Criptología y Seguridad de los Datos

Master de Ciberseguridad y Ciberinteligencia

ETSInf - UPV

---

Criptología de clave pública

# Criptoanálisis

---

# 1. Introducción

El objetivo en este trabajo consiste en demostrar la capacidad de atacar las funciones unidireccionales en las que los métodos criptográficos de clave pública basan la seguridad. Es por lo tanto un trabajo de ataque a sistemas de clave pública.

Habitualmente son dos los problemas utilizados: el cálculo del logaritmo discreto y el problema de factorizar un entero, siendo suficiente abordar y resolver uno de estos problemas para considerar el trabajo resuelto. Para medir el grado de resolución se publicarán en Poliformat datos de distintos problemas (claves públicas) para, a partir de esta información, obtener la solución (romper la clave pública y obtener la clave privada). Notamos que este trabajo se enfoca en el proceso de ataque, por lo que se proporcionará la información de las claves a romper procesada para su uso fácil directo.

Si bien en la memoria del trabajo se necesitará probar el esfuerzo de programación realizado, se dejará a elección personal el lenguaje o entorno de programación a utilizar. En cualquier caso deberá informarse convenientemente de los parámetros utilizados y/o la configuración de los algoritmos considerada.

Independientemente de las aproximaciones abordadas, se valorará especialmente cualquier aportación original que se incluya en el esquema clásico. En caso de que se incluyan aportaciones personales, los resultados deberán compararse con los obtenidos por una versión no alterada de los mismos algoritmos para evaluar el comportamiento, aunque en la evaluación del trabajo se valorará más la justificación de la hipótesis en la que se basa la modificación que los resultados obtenidos por esta.

El trabajo puede realizarse en grupos reducidos (dos o tres personas) previa comunicación y validación por el profesorado. En ese caso, se considerará el tamaño del grupo y por lo tanto la *fuerza de trabajo* para la consideración de objetivos más ambiciosos.

**Es importante distinguir entre experimentación y pruebas de corrección**. Si bien para una prueba de corrección es suficiente con mostrar la ejecución correcta del algoritmo para algunas entradas con características que las distingan, en una experimentación es necesario obtener una representación del comportamiento considerando para cada punto de la gráfica/tabla más de una ejecución, resumiendo estas mediante medidas estadísticas (media, moda, desviación estándar,...).

# 2. Cálculo del logaritmo discreto

Dado que existen distintas aproximaciones para el cálculo del logaritmo discreto, se considerará cualquier algoