Criptografía en el profesorado de matemática

Una propuesta para abordar el protocolo criptográfico RSA en un profesorado de matemática

E. Cesaratto [1,2] *y C. Fuentes* [1]

Resumen

La actividad descripta en este artículo es consecuencia de la preocupación de los autores por hacer conocer a los estudiantes de los profesorados de matemática la importancia de la matemática en el desarrollo de otras disciplinas científicas y de la tecnología. De hecho, con esta actividad se logró incluir el tratamiento del protocolo criptográfico RSA (un tema de relevancia en la comunicación digital) en un curso de álgebra del profesorado de matemática de la Universidad Nacional de Gral. Sarmiento. Este artículo se concentra en describir el tratamiento dado al tema para su puesta en práctica efectiva en el aula.

Con el objetivo de favorecer en los estudiantes el desarrollo de habilidades de lecto-escritura, se interactuó con un docente de ese área. Este docente acompañó a los docentes de matemática participando del diseño, dictado de clases, producción de materiales específicos y de la evaluación. Entendemos que este tipo de trabajo es novedoso en las aulas de matemática. La apreciación de los docentes es que la actividad descripta promovió en los estudiantes el desarrollo de habilidades de resolución de problemas, de escritura académica y favoreció aprendizajes propios de los contenidos de álgebra.

1 Introducción

Este trabajo presenta una actividad puesta en práctica en un curso de álgebra cuyo diseño fue consecuencia de algunas preocupaciones que tenemos los autores sobre la formación de los profesores de matemática.

De acuerdo a nuestra experiencia, en los cursos de los profesorados de matemática se suele enseñar matemática como una disciplina descontextualizada y sin vínculos con otras ciencias. Sin embargo, es común encontrar en los programas de las materias de matemática la intención de enseñar las

[1]Carlos Fuentes fue parcialmente financiado por la Beca de formación en docencia para graduados UNGS Resolución (CS) N 5023/13 y el Proyecto UNGS 30/3158.
Fecha: 5 de febrero de 2015.

"aplicaciones" de los contenidos matemáticos para resolver problemas de otras disciplinas. Esta intención se suele relegar en las puestas en práctica efectivas en el aula. Consideramos que las razones principales de tal relegación suelen ser "la falta de tiempo" para tratar los contenidos de la materia, las dificultades que presupone introducir conceptos de otras disciplinas de forma tal que los mismos sean significativos para los estudiantes y que el tratamiento de los mismos durante la cursada deje aprendizajes matemáticos relevantes.

En este sentido, suele ser un desafío encontrar problemáticas de otras disciplinas que dialoguen con el contenido matemático de la materia y que involucren conceptos "extra matemáticos" accesibles para los estudiantes en un tiempo breve. Otro desafío es lograr una adaptación de la problemática para que esta pueda ser tratada dentro de los tiempos de la cursada y que, al mismo tiempo, guarde los principios básicos de la misma. Asimismo, es necesario ser cuidadoso con el diseño de las consignas para la ejercitación y evaluación. Se debería lograr que las mismas sean accesibles a los estudiantes (quienes, en general, no tienen formación en la disciplina de aplicación) sin que sean una mera repetición de procedimientos.

Por otro lado, también nos preocupa la falta de atención que se presta a la enseñanza de la lectura y escritura de textos matemáticos. En este sentido acordamos con quienes sostienen que el desarrollo de habilidades en lectocomprensión y producción de textos académicos forman parte de la enseñanza de la disciplina y, además, que estas habilidades permiten un mejor desempeño académico y profesional de los futuros profesores (ver, por ejemplo, [3]).

Estas preocupaciones motivaron el desarrollo de la actividad que describimos a continuación. La misma fue realizada durante la cursada de la materia Álgebra del Profesorado Universitario en Matemática de la Universidad Nacional de General Sarmiento (U.N.G.S., en adelante). En esta materia se tratan algunos temas básicos de teoría de números, del álgebra de polinomios y de teoría de cuerpos. Por esta razón, nos pareció adecuado trabajar el protocolo criptográfico diseñado en 1978 por R. Rivest, S. Shamir y L. Adleman y popularmente conocido por RSA (ver, por ejemplo, [8]). Este protocolo es una de las aplicaciones típicas de la teoría de números a la informática puesto que el proceso de "encriptamiento" de textos utiliza propiedades de la aritmética modular. Además, la garantía que ofrece el protocolo para la transmisión "segura" de datos por medios digitales radica en la consabida dificultad computacional para factorizar números enteros grandes.

La actividad en su conjunto está diseñada para promover la búsqueda bi-

bliográfica y la lectura autónoma de textos. Una ventaja que presenta el tema elegido es que versiones elementales del mismo se encuentran descriptas en libros de álgebra de nivel de grado disponibles en la Argentina como [6] y [2] (una descripción más amplia y con detalles sobre la fundamentación teórica del mismo se puede consultar en el manual [8] y en las referencias que allí se encuentran). Disponer de esta bibliografía nos permitió trabajar con los estudiantes la lecto-escritura y producción de textos académicos.

Para favorecer la producción de textos, el tema se evaluó con la redacción de un informe breve. Cabe destacar que la evaluación de un tema con las características del protocolo RSA resulta muy dificultosa a través de un examen tradicional (una lista de ejercicios a ser resuelta de forma presencial en algunas horas) porque una aplicación significativa del mismo, aún a nivel elemental, es muy extensa. Como corolario de esta experiencia, consideramos que la forma adecuada para la evaluación de un tema con estas características es a través de un informe escrito domiciliario.

El contexto

La cursada de la materia Álgebra tiene una carga horaria de ocho horas semanales repartidas en dos clases de cuatro horas cada una. La materia trata temas básicos de teoría de números, del álgebra de polinomios y de teoría de cuerpos. Además de la enseñanza tradicional de los contenidos, durante la cursada se busca favorecer el aprendizaje de los aspectos computacionales de los mismos. También, se busca mejorar el desempeño académico de los estudiantes a través del desarrollo de habilidades en la lecto - comprensión y en la producción de textos académicos de nivel universitario. Este objetivo es respaldado por la UNGS a través del Programa de desarrollo de habilidades de lectura y escritura académica (PRODEAC) a cargo de docentes del área de lecto-escritura.

