener un número de letras igual al del texto llano (puede que la última repetición quede truncada). Luego la clave actúa modificando las letras del texto llano, de tal manera que la primera letra de la clave modifica la primera del texto llano, la segunda de la clave a la segunda del texto llano, y así sucesivamente. Sobre cada letra del texto llano la modificación se hace siguiendo la cifra de César. Este nuevo método de cifrado se denomina polialfabético.

Un ejemplo: Clave: SOL
Texto llano: M A T E M A T I C A

| M | A | T | E | M | Á | T | I | C | A |
|---|---|---|---|---|---|---|---|---|---|
| 12 | 0 | 19 | 4 | 12 | 0 | 19 | 8 | 2 | 0 |
| S | 0 | L | S | O | L | S | O | L | S |
| 18 | 14 | 11 | 18 | 14 | 11 | 18 | 14 | 11 | 18 |

Ahora se suma módulo 26 cada columna, resultando: 4 14 4 22 0 11 11 22 13 18

| Texto cifrado: E O E W A L L W N S |
|---|

La clave es un secreto celosamente guardado por el emisor y el receptor del mensaje.
Recién a mediados del siglo XIX ese excéntrico genio inglés que fue Charles Babbage (1791-1871), precursor de la moderna computación, tuvo éxito en la tarea de quebrar el cifrado polialfabético. Para ello, a través de la repetición de letras en un texto cifrado suficientemente extenso, trató primero

de identificar la longitud de la clave, y luego mediante el análisis de frecuencias cuál es esta palabra. Su tarea se vio facilitada por el hecho de que en general (como en el ejemplo anterior) se toma como clave una palabra con significado.
Luego de este éxito de los criptoanalistas los criptógrafos idearon perfeccionamientos tomando claves muy largas y sin significado. El máximo perfeccionamiento en esta línea fue logrado con la máquina ENIGMA, utilizada por los alemanes durante la Segunda Guerra Mundial. Sin embargo los criptoanalistas, mediante un trabajo sistemático y empleando cada vez más recursos matemáticos, lograron quebrar el cifrado de ENIGMA. Deben destacarse en esta tarea a los matemáticos Marian Rejewski (polaco; 1905-1980; recurrió a la teoría de grupos de sustituciones) y Alan Turing (inglés; 1912-1954; profundizó las ideas de Rejewski) [4],[5].

## 2.2 La Clave Pública

En este proceso de cifrar y descifrar mensajes la clave puede ser: Simétrica (o Secreta, este es el método usado en la criptografía clásica) o Asimétrica (o Pública). En el caso de Clave Secreta, Alicia aplica $f_K$ al mensaje para enviarlo y Benito $f_K^{-1}$, ambos comparten en secreto la clave K. Si un intruso accede a la misma tiene la posibilidad de cifrar y descifrar mensajes pudiendo además falsear la identidad del emisor del mensaje. Aquí hace su aparición la Teoría Elemental de números, ya que proporciona recursos matemáticos que han solucionado estos problemas. La primera conquista se dio en el año 1976 cuando los matemáticos norteamericanos contemporáneos Whitfield Diffie y Martin Hellman solucionaron el problema de la distribución de claves. Concretamente, idearon un ingenioso método que permite a dos usuarios de una red abierta compartir un secreto (por ejemplo una "palabra"), sin interesarle que puedan ser interceptados los mensajes que a tal fin se intercambian. El paso siguiente lo dio en 1977 otro equipo de matemáticos e informáticos también en los Estados Unidos, integrado por Ronald L. Rivest, Adi Shamir y Leonard Adleman. Idearon un sistema que trabaja con dos claves:

- una clave pública para el cifrado,
- una clave secreta para el descifrado.

