UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA, 2023-1

CRIPTOGRAFÍA

Practical Session 5

Kid Krypto

PROFESORA:

Dra. Rocío Aldeco Pérez

ALUMNA:

Karla Andrea Najera Noyola

Kid Krypto

Instrucciones

a. Use Kid Krypto con los valores a=10, b=2, A=15, B=5 para encriptar x=112
b. Conteste las siguientes preguntas:
    i. ¿Todos los enteros pueden ser elegidos para establecer Kid Krypto?
    ii. En caso de ser no la respuesta anterior, menciona que números no pueden ser utilizados y porqué.
c. Suba un archivo con todos los hallazgos.
d. Realice un envío individual de su implementación utilizando el lenguaje de programación de su elección. Los casos de prueba son los presentados en la siguiente tabla:

Testing Vectors					
a	**b**	**A**	**B**	**Plaintext**	**Ciphertext**
3	4	5	6	200	161
3	4	5	6	650	62
9	11	5	8	1028	572
9	11	5	8	54	2546
47	22	11	5	12223	13268
47	22	11	5	4356	28929

Introducción

Con el paso de los años la criptografía ha ido evolucionado con el fin de brindar soluciones cada vez más robustas, dando lugar a lo que hoy se conoce como la Criptografía Moderna. Esta rama fue creada en1948 a raíz de la Segunda Guerra Mundial y tomando como referencia la Teoría de la Información de Claude Shannon cuyo postulado principal era que ningún texto cifrado debía revelar ningún tipo de información acerca del texto sin formato, lo que implica que ningún atacante debería conocer información relacionada que sirva para su descifrado.

Hoy en día se ha vuelto crucial el uso de algoritmos que permitan la transferencia segura de datos a través de canales que no siempre pueden tener las máximas medidas para garantizar que la información cumpla con la triada de la seguridad. Por ello, es cada vez más frecuente la aparición de nuevos algoritmos con un mayor nivel de complejidad. Tomando en cuenta lo anterior, dentro de la Criptografía Moderna existirá la siguiente clasificación:

- **Algoritmos asimétricos**: Son aquellos métodos que se basan en una codificación de información haciendo uso de 2 claves: una privada y una pública, con el fin de que el

remitente conserve la clave privada y cualquier receptor pueda recibir la clave pública. Se les considera relativamente nuevos.

- **Algoritmos simétricos:** Son métodos más simples que los asimétricos debido a que utilizan la misma llave para las funciones de encriptación y desencriptación. Esta clave debe ser compartida con todas las personas que requieren recibir el mensaje.

En la actualidad, muchos de los algoritmos de ambas categorías requieren el uso de funciones matemáticas complejas y conceptos avanzados acerca de teoría de números. No obstante, en 1993 Michael Fellows y Neal Koblitz inventaron una familia de criptosistemas asimétricos denominada como Kid Krypto en la que podrían enseñar criptografía sin hacer uso de matemáticas avanzadas (esencialmente para niños). Por ello, en la siguiente práctica se realizará su implementación en el lenguaje de programación Java.

Marco Teórico

La presente práctica hará uso de los siguientes conceptos:

- **Llave pública**

Es un valor público obtenido mediante un determinado algoritmo que se crea en conjunto con una llave privada y que se puede compartir con el fin de cifrar a un destinatario que posea una llave privada generada por el mismo algoritmo y con los mismos valores de entrada.

- **Llave privada**

Es un valor que solo el usuario debe ser capaz de conocer y que le permitirá descifrar un mensaje que haya sido encriptado a partir del uso de una llave pública. Se obtiene en conjunto con la llave pública haciendo uso de algún algoritmo criptográfico y/o función matemática.

- **Estructura general del funcionamiento del cifrado asimétrico**

Haciendo uso de la llave pública, privada y el mensaje (ya sea cifrado o como texto plano) se describen las siguientes operaciones fundamentales:

  - Mensaje + clave pública = Mensaje cifrado
  - Mensaje encriptado + clave privada = Mensaje descifrado
  - Mensaje + clave privada = Mensaje firmado
  - Mensaje firmado + clave pública = Autenticación

Hipótesis

Previo a la realización de este algoritmo en un lenguaje de programación y conociendo que el objetivo de Kid Krypto es enseñar a gente joven los conceptos de criptografía sin usar funciones matemáticas complejas, asumiremos que en esta implementación solo haremos uso de operaciones básicas como suma, resta, multiplicación, división y módulo.

Asimismo, podemos determinar que existirá algunos problemas para su creación al hacer uso de determinados números (probablemente 1,0 o negativos), además de alguna vulnerabilidad relacionada al tamaño de los valores que generan la llave pública y privada.

Desarrollo

¿Qué es Kid Krypto?

Kid Krypto [1] es una familia de criptosistemas desarrollados por Michael Fellows y Neal Koblitz con el fin de enseñar criptografía sin el uso de matemáticas avanzadas. Se le puede considerar como un algoritmo asimétrico debido a que hace uso de 1 llaves para cifrado y descifrado, siendo una de ellas pública y una privada.

Su objetivo principal es crear algoritmos para niños de tal forma que entiendan los conceptos básicos que un método criptográfico posea, pero tan solo haciendo uso de funciones básicas elementales que se puedan llevar a cabo incluso sin el uso de computadoras.

Funcionamiento general y pseudocódigo.

Para el funcionamiento de Kid Krypto, es posible definir las siguientes 3 operaciones básicas:

- **Generación de llaves -** A partir de 4 valores enteros introducidos por el usuario (a, b, A y B) se generará una llave privada y pública a partir de las siguientes operaciones:

$$M=a*b-1$$
$$e=A*M+a$$
$$d=B*M+b$$
$$n=(e*d-1)/M$$

  Lo que se conocerá como llave pública se conformará con la dupla **(n,e)**, mientras que la llave privada corresponderá al valor **d.**

- **Cifrado del mensaje –** Haciendo uso de un mensaje denominado como **x**, así como de los valores de la dupla **(e,n)** se generará el cifrado del mensaje tomando como referencia las siguientes operaciones:

```
aux1=x*e
aux2=aux1%n
```

Cabe destacar que los valores **aux1** y **aux2** anteriores corresponden a variables auxiliares que facilitarán el proceso de cifrado. En este caso, el mensaje cifrado corresponde a la variable **aux2.** Asimismo, que se debe cumplir que **x<n.**

- **Descifrado del mensaje –** Se realiza un proceso similar al de cifrado, solo que ahora considerando a la llave privada **d,** una cadena cifrada que se nombrará como **y**, así como una parte de la dupla que conforma a la clave pública (**n**).

```
aux1=y*d
aux2=aux1%n
```

Al igual que en el caso anterior, **aux1** y **aux2** corresponden a variables auxiliares que facilitarán el proceso de descifrado. En este caso, el mensaje descifrado corresponde a la variable **aux2.**

Implementación del algoritmo en el lenguaje de programación Java

Se selecciono Java para la implementación de este algoritmo debido a que es el lenguaje que manejo con mayor facilidad, aunque dada la naturaleza del algoritmo es posible utilizar cualquiera, ya que solo se estará haciendo uso de operaciones aritméticas básicas.

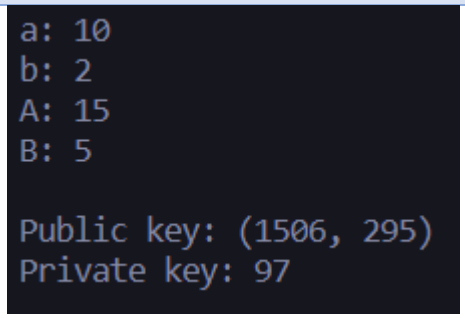
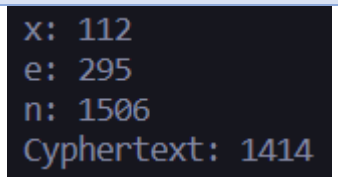
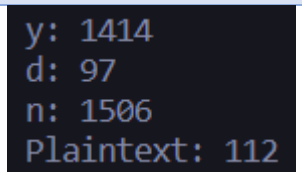
Para la aplicación del algoritmo se utilizará una única clase conocida como Main.java en la cual se creará un menú donde el usuario podrá realizar alguna acción relacionada al algoritmo de Kid Krypto y solicitará los valores que le permitirán llevarlo a cabo.

El menú de este programa contendrá las siguientes opciones para la ejecución:

1. **Generación de clave pública y privada:** Se le solicitarán al usuario los valores de a, b, A y B y mediante las operaciones indicadas en el algoritmo se generarán los valores de la dupla (n,e) para la llave pública, así como d que es la llave privada.
2. **Cifrado:** El usuario indicará el número que desee cifrar en conjunto con los valores de la clave pública generada en el paso anterior. La salida de esta opción del menú mostrará el texto cifrado.
3. **Descifrado:** El usuario indicará el texto cifrado en conjunto con la clave privada y el valor n de la llave pública para descifrar el número. Se mostrará en la pantalla el texto obtenido tras aplicar el proceso de descifrado de Kid Krypto.
4. **Salir:** Termina la ejecución del programa.

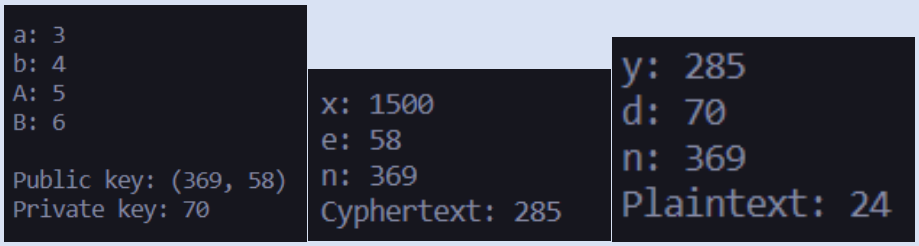
Ejemplo de funcionamiento

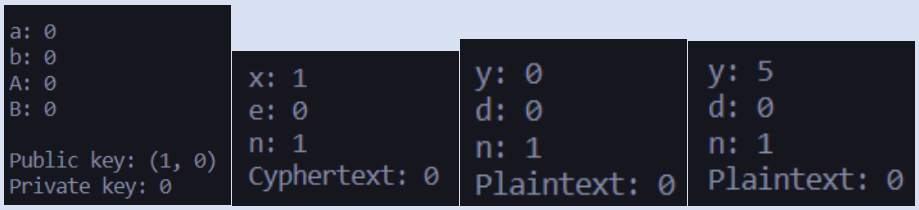
En primer lugar, probaremos con los valores indicados en las instrucciones de esta práctica: **a=10, b=2, A=15, B=5, x=112.** Compararemos el ejercicio manual con los resultados mostrados en el programa generado:

Pasos intermedios	Salida en el programa de Java
Generación de llaves	
M=(10*2)-1=19 e=(15*19)+10=295 d=(5*19)+2=97 n=((295*97)-1)/19=1506 **Llave pública: (1506,295)** **Llave privada: 97**	
Cifrado	
aux1=112*295=33040 aux2=33040%1506=1414 **Cifrado: 1414**	
Descifrado	
aux1=1414*97=137158 aux2=137158%1506=112 **Texto plano: 112**	