La experiencia se llevó a cabo durante el primer cuatrimestre de 2013. A lo largo de esta cursada se destinó tiempo de la clase a la lectura de bibliografía específica y al acompañamiento tutelar de los estudiantes. Además, se contó con la colaboración de un docente del programa PRODEAC. Esta forma de trabajo dio un marco propicio al momento de llevar adelante la actividad que se describe en este artículo.

Cabe destacar que de acuerdo al plan de estudios, la única materia correlativa con contenidos de álgebra es Álgebra Lineal. En sus trayectos académicos, nuestros estudiantes solamente tuvieron alguna experiencia con el Geogebra y no se encontraban familiarizados con el uso de otros softwares específicos de

matemática (Sage, Maple, Mathematica, etc.). En el trayecto de la carrera tampoco se estudian aspectos propios de la computación teórica o el uso de lenguajes de programación. Sin embargo, la mayoría de los estudiantes mostró un manejo adecuado de planillas de cálculo (Excel) y procesadores de texto (Word).

Plan del artículo:

En la sección 2 se describen con más detalle los criterios generales utilizados en el diseño de la actividad. Las secciones 3 y 4 describen la implementación de la actividad durante la cursada. En particular, en la sección 4 se describe brevemente el abordaje que se dio al protocolo RSA y al análisis de su seguridad. Este abordaje está basado en la presentación de este protocolo a nivel elemental que se encuentran en los libros [2], [6] y [7]. En la sección 5 se describe la consigna para la evaluación y en la sección 6, el desempeño de los estudiantes.

2 Objetivos y aspectos generales de la actividad

De manera global, durante la cursada de la materia buscamos favorecer en los estudiantes habilidades de resolución de problemas y mejorar su capacidad para argumentar, defender y comunicar sus producciones no solamente entre estudiantes y docentes sino también entre pares. Por ello, tuvimos en cuenta los siguientes objetivos al momento de decidir el tema y diseñar la actividad:

- que el problema seleccionado como disparador sea propio de otra disciplina y que admita una adaptación acorde a los contenidos del curso de Álgebra,
- que el problema tenga interés para la comunidad científica o aplicaciones tecnológicas,
- que la adaptación conserve los principios básicos que dan origen al problema elegido,
- que propicie el uso de Tic's,
- que para responder a la consigna propuesta para la evaluación, los estudiantes se encuentren frente a la necesidad de diseñar una estrategia de resolución,
- que la resolución requiera del abordaje de bibliografía,

- que los estudiantes deban comunicar en forma escrita lo elaborado en la resolución.

En este sentido, el protocolo criptográfico RSA utiliza como herramientas matemáticas cuestiones relacionadas con la aritmética modular y cuestiones teóricas sobre la factorización de enteros (ver sección 4.1.2). Brevemente, en primer lugar, se buscan dos números primos impares p y q y se considera el entero $n = p \cdot q$. El cifrado y descifrado de un texto numérico se realiza calculando congruencias módulo n de ciertas potencias de los números que conforman el texto. En este contexto, al número n se lo suele llamar un *módulo* RSA.

El interés en estudiar este protocolo en particular radica en el hecho que ha sido uno de los más usados para la transmisión segura de datos vía internet durante los últimos 30 años. En la actualidad, se están explorando nuevos protocolos aunque RSA sigue vigente (ver, por ejemplo, [1]). Utilizamos la versión más simple posible de este protocolo siguiendo el abordaje propuesto por los libros [6] y [2]. La fundamentación de la seguridad del método para la transmisión de datos se encuentra enmarcada en la teoría de complejidad computacional que no forma parte de los contenidos de la materia. En la sección 4.1 explicamos el abordaje de esta fundamentación durante la actividad.

Se pueden implementar instancias de este protocolo con módulos de 2 cifras en adelante aunque en las implementaciones no escolares se consideran módulos de 200 cifras en adelante (ver, por ejemplo, [1]). En la actividad que estamos describiendo usamos módulos de 8 cifras para promover que los estudiantes usen herramientas computacionales (Tic's) y, al mismo tiempo, la dificultad computacional resulte accesible. Esta elección resultó ser acertada porque las herramientas computacionales con las que contaban los estudiantes (Excel y calculadora) les resultaron insuficientes y tuvieron que acudir a las propiedades de aritmética modular aprendidas en la materia para resolver la actividad satisfactoriamente. En este sentido, los estudiantes aprendieron a valorar el uso de softwares específicos.

Para que los estudiantes encuentren la necesidad de diseñar una estrategia de resolución, en la consigna de la evaluación se propuso desencriptar un mensaje de los cuales ellos no eran destinatarios (hackear un mensaje), mientras que en la clase abordamos la construcción del protocolo y el encriptado y desencriptado de mensajes entre emisor y receptor. Para hackear el mensaje, los estudiantes tuvieron que recurrir al método de factorización de Fermat que se encuentra en la bibliografía de la materia pero que no se había tratado en clase. También, tuvieron que profundizar sus conocimientos sobre aritmética modular

para lograr el objetivo de calcular el residuo de potencias de números grandes módulo n.

Finalmente, la evaluación se realizó a través de un informe domiciliario de 4 páginas de extensión en el cual los estudiantes debían explicar y fundamentar todo lo hecho.

3 Puesta en práctica y materiales

La puesta en práctica de la actividad durante la cursada constó de cinco etapas:

1. una clase teórico - práctica sobre criptografía y el protocolo RSA,
2. la entrega, por parte de los docentes, de una consigna de práctica sobre un problema criptográfico y con indicaciones para la confección del informe,
3. una clase y un apunte sobre redacción de informes técnicos,
4. elaboración del informe técnico,
5. la entrega de la versión final del informe.

En lo que sigue haremos una descripción de los aspectos relevantes de cada una de estas etapas.

Clase sobre criptografía

En esta clase, de cuatro horas de duración, se explicó a los estudiantes los objetivos de la criptografía y se les comentó sobre dos sistemas criptográficos simples para ilustrar las ideas principales de un protocolo. En particular se describió el protocolo denominado "la clave del Cesar" y un ejemplo simple que involucraba funciones modulares. Con estos ejemplos se introdujeron las nociones de mensaje, información de un mensaje, bloques de información, emisor, receptor, codificar, decodificar, encriptar, desencriptar, criptosistema y criptoanálisis.

A continuación se comentó el interés de contar con un criptosistema de clave pública para el intercambio de información por medios digitales. Esto motivó la introducción del protocolo RSA que fue el primero con esta característica. Luego se describió la construcción de este protocolo (ver sección 4.1) y se discutieron sus ventajas respecto de otros y su utilización en la actualidad en la transmisión segura de información por medios digitales.

Se explicó que la fiabilidad de un criptosistema radica en la dificultad para obtener la información que se transmite en un texto encriptado de acuerdo a dicho criptosistema para alguien que intercepte la comunicación. En el caso de RSA, la fiabilidad descansa en la dificultad computacional que entraña la factorización de enteros grandes (ver sección 4.2). Si bien hay procedimientos conocidos para realizar esta tarea, la cantidad de operaciones necesarias para lograr la factorizción crece en forma exponencial con de la cantidad de cifras. Estos procedimientos resultan ineficientes para números del orden de 200 cifras (ver, por ejemplo, [1]).

Para explicar el sustento teórico de la seguridad del criptosistema RSA, se discutieron algunas nociones de la teoría de complejidad computacional. Presentamos estas nociones a nivel de divulgación puesto que las mismas no forman parte del trayecto de formación de los profesores de matemática de la UNGS. Al final de la sección 4.1 se muestra el enfoque introductorio que se utilizó para estas nociones.

Consigna de práctica.

Propusimos la siguiente situación: dos docentes intercambian un mensaje encriptado usando un criptosistema armado bajo el protocolo RSA Los estudiantes interceptan el mensaje y conocen sólo la clave pública, y están interesados en conocer la información contenida en dicho mensaje. Cada grupo de estudiantes recibió la misma consigna pero con mensaje y clave diferentes.

La consigna fue entregada a los estudiantes tres semanas antes del final de la cursada quienes debieron resolverla en forma domiciliaria y grupal (no más de tres personas). Esta modalidad implica el desafío de planificar el desarrollo del trabajo. Se incluyó en la consigna una explicación detallada de qué se esperaba en la confección del informe (ver sección 7).

Clase y apunte sobre redacción de informe técnico

En esta clase, un docente del grupo del proyecto PRODEAC explicó las características de un "informe técnico", como así también aspectos que se deben contemplar en la redacción de una producción de nivel universitario. El docente confeccionó un apunte para guiar la redacción del informe que daba indicaciones precisas sobre cómo estructurar el informe en secciones y que debería contener de cada una de ellas.

Elaboración y entrega del informe técnico

En el informe técnico esperábamos que los estudiantes explicaran y fundamentaran las estrategias de resolución y los resultados obtenidos de acuerdo a nuestras indicaciones y las del docente del proyecto PRODEAC.

Luego de tres semanas de trabajo, cada grupo entregó el informe en la fecha del último examen regular de la cursada de la materia. Los estudiantes tuvieron una devolución personalizada en la que se indicaba los errores encontrados tanto en la resolución del problema como en la redacción del informe. Aquellos grupos que no alcanzaron la aprobación en esta primera entrega tuvieron la oportunidad de realizar una segunda (y definitiva) en la cual debían mejorar su producción en concordancia con las observaciones realizadas.

4 Enfoque teórico: Protocolo RSA y seguridad en la transimisión de datos

La enseñanza de un protocolo criptográfico requiere de que se aborden diferentes temas propios de la informática que no forman parte de los programas de las materias del profesorado de matemática. Para que los estudiantes puedan apropiarse de los conceptos y nociones involucrados, el tratamiento de los mismos debe ser intuitivo. Sin embargo, los conceptos y las nociones deben ser tratados de forma lo suficientemente precisa como para que los estudiantes puedan operar con ellos.

En esta sección se describe el enfoque con el que tratamos los diferentes temas de la informática necesarios para comprender y abordar esta actividad.

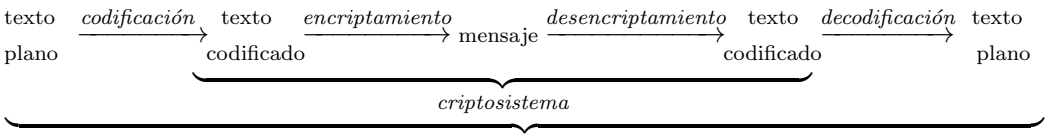
4.1 Adaptación del protocolo RSA presentada en el curso.

En este apartado, describimos algunas generalidades sobre criptosistemas y a continuación estas se particularizan al caso de RSA.

4.1.1 Generalidades sobre criptosistemas.

Un protocolo criptográfico o criptosistema es un procedimiento que permite intercambiar información de forma segura entre dos personas, que llamaremos **C** y **M**, si ambas o alguna de ellas conoce la "clave" que el protocolo establece. Se entiende por seguridad que si esta información circula por un canal público y es interceptada por un tercero, este no pueda acceder a la misma.

Para describir las etapas básicas de un protocolo criptográfico, comenzamos suponiendo que **M** quiere enviar información a **C** de forma segura y que la misma está escrita en un texto en idioma español. Al texto original lo llamamos *texto plano*. Para que la transmisión de la información sea segura es necesario "encriptar" el texto. El primer paso para encriptarlo es transformar al texto plano en una tira de números que sea susceptible de ser manipulada matemáticamente. Este procedimiento se suele llamar *codificación* y su resultado, *texto codificado*. Al texto codificado se lo *encripta*, es decir, se lo modifica de acuerdo a lo estipulado por el procolo que se esté usando, dando lugar a una nueva tira de números que llamaremos *mensaje*. El mensaje es recibido por **C** quien, conociendo el protocolo y las "claves" necesarias, puede recuperar el texto codificado, decodificarlo y recuperar la información. Se resume este proceso en el siguiente esquema:



4.1.2 Armado de un criptosistema RSA

La característica principal del protocolo RSA es que el mismo está diseñado para que sus usuarios no tengan que encontrarse para compartir la clave que permite encriptar o desencriptar. Este tipo de criptosistemas se conocen como protocolos de clave pública puesto que un usuario **C** produce dos claves: una pública y una privada. La pública es conocida por cualquier persona **M** del resto del mundo y la privada es conocida solo por **C**. Si alguien del resto del mundo desea enviar un mensaje a **C** usa solamente la clave pública de **C** para encriptarlo y este desencripta usando su clave privada.

Se describen a continuación los pasos a seguir para el armado de estas claves y el procedimiento que permite encriptar y desencriptar.

Construcción de la clave pública.

El creador del criptosistema, que identificamos con la letra **C**, elige dos números primos p y q distintos entre sí con los que calcula el número $n = p \cdot q$. Estos números p y q no se dan a conocer al resto del mundo **M**. Como **C** conoce p y

q, puede calcular fácilmente el valor de la función ϕ de Euler de dicho número puesto que

$$\phi(n) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1).$$

Recordamos que la función ϕ de Euler de un número n es la cantidad de números enteros coprimos con n entre 1 y n.

Como se explica más adelante, es necesario elegir p y q de forma tal que n sea coprimo con todos los números utilizados para codificar los caracteres del texto plano. En nuestra adaptación esto quedó garantizado pues elegimos primos p y q mayores que la cantidad de caracteres utilizados en el texto plano. Esta condición es suficiente para que el protocolo funcione. Las condiciones para garantizar la seguridad del protocolo con los recursos informáticos actuales se discute en el artículo [1]. En dicho artículo los autores reportan la factorización de un módulo RSA de 768 bits (238 cifras decimales) y discuten la viabilidad de factorizar un módulo RSA de 1024 bits.

Conocido el valor de $\phi(n)$, el creador del criptosistema **C** elige un número e, que se lo denomina *exponente de encriptamiento*, que debe satisfacer las siguientes condiciones: $1 < e < \phi(n)$ y $(e; \phi(n)) = 1$. El par de valores $(n; e)$ se llama clave pública y es dada a conocer por **C** al resto del mundo **M**.

4.1.3 Construcción de la clave privada.

Determinada la clave pública, **C** busca un número entero d, llamado *exponente de desencriptamiento*, tal que

$$d \cdot e \equiv 1 \pmod{\phi(n)}.$$

En otras palabras, d es un inverso de e módulo $\phi(n)$. La existencia de d está garantizada porque e y $\phi(n)$ son coprimos. El par de valores $(n; d)$ es la *clave privada* y es conocida solamente por **C**.

Codificación y encriptamiento del texto plano

El proceso de codificación de un texto plano le asigna un número a cada caracter o bloques de caracteres del texto. En esta experiencia consideramos que el texto plano está escrito con 27 tipos de caracteres: las letras de nuestro alfabeto sin la ñ y el caracter [ ] que representa el espacio entre palabras. Asignamos el valor 01 a la A, 02 a la B y así siguiendo. Al caracter [ ] le asignamos el 27. En usos realistas del protocolo se suelen agrupar caracteres para la asignación numérica.

Supongamos que **M** quiere enviarle un mensaje (un texto plano encriptado) a **C**. Al codificar el texto plano de N letras, **M** obtiene una lista de números $(P_1, \ldots, P_N)$ donde cada $P_i \in \{1, 2, \ldots, 27\}$ es la codificación de una de las letras. Para encriptar, **M** asigna a cada P en el conjunto $\{P_1, \ldots, P_N\}$ un número E que es la reducción de P^e módulo n, es decir

$$E \equiv P^e \pmod{n} \quad \text{y} \quad 0 \leq E < n.$$

Como P y n son coprimos, siempre se tiene que $E \neq 0$. Al aplicar este procedimiento a todos los caracteres del texto plano, **M** obtiene una N–upla $(E_1, \ldots, E_N)$ que es el mensaje que envía a **C**.

Recuperación del texto plano

Para recuperar la codificación P de cada caracter, **C** toma cada número E del mensaje y lo eleva al exponente de desencriptamiento d puesto que la construcción de e, d y n garantiza que

$$P \equiv E^d \pmod{n}.$$

En efecto, como d satisface que $d \cdot e \equiv 1 \pmod{\phi(n)}$, por la identidad de Bèzout, existe k tal que $d \cdot e = 1 + k \cdot \phi(n)$ con $k \in \mathbb{Z}$, por lo tanto,

$$E^d \equiv P^{e \cdot d} \equiv (P)^{1 + k \cdot \phi(n)}.$$

Ahora se utiliza el teorema de Euler que establece que $a^{\phi(n)} \equiv 1 \pmod{n}$ si a y n son coprimos. En nuestro caso, P y n son coprimos porque los factores p y q de n son ambos mayores que P (ver el apartado sobre la construcción de la clave pública).

Por lo tanto,

$$E^d \equiv P \cdot (P^{\phi(n)})^k \equiv P \cdot 1^k \equiv P \pmod{n}.$$

El receptor **C** recupera cada letra del texto plano decodificando la lista de valores $(P_1, \ldots, P_N)$ de acuerdo a la convención establecida en el apartado "Codificación y encriptamiento del texto plano". Así queda completado el procedimiento para encriptar un texto plano, enviarlo y recuperar la información que en él se transmite.