Cuando un usuario (Alicia) desea enviar un mensaje a otro usuario (Benito), sólo debe cifrar el mensaje que desea enviar utilizando la clave pública del receptor (Benito). El receptor podrá descifrar entonces el mensaje con su clave privada (que sólo él conoce). Este sistema se basa en una función que es fácil de implementar en una dirección (para cifrar) y que computacionalmente resulte muy difícil de invertir sin la clave privada (esta función se denomina función unidireccional con trampa). De esta manera aunque un intruso, que naturalmente conoce la clave pública de Benito, intercepte todas las comunicaciones intercambiadas por Alicia y Benito, será incapaz de descifrar el mensaje.

El sistema que ellos crearon se denomina RSA, y se basa en la inteligente utilización de conceptos de la Teoría Elemental de Números: números primos, máximo común divisor algoritmo de Euclides, pequeño teorema de Fermat,…. La seguridad del sistema RSA descansa sobre la imposibilidad práctica de factorizar el producto de dos números primos suficientemente grandes [5], [6],[7],[8].

El algoritmo consta de tres partes: la generación de claves, la función de cifrado y la función de descifrado. Inicialmente es necesario generar aleatoriamente dos números primos grandes, a los que llamaremos p y q. A continuación calculamos n como producto de p y q: n = p q. Se calcula $\varphi(n) = (p-1)(q-1)$.

Se determina un número natural *e* de manera que resulte coprimo con $\varphi(n)$. Mediante el algoritmo extendido de Euclides se calcula el número d, tal que $e.d \bmod \varphi(n) = 1$. La clave

pública está dada por el par de números (e, n) mientras que los números (d, n) son la clave privada.

La función de cifrado es $C = P^e \bmod n$ y la de descifrado: $P = C^d \bmod n$.

Aquí no hay magia. Se trata sólo de una ingeniosa aplicación del Pequeño Teorema de Fermat.

## 3 El Taller: un encuentro de docentes

Con estas ideas se realizó un trabajo en el marco del Proyecto "Universidad-Escuela Media: una complejidad para compartir II", implementado por la Universidad Nacional de Entre Ríos junto con el Consejo General de Educación de la provincia que se realizó durante el año 2004. Desde la Secretaría Académica de la UNER, se llevó adelante un relevamiento del tipo de necesidades que presentan las Escuelas de Nivel Medio de la provincia. Surgió así un módulo destinado a favorecer la formación de los docentes de la Escuela Media y lograr un mejor desenvolvimiento de los futuros egresados y de los ingresantes, sobre todo en los primeros años de la Universidad. La propuesta estaba pensada para poner en práctica nuevas estrategias para el tratamiento de los contenidos disciplinares que lleva adelante el docente en el aula, generando procesos de reflexión y crítica sobre sus prácticas educativas" [9].

El proyecto estuvo dirigido a docentes y alumnos de aproximadamente 150 Escuelas de Nivel Medio ubicadas en distintos puntos de la provincia, con una especial consideración en las instituciones educativas pertenecientes a los Departamentos del norte y el centro de Entre Ríos, cuyas condiciones de vulnerabilidad demandan actividades de manera urgente. Nuestra larga experiencia docente nos indica que es muy difícil enseñar algo que no se quiere aprender, por lo tanto se elaboró, en este marco una propuesta de Seminario-Taller, tratando de atacar el síntoma de desinterés en las clases de Matemática, desde tres puntos de vista diferentes pero íntimamente relacionados: la vinculación de la matemática con las ciencias aplicadas, la posibilidad de desarrollar contenidos en diferentes niveles de enseñanza que permitan al estudiante percibir la presencia de la matemática en la tecnología de uso cotidiano y las estrategias didácticas motivadoras. Este fue el origen del Seminario: "Aritmética y Criptografía", que se dictó con sede en escuelas ubicadas en las ciudades de la Paz, Nogoyá y Feliciano de nuestra provincia.

### 3.1Objetivos

•Brindar a los docentes de Matemática en Escuelas Medias los conocimientos aritméticos (teóricos y prácticos) necesarios para comprender aspectos de las actuales Tecnologías de la Información.