Deficiencias encontradas en el algoritmo

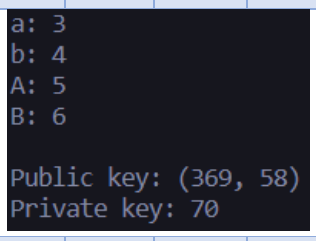
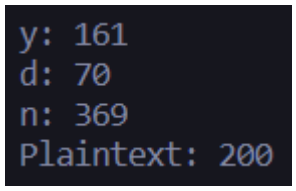
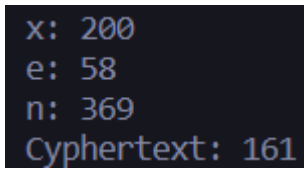
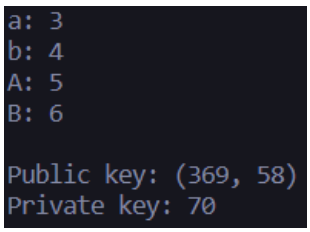
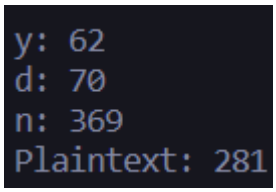
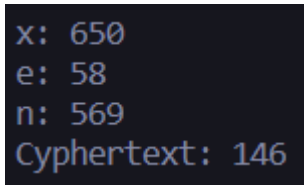
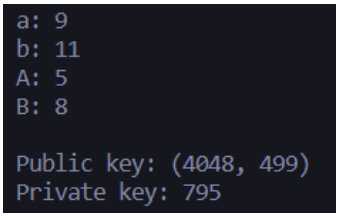
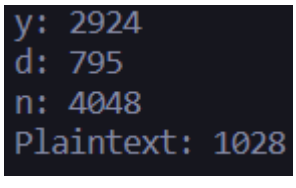
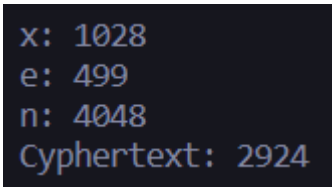
Al realizar este algoritmo se encontraron ciertas deficiencias en su implementación. Algunas de estas se explican con la siguiente tabla:

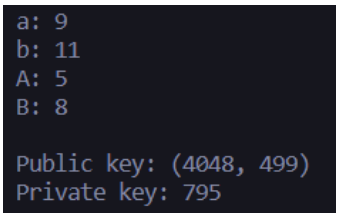
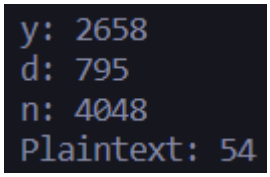
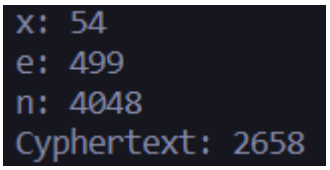
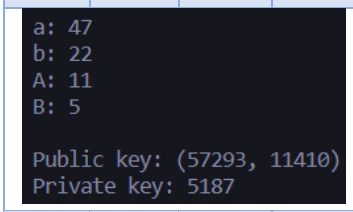
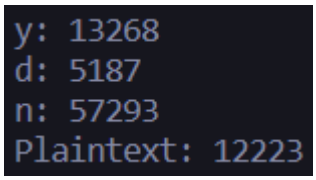
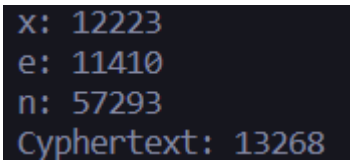
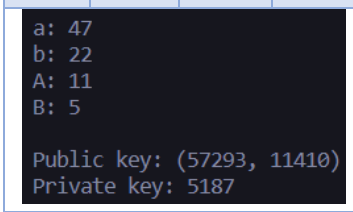
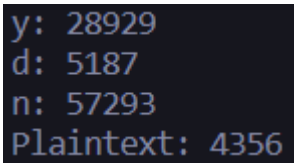
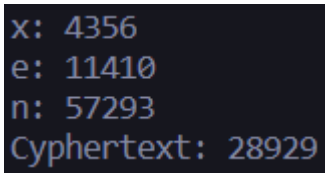
Problema	Demostración
Un número debe cumplir estrictamente la propiedad de x<n, ya que de lo contrario el cifrado no se realizará correctamente.	
Los valores a y b no pueden ser simultáneamente 1, ya que se generarán problemas al calcular n	M=1*1-1=0 

y se intentará realizar una división entre 0.	
No se pueden utilizar puros 0 en los valores, ya que genera inconsistencias en los valores de cifrado.	