4.2 La seguridad de RSA. Problemas computacionalmente fáciles o difíciles

En un criptosistema de clave pública, se pretende que solamente el destinatario de un mensaje pueda obtener la información que viaja en dicho mensaje. En este sentido, se impone considerar el problema de si es posible obtener la clave privada teniendo como única información la clave pública y, en caso de que haya un procedimiento que lo permita, estudiar si tal procedimiento es computacionalmente factible. Este tipo de análisis se suele llamar criptoanálisis.

4.2.1 Criptoanálisis para el protocolo RSA

En el caso del protocolo RSA, si se conoce el valor de $\phi(n)$ y la clave pública $(n; e)$ se puede obtener d fácilmente resolviendo la ecuación $d \cdot e \equiv 1 \pmod{\phi(n)}$. Es evidente que resulta simple calcular $\phi(n) = (p-1)(q-1)$ si se conocen los factores p y q de n. Lo interesante es que, por la particular factorización de n, si se conoce el valor de n y de $\phi(n)$ es posible deducir fácilmente los enteros p y q resolviendo el sistema

$$\begin{cases} \phi(n) = (p-1) \cdot (q-1) \\ n = p \cdot q \ . \end{cases}$$

Esta argumentación muestra que el problema de obtener la clave privada a partir de la pública es equivalente a factorizar el módulo n.

El interés del protocolo RSA radica en que todas las operaciones involucradas para encriptar son "computacionalmente fáciles" mientras que factorizar módulos RSA es un problema "computacionalmente difícil". En el siguiente apartado mostramos como se explicó el sentido de estos términos durante la cursada de la materia Álgebra.

Problemas computacionalmente fáciles o difíciles

Informalmente, un problema computacionalmente fácil es un problema para el cual se dispone de un "algoritmo eficiente" para resolverlo. Por algoritmo se entiende a una secuencia de operaciones computacionales que toma un valor, o conjunto de valores, que se llama "entrada" y produce un valor, o conjunto de valores, que se llama "salida". Por ejemplo, para la construcción de las claves, se utiliza el algoritmo de Euclides. Este algoritmo resuelve el problema de calcular el máximo común divisor de dos enteros dados. Para este algoritmo,

la entrada es el par de enteros y la salida es el máximo común divisor de esos dos enteros.

La eficiencia de un algoritmo depende de la cantidad de recursos computacionales que dicho algoritmo utiliza para calcular la salida. Los recursos que se suelen considerar primordialmente son el tiempo y el espacio:

- el tiempo corresponde a la cantidad de pasos requeridos para la ejecución del algoritmo considerado.
- el espacio corresponde a la cantidad de memoria utilizada en dicha ejecución.

Es claro que la cantidad de recursos computacionales utilizados por un determinado algoritmo depende, no solamente del algoritmo, sino también de las entradas. En general, se busca determinar el tiempo y el espacio necesarios para el procesamiento de una operación como una función de la "longitud de la entrada". Cuando las entradas son números enteros, la longitud de la entrada es la cantidad de cifras binarias que se necesitan para escribir dicho número. En nuestro contexto, tomamos cifras decimales.

Se define un algoritmo de tiempo polinomial si el máximo tiempo de ejecución para todas las entradas de longitud m está acotado por un polinomio en m. Si el tiempo de ejecución de un algoritmo depende exponencialmente de la longitud de la entrada, el mismo es llamado algoritmo de tiempo exponencial.

La mayoría de los algoritmos de tiempo exponencial son simples variaciones de una búsqueda exhaustiva, mientras que los algoritmos de tiempo polinomiales, usualmente se obtienen mediante un análisis más profundo de la estructura del problema. Bajo este marco, se dice que un problema está bien resuelto cuando se conoce un algoritmo de tiempo polinomial que lo resuelva, por lo tanto, un problema se define como intratable (o dificultoso) si es tan difícil que no existe (hasta el momento) un algoritmo de tiempo polinomial capaz de resolverlo. A los algoritmos de tiempo polinomial se los suele llamar eficientes. Es importante hacer notar que una ejecución de un algoritmo ineficiente puede llevar años aún para entradas de longitud no muy grande. Por ejemplo, los autores del artículo [1] reportan que factorizar un entero del tipo RSA de 768 cifras binarias llevó varios años.

En criptografía, para que un sistema sea considerado seguro se tiene que verificar que el correspondiente problema de criptoanálisis (hackeo de mensajes) sea dificultoso o intratable desde el punto de vista señalado anteriormente.

En el caso del protocolo RSA, es necesario obtener la clave privada para hackear el criptosistema o criptoanalizarlo. Es posible calcular la clave privada si se conoce el valor de $\phi(n)$ donde n es el módulo RSA. Este problema es equivalente a factorizar n y se cree que la factorización de enteros es un problema difícil. En el cuadro 1 se clasifican en fáciles y difíciles, los procesos que se deben realizar cuando se usa RSA (ver, por ejemplo, [8]).

Fácil	**Difícil**
Calcular $n = p.q$ conocidos p y q.	Factorizar n
Calcular $\phi(n)$ si se conoce la factorización en primos de n	Calcular $\phi(n)$ si no se conoce la factorización de n
Calcular el máximo común divisor entre dos enteros (algoritmo de Euclides)	
Calcular d tal que $e.d \equiv 1 \pmod{\phi(n)}$	
Calcular $p^d \pmod{n}$	

Table 1: Operaciones fáciles y dif'iciles computacionalmente

Cabe destacar que la información volcada en el cuadro no fue fundamentada durante en la clase puesto que la teoría necesaria para tal fundamentación no forma parte de los contenidos de las materias del trayecto académico de los estudiantes. A pesar de esta dificultad, ellos pudieron interpretar intuitivamente la noción de "dificultad computacional". Entendemos que la resolución de la consigna reforzó la idea de que hay "cuentas" que podrían exceder la capacidad de cálculo de la computadora.