•Mostrar cómo conceptos y métodos de la Matemática clásica permiten resolver problemas planteados por la moderna Tecnología.

•Reflexionar sobre las relaciones entre la Matemática, otras Ciencias y las Tecnologías.

### 3.2 Contenidos

Se enumeran los contenidos a desarrollar: Divisibilidad. Aritmética modular. Números primos. Máximo común divisor. Algoritmo de Euclides. Pequeño Teorema de Fermat. Indicador de Euler. Teorema de Euler-Fermat. Logaritmo discreto. Conceptos básicos de Criptografía. Intercambio de claves. El sistema RSA. Firma digital.

4.3 Metodología

Se trabajó sobre un material impreso preparado especialmente. En cada encuentro se presentó y discutió los contenidos correspondientes, y los conocimientos así adquiridos se aplicaron a la resolución de ejercicios y problemas.

### 3.3Evaluación

Se realizó en una prueba escrita, a libro abierto y grupal, en la que se deberán resolver ejercicios y problemas del tipo de los desarrollados en el curso.

## Conclusiones

El Dr. Enzo Gentile, matemático argentino con proyección internacional, expresó: "La Aritmética representa una excelente opción para mejorar la enseñanza de la Matemática... La Aritmética es una ciencia cotidiana, capaz de atraer a cualquier persona que posea sólo un poco de curiosidad. Observamos cómo las revistas de entretenimientos numéricos llaman la atención de mucha gente, a veces con poca instrucción. ¿Por qué no explorar ese germen de curiosidad que posee la gente joven y los niños en *especial?"* [10]

Posteriormente en la misma obra Gentile cita la autorizada palabra del conocido matemático Godfrey Harold Hardy (1877 – 1947), quien expresó: "La teoría elemental de números debería ser uno de los mejores temas para la instrucción matemática temprana. Requiere muy pocos conocimientos previos, el tema que trata es tangible y familiar, los procesos de razonamiento que emplea son simples, generales y pocos, y es única dentro de la ciencia matemática por su apelación a la curiosidad natural". Por otra parte la vinculación de esta rama de la Matemática con la Informática brinda la oportunidad de motivar y promover el estudio de ambas disciplinas.

## Referencias


[1] M.S. Perassi, M.C. Exner, V.Casco: "¿Cómo abordar la problemática de la deserción en la Universidad?". Biociencias Nº1, http://www.biociencias.org.ar/, 2005.

[2] F. Díaz Barriga, F. Cognición situada y estrategias para el aprendizaje significativo. Revista Electrónica de Investigación Educativa, (2003). 5 (2). Consultado el día 10 de marzo de 2008 en: http://redie.ens.uabc.mx/vol5no2/contenido-arceo.html.

[3] Guzmán Ozámiz, M.: Enseñanza de las Ciencias y de las Matemáticas. Tendencias e innovaciones. Ibercima, Madrid, 1993.

[4] S. Singh: LOS CÓDIGOS SECRETOS. El arte y la ciencia de la criptografía desde el antiguo Egipto a la era Internet. Editorial Debate, 2000.

[5] N. Koblitz N.: A Course in Number Theory and Cryptography. Springer-Verlag, 1994.

[6] J. Ramió Aguirre: Libro Electrónico de Seguridad Informática y Criptografía con 1.106 diapositivas, versión 4.1 en su sexta edición de 1 de marzo de 2006, de libre distribución en Internet.

[7] P. Caballero Gil: Introducción a la criptografía, Ra-Ma Librería y Editorial Microinformática, 2002.

[8] M. E. Becker, N. Pietrocola, y C. Sánchez.: Aritmética. Red Olímpica. Olimpíada Matemática Argentina, 2001.

[9] M. A. González Frígoli, M.T. Rodríguez.: Presen—tación Módulo 4. Proyecto Articulación: "Universidad - Escuela Media: una complejidad para compartir II". UNER, 2005.

[10] E.Gentile: Aritmética Elemental en la formación matemática. Olimpíada Matemática Argentina, 1999.