Criptografía + Evolutivos + Criptoanálisis

Dr. Eduardo Vázquez Fernández

IPN - ESIME Culhuacan

11-may-2018

Bosquejo de la presentación

1. Algoritmos evolutivos
2. Algoritmos de cifrado
3. Minimización de Cadenas de Adición a través de Algoritmos Evolutivos
4. Generación de curvas elípticas seguras a través de algoritmos evolutivos
5. Generación automática de factorización de números primos a través de AE
6. Criptoanálisis e Internet de las cosas

Bosquejo de la presentación

Algoritmos evolutivos

Computación evolutiva

- Engloba una serie de técnicas inspiradas biológicamente basadas en la “sobre vivencia del más apto”
- Estas técnicas se basan en los principios básicos de la teoría Neo-Darwiniana de la evolución natural de las especies
- La idea fundamental es crear un conjunto de individuos virtuales que compiten entre si buscando su sobrevivencia

Algoritmos evolutivos

Principales paradigmas

- Algoritmos Genéticos
- Programación Evolutiva
- Estrategias Evolutivas
- Evolución Diferencial

Aplicaciones de los algoritmos evolutivos

- Optimización (estructural, de topologías, numérica, combinatoria, etc.)
- Aprendizaje de máquina (sistemas clasificadores)
- Bases de datos (optimización de consultas)
- Reconocimiento de patrones (por ejemplo, imágenes)
- Generación de gramáticas (regulares, libres de contexto, etc.)
- Planeación de movimientos de robots
- Predicción
- **Seguridad informática y criptografía**

Bosquejo de la presentación

Criptografía

La **Criptografía** es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante claves entre el emisor y el destinatario, para después devolverlo a su forma original, sin que alguien más sea capaz de entenderlo.

Sistemas de cifrado de llave pública

Existen diversos sistemas de cifrado de llave pública, tales como:

- Algoritmo Rivest, Shamir y Adleman (RSA)
- Diffie-Hellman
- Digital Signature Algorithm
- ElGamal

Este tipo de algoritmos utilizan la exponenciación modular para poder cifrar y descifrar datos.

Exponenciación modular

La **exponenciación modular** consiste en encontrar un entero positivo b que satisfaga la siguiente ecuación:

$$b \equiv a^e mod\ p$$

Donde:
$a\ \epsilon\ \{0, 1, ..., p-1\}$
e es un entero positivo
p es un primo grande o producto de primos grandes

Exponenciación modular

$$b \equiv a^e mod\ p$$

- La operación anterior se debe realizar con cada dato que se necesite cifrar o descifrar.
- Es muy conveniente reducir la cantidad de multiplicaciones asociadas, ya que con esto se puede reducir el costo computacional del algoritmo involucrado.

Bosquejo de la presentación

Cadenas de adición

- Se puede reducir el número de multiplicaciones empleando cadenas de adición.
- Una **cadena de adición** es una secuencia de números donde el primer número es 1 y el último número es el exponente e.
- Cada número en la cadena es la suma de dos números previos, no siempre distintos.

Cadenas de adición

- Por ejemplo, la cadena de adición para el número 12 es la secuencia 1, 2, 4, 6 y 12.
- Si realizamos el calculo convencional de a^{12} tendríamos que realizar 11 multiplicaciones.
- Pero con la cadena de adición anterior podemos efectuar sólo cuatro multiplicaciones:

$$a^1 = a \ mod \ p$$
$$a^2 = a^1 \times a^1 (mod \ p)$$
$$a^4 = a^2 \times a^2 (mod \ p)$$
$$a^6 = a^2 \times a^4 (mod \ p)$$
$$a^{12} = a^6 \times a^6 (mod \ p)$$

Longitud de cadenas de adición

- Un número dado puede tener diferentes cadenas de adición y lo más conveniente es elegir la cadena de adición más corta.
- Por ejemplo, el número 79 tiene las siguientes cadenas de adición:
  1, 2, 4, 6, 10, 16, 26, 42, 68, 74, 78, 79 (de longitud 11)
  1, 2, 3, 6, 12, 13, 26, 52, 78, 79 (de longitud 9)
- Eligiendo la segunda cadena de adición se realizan menos multiplicaciones.

Desarrollos posibles

- Diseñar e implementar un algoritmo evolutivo para minimizar la longitud de una cadena de adición.
- Implementar el AE en un algoritmo de cifrado de llave pública para reducir su costo computacional.

Bosquejo de la presentación

Curva elíptica

- Básicamente, una curva elíptica está definida por:
  $y^2 + xy = x^3 + ax^2 + b$
- Se deben ajustar los parámetros:
  - a y b: elementos del campo finito.
  - G es el punto base.
  - n es un número primo grande que denota el orden de G.
  - h es un entero pequeño que determina el número de elementos del campo $\#E(F_q)$

Bosquejo de la presentación

Generación automática de factorización de números primos a través de AE

- Dado un entero, se debe generar una lista completa de primos de tal forma que su producto (utilizando el grado apropiado) proporcione el entero original.
- Así por ejemplo, $147 = 3 \times 7^2$

Bosquejo de la presentación

Criptoanálisis

- Busca encontrar debilidades y romper la seguridad de sistemas de cifrado sin el conocimiento de información secreta.
- Proponer algoritmos evolutivos para llevar a cabo criptoanálisis.

Internet de las cosas

- Es la interconexión digital de objetos cotidianos con Internet.
- Proponer algoritmos de cifrado para el Internet de las cosas.

eduardovf@hotmail.com