5 Consigna de práctica

En esta sección se describe y resuelve la consigna de práctica. La versión completa del enunciado de la consigna se encuenta en el anexo. La consigna plantea que dos personas intercabian información enviando un mensaje que ha sido encriptado usando el protocolo RSA tal como fue explicado en la sección 4.1. Se dan como datos la clave pública $(n; e)$ y el mensaje que es una tira de números

$(E_1, \ldots, E_N)$ entre 1 y $n-1$. La tarea de los estudiantes fue obtener la información contenida en el mismo, es decir, hackear el mensaje. La clave pública y el mensaje eran diferentes para cada grupo de estudiantes. El texto plano original era el nombre de un matemático reconocido y tenía una extensión no superior a 8 letras.

Para construir los módulos RSA, se utilizaron primos p y q de 4 cifras cada uno y, por consiguiente, se obtuvieron módulos $n = p \cdot q$ de 8 o 9 cifras. Para la elección de los primos p y q se tuvieron en cuenta las siguientes consideraciones:

1. De acuerdo a las recomendaciones de la bibliografía específica, los primos p y q deben tener un orden de magnitud similar (ver, por ejemplo, [8] o [7]).

2. En nuestra versión simplificada del protocolo, la codificación de cada letra del texto plano se encripta con un número entre 1 y $n-1$ y, luego, el mensaje resulta ser una lista de números donde cada número tiene, aproximadamente, tantas cifras como tiene n. Por esta razón, los cálculos involucrados no son factibles para los estudiantes si n es muy grande. En aplicaciones realistas, el texto plano es encriptado por bloques de letras.

3. El primer paso del "hackeo" es la factorización del módulo n. Para que los estudiantes puedan factorizar el módulo, este no debe ser excesivamente grande. Por otro lado, el módulo debe ser lo suficientemente grande como para que los estudiantes perciban la dificultad computacional de "hackear" un criptosistema.

4. Uno de nuestros objetivos es favorecer en los estudiantes habilidades de aprendizaje autónomo a partir de la bibliografía. Durante la cursada se explicó el método de factorización conocido como "criba de Eratóstenes", por esta razón, los primos p y q fueron escogidos de forma tal que la factorización del módulo $n = p \cdot q$ fuera más eficiente con el "método de Fermat" que con la criba. Se sugirió a los estudiantes abordar el método de Fermat desde el libro de M. Becker, N. Pietracola y C. Sánchez [2].

Resolución esquemática de la consigna

En lo que sigue se resuelve esquemáticamente la consigna propuesta a los estudiantes para los siguientes datos:

Clave pública: $(n; e) = (12\,536\,527; 3\,055\,961)$.

Mensaje: $[E_1, \ldots, E_5] = [4541619, 1, 4614032, 4016627, 4016627]$.

Recordemos que el objetivo es desencriptar y decodificar el mensaje para recuperar el texto plano. Brevemente, para hackear el mensaje, se factoriza n y se calcula $\phi(n)$. Luego, se calcula el exponente de desencriptamiento d. Para recuperar el texto codificado, se reduce módulo n la potencia d de cada uno de los 5 números E_i que componen el mensaje. Finalmente, el texto plano se recupera decodificando cada uno de los 5 residuos. A continuación se explica más detalladamente cada uno de estos pasos.

Paso 1: Factorización del módulo. El número $n = 12\,536\,52$ es susceptible de ser factorizado con 4 etapas del método de Fermat. Se obtiene que $n = p \cdot q$ con $p = 3\ 313$ y $q = 3\ 643$. Esperábamos que los estudiantes verifiquen que estos factores son primos.

Paso 2: Cálculo del valor de $\phi(n)$. Con las propiedades de la función ϕ de Euler, resulta que

$$\phi(12\,536\,52) = \phi(3\,391) \cdot \phi(3\,697) = 3\ 390 \cdot 3\ 696 = 12\,529\,440.$$

Paso 3: Cálculo del exponente de desencriptamiento. El exponente de desencriptamiento d es el inverso multiplicativo módulo $\phi(n)$ del coeficiente de encriptamiento e. Es decir, d satisface la ecuación

$$d \cdot e \equiv 1 \pmod{\phi(n)}$$

que es equivalente a la ecuación diofántica

$$d \cdot e + k \cdot \phi(n) = 1.$$

Usando el algoritmo de Euclides extendido con $e = 3\,055\,961$ y con el valor de $\phi(n)$ calculado en el paso anterior resulta que $d = 41$.

Paso 4: Desencriptamiento del mensaje. Para desencriptar el mensaje, se reduce E_i^d módulo n para cada uno de los 5 números E_i que componen el mensaje. El primer número del mensaje de la consigna es $E_1 = 4\,541\,619$ y resulta que

$$(4\,541\,619)^{41} \equiv 7 \pmod{12\,536\,527}. \tag{1}$$

Procediendo de igual forma con todos los números del mensaje, se recupera el texto codificado que es

$$[7, 1, 21, 19, 19].$$

La forma más elemental de calcular E_1^d módulo n es elevar el entero E_1 a la d y luego realizar la división entera de E_1^d por n. El tamaño de los números involucrados hace inviable esta forma de abordar el cálculo con una calculadora o el Excel. También resulta inviable reducir potencias pequeñas de E_1.

Para obtener la igualdad (1) es necesario utilizar un software específico (por ejemplo, Maple) o bien acudir al teorema chino del resto. Para utilizar esta última opción se debe calcular $E_1^d \pmod p$ y $E_1^d \pmod q$ y reconstruir el residuo $E_1^d \pmod n$. Como $E_1 \pmod p$ y $E_1 \pmod q$ son enteros de 4 cifras, resulta factible calcular los residuos de la potencia E_1^d con una calculadora. De todas formas, es necesario calcular los residuos de potencias pequeñas de E_1 módulo p o q para luego reconstruir los residuos $E_1^d \pmod p$ y $E_1^d \pmod q$.

Paso 5: Decodificación del mensaje. Para obtener el texto plano, a cada número del texto codificado $[7, 1, 21, 19, 19]$, se le asigna la letra que le corresponde de acuerdo a la convención que describimos en el apartado 4.1.2. Por ejemplo, como el primer número del texto codificado es 7, la primera letra del texto plano es la séptima letra del alfabeto que es la "G". Decodificando de esta forma cada uno de los números, se obtiene que el texto plano es la palabra "GAUSS".