Funcionamiento con vectores de prueba propuestos

A continuación, se muestran algunas capturas de pantalla de su funcionamiento tomando como referencia los vectores de prueba proporcionados para esta práctica

a	b	A	B	Texto Plano	Texto cifrado	Observaciones
3	4	5	6	200	161	
						Vector correcto.
3	4	5	6	650	62	
						Vector incorrecto ya que x<n (650>369), por lo cual se generan inconsistencias a la salida.
9	11	5	8	1028	572	
						El vector indicado para esta práctica es incorrecto. No obstante, se puede conocer el valor correcto a través del método implementado

						ya que cumple que x<n.
9	11	5	8	54	2546	
						El vector indicado para esta práctica es incorrecto. No obstante, se puede conocer el valor correcto a través del método implementado ya que cumple que x<n.
47	22	11	5	12223	13268	
						Vector correcto.
47	22	11	5	4356	28929	
						Vector correcto.

Ejecución del programa

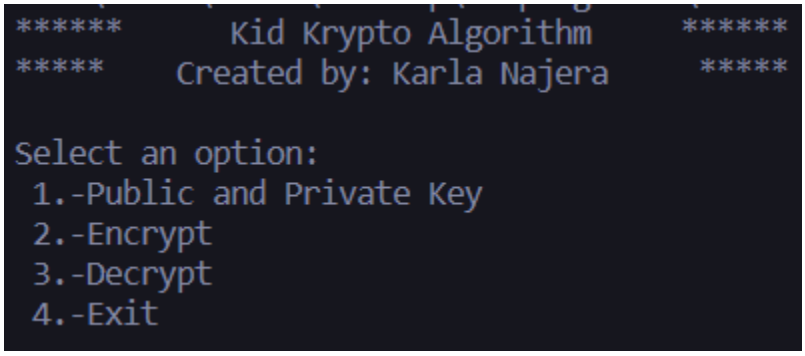
Aunque las clases ya han sido compiladas, en caso de ser requerido se puede compilar con la siguiente instrucción:

javac Main.java

Y se ejecuta con el siguiente comando:

java Main.java

Nota: Para su compilación es necesario tener instalada alguna versión de JDK, aunque la versión que fue utilizada para su elaboración es la 18.0.2.1.



Aunque se adjunta un archivo en zip con los archivos utilizados para esta práctica, se comparte el enlace de GitHub: https://github.com/kiliapplered/Practica5Cripto.git

Conclusiones

Del presente trabajo es posible obtener las siguientes conclusiones:

- A partir de la presente práctica fue posible conocer el algoritmo Kid Krypto, el cual permitirá cifrar valores enteros numéricos sin el uso de funciones matemáticas con gran complejidad.
- La hipótesis presentada para esta práctica fue correcta, siendo que hace uso de operaciones numéricas básicas.
- La implementación de este algoritmo como una solución "compleja y segura" no es para nada deseable y solo debe usarse con fines educativos (y siendo más específicos, para niños).
- La realización de este ejercicio permitió solidificar los conocimientos adquiridos durante la revisión teórica de la asignatura acerca de los algoritmos asimétricos.

Referencias

[1] M. Fellows y N. Koblitz, «Kid Krypto,» *Annual International Cryptology Conference,* vol. 740, nº 92, pp. 371-389, 1992.

Yo, Karla Andrea Najera Noyola, hago mención que esta práctica fue de mi autoría.