6 Evaluación general de la actividad y desempeño de los estudiantes

En esta sección se describe el desempeño de los estudiantes en los aspectos matemáticos y comunicacionales.

6.1 Aspectos matemáticos

Una clase de 4 horas fue suficiente para que los estudiantes pudieran comprender el funcionamiento del protocolo. Esto se confirmó al observar que la mayoría de los estudiantes pudo resolver el ejercicio de encriptar y desencriptar mensajes usando módulos de 2 cifras. Esta apreciación se reforzó pues la mayoría de los grupos pudo elaborar la estrategia de resolución de la consigna de forma independiente.

En el paso 1 de la resolución presentada en la sección 5, los estudiantes debieron factorizar un entero de 8 cifras y, como se explica en esa misma sección, se esperaba que ellos recurrieran al método de Fermat. Los estudiantes abordaron el método de factorización de Fermat directamente desde la bibliografía (más precisamente, usaron la versión de [2]), lo comprendieron autónomamente y lo aplicaron correctamente.

No se observaron dificultades en el paso 2, puesto que se habían trabajado las propiedades de la función ϕ durante la cursada. Lo mismo ocurrió en el paso 3 con el cálculo del coeficiente de desencriptamiento d.

La reducción módulo n de la potencia d de cada letra E del paso 4 representó un problema para los estudiantes. En este paso intentaron calcular el entero E^d y dividirlo por n utilizando la calculadora o una planilla de cálculo (Excel). El tamaño de los de números involucrados hace que el cálculo pretendido exceda las capacidades de estas tecnologías. Este problema no se hubiera planteado si los estudiantes hubieran recurrido a algún software específico como MAPLE que es capaz de manejar reducciones modulares para enteros muy grandes.

Los estudiantes se vieron forzados a buscar algún truco matemático para realizar la reducción módulo n. A partir de nuestra sugerencia, redujeron E^d módulo p y módulo q y usaron el teorema chino del resto para calcular E^d módulo n tal como se explica en la sección 5, paso 4. Como $E \pmod p$ o $E \pmod q$ son enteros de a lo sumo cuatro cifras, la reducción de la potencia es accesible con la calculadora o el Excel.

Este tema se había trabajado en la materia pero para reforzar se les propuso como referencia el libro de E. Gentile [5]. Algunos estudiantes encontraron de forma independiente el método "repeated squares" (el mismo se encuentra explicado en [6]).

Cabe mencionar que uno de los estudiantes programó el método en C^{++}.

La recuperación del texto plano no presentó dificultades.

6.2 Aspectos comunicacionales

Los estudiantes encontraron dificultades importantes para redactar el informe técnico. En sus primeras versiones, la estructura del mismo era desordenada, no quedaban claros los objetivos ni la conclusión del trabajo, los términos usados no estaban definidos. También encontraban fuertes dificultades en la argumentación: confusiones entre definiciones y proposiciones, falta de verificación de las hipótesis de los teoremas usados, falta de mención de los resultados teóricos utilizados, tendencia a incluir solamente cálculos, uso incorrecto del

lenguaje simbólico y uso inapropiado de ciertos conectores como, por ejemplo, "entonces", "luego", "por otro lado", etc.

Los grupos que lograron mejores producciones tomaron como punto de referencia los trabajos realizados en las materias pedagógicas. Algunos estudiantes incluyeron en el informe evaluaciones didácticas de la actividad.

6.3 Algunos datos de la evaluación

La acreditación satisfactoria de la actividad requerió la aprobación de los dos aspectos trabajados. Por un lado, los estudiantes debían conseguir el objetivo matemático de "romper" el criptosistema dado y descifrar la información que viaja en el mensaje. Por otro lado, ellos debían aprobar la escritura del informe técnico en el cual comunicaban los procesos realizados y los resultados obtenidos conjuntamente con la argumentación que avalaba su estrategia.

La evaluación de las producciones de los 15 grupos de estudiantes refuerza la conjetura de que las dificultades se encuentran en la comunicación de sus ideas y no en la comprensión de la teoría o de su aplicación en la resolución de un problema. De hecho, 13 de los 15 grupos lograron "romper" el criptosistema y recuperar el texto plano. Sin embargo, solamente 7 grupos aprobaron directamente la producción escrita.

Conclusión

El desarrollo de esta actividad centrada en el protocolo criptográfico RSA fue factible en los tiempos del curso de Álgebra del profesorado de matemática de la UNGS. Los alumnos se mostraron interesados en el tema y muchos comentaron que percibieron el posible uso de algunos contenidos del curso en la resolución de problemáticas de la "realidad". Tuvimos indicios de que el problema propuesto permitió a los estudiantes percibir algunas limitaciones de ciertos recursos tecnológicos (calculadora y planilla de cálculo). La evaluación a través de un informe técnico nos resultó adecuada puesto que la misma fue accesible para los estudiantes y al mismo tiempo nos permitió evaluarlos. Además, este tipo de evaluación favoreció el objetivo de promover la escritura en el área de matemática a nivel universitario.

Fortalecimos nuestra percepción de que los estudiantes encuentran mayores dificultades en la comunicación de sus producciones matemáticas que en la producción propiamente dicha. Esta percepción se afianza observando que la mayoría de los grupos alcanzaron el objetivo de romper el criptosistema, pero

aproximadamente la mitad de ellos debieron reescribir su informe para una nueva evaluación.

Una explicación posible de estas dificultades es la falta de familiaridad de los estudiantes con la lectura de textos de matemática. Entendemos que esta falta de familiaridad se debe a que, en general, los profesores trabajamos los temas principalmente desde la "toma de apuntes" en la clase y no proponemos con el énfasis necesario la lectura de textos específicos. Por otro lado, las listas de ejercicios, con las que frecuentemente trabajamos en las materias, proponen producciones textuales fragmentadas que hace que los estudiantes encuentren dificultades al momento de elaborar un texto donde varios argumentos interactúan entre sí.

A modo de reflexión nos preguntamos cómo consolidar la práctica de proponer actividades que fortalezcan las habilidades en la argumentación en matemática, que vinculen los contenidos matemáticos con la resolución de problemas del "mundo real" y que propongan a los estudiantes el desafío de comunicar sus producciones favoreciendo este aspecto formativo de los futuros docentes.

Agradecimientos

Los autores agradecemos especialmente a Pablo Zdrojewski, docente del programa PRODEAC, por su participación y guía en la puesta en práctica de esta experiencia. Nuestro agradecimiento es también para Nino Cafure por su lectura atenta.

References

[1] Aoki, K., Franke, J., Lenstra, A.,Thomé, E., Bos, J., Gaudry, P., Kruppa, A., Montgomery, P., Osvik, D., Riele, H., Timofeev, A., Zimmermann, P., Factorization of a 768-bits RSA modulus. Advances in Cryptology CRYPTO 2010, Lecture Notes in Computer Science Vol. 6223, 2010.

[2] Becker, M. , Pietracola, N., Sanchez, C., *Aritmética.* Red Olímpica Buenos Aires, Buenos Aires, 2001.

[3] Carlino, P., Afabetización académica diez años después. Revista Mexicana de Investigación Educativa, vol. 18, núm. 57, 2013, pp. 355-381.

[4] Childs, Lindsay N., *A Concrete Introduction to Higher Algebra.* 3 ed. U.S.A. Springer, 2000.

[5] Gentile, E., *Aritmética Elemental.* 1 ed. Buenos Aires. O.E.A., 1985.

[6] Graña, M. , Jeronimo, G., Paceti, A., Jancsa, A., Petrovich, A., *Los números. De los números naturales a los complejos.* 1 ed., Ministerio de Educación de la Nación, Buenos Aires, 2009.

[7] Koblitz, N., *A Course in Number Theory and Cryptography.* 2 ed. U.S.A. Springer, 2000.

[8] Menezes, A., van Oorschot, P. Vanstone, S., *Handbook of applied cryptography.* 1 ed., CRC Press, 1996.

7 Anexo

En este anexo incluimos la consigna tal como fuera presentada a los estudiantes.

Los profesores Nardo y Eda quieren compartir información sobre la materia Álgebra por medios informáticos de forma segura. Para ello Nardo crea un criptosistema utilizando el protocolo criptográfico RSA. Como se acerca el examen integrador, Eda envía información relevante sobre dicho examen a Nardo en un mensaje, y para ello utiliza la clave pública de Nardo para encriptarlo. Ustedes han interceptado el mensaje y, como es de su interés, desean conocer la información que se transmite en él, y se ponen a trabajar con el fin de descifrar el mensaje. Se espera que determinen cuál es la información contenida en dicho mensaje conociendo la clave pública.

Datos

$$\text{Clave pública:} \quad (n; e) = (12\,536\,527; 3\,055\,961)$$

$$\text{Mensaje:} \quad [4541619, 1, 4614032, 4016627, 4016627].$$

Instructivo para la elaboración y entrega del informe final.

El trabajo deberá ser presentado en forma escrita el día designado para el examen integrador de la materia. No es necesario que sea entregado en formato digital, pero de hacerlo en forma manuscrita se solicita prolijidad en la presentación.

Las fuentes para realizar la presentación son los apuntes de las clases y la bibliografía de la materia. En particular, para el método RSA se pide circunscribirse a la clase sobre el tema criptografía y al libro Aritmética de Becker, M. E.; Pietrocola, N.; Sánchez, C.; capítulo 9. Si fuese necesario factorizar un número entero se deberá usar el método de Fermat siguiendo la descripción y notaciones del libro antes mencionado. La presentación constará de:

1. Carátula con el título, número de grupo y los datos de todos los integrantes del mismo, nombres de los docentes de la materia y fecha de entrega.

2. Una introducción conforme a la explicación de Pablo Zdrojewski integrante del proyecto PRODEAC.

3. Un cuerpo principal donde se describa cómo se particulariza la teoría general al caso que ustedes están tratando. Se debe explicar claramente cómo se aplican los métodos y propiedades que figuran en las bibliografía o que se dieron en clase y que son necesarios para resolver su problema particular. Además, en el momento de introducir dichos métodos o propiedades se debe citar la fuente. No se deben incluir citas o explicaciones de métodos o propiedades que no son utilizados. No se deben incluir copias textuales de las descripciones de los métodos o demostraciones de propiedades generales. Se pretende que usen la teoría general verificando que la resolución propuesta para su caso particular se ajusta a un desarrollo general ya descripto. Si para lograr el objetivo presentado en la consigna se deben realizar reiteradamente cálculos similares entre sí (procesos que involucran cálculos idénticos pero con diferentes valores numéricos), basta con que describan cómo se realiza sólo uno de estos cálculos, dejando el resto para el anexo.

4. La organización del texto es conforme a lo trabajado en la clase con el docente Pablo Zdrojewski.

5. Una conclusión conforme a las indicaciones de Pablo Zdrojewski.

6. Un anexo en donde figuren la totalidad de los cálculos relevantes para el objetivo del trabajo práctico. Aquí no se espera que justifiquen ni muestren un desarrollo como en el cuerpo principal, sólo se espera disponer de la totalidad de los cálculos. Sin embargo, es conveniente organizar dichos cálculos incluyendo subsecciones y referencias al cuerpo principal.

7. En la conclusión o en la introducción deben figurar la información o texto plano contenido en el mensaje (texto cifrado) así como los parámetros principales del criptosistema. El cuerpo principal del trabajo práctico junto con la introducción y la conclusión no podrá tener una extensión superior a 4 carillas A4 si lo realizaran en formato digital, y no superior a 4 hojas si fuera realizado en forma manuscrita.

[1] Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina.

[2] CONICET,Argentina.
E-mail: ecesarat@ungs.edu.ar , cfuentes22@yahoo.com
Fecha: 5 de febrero de 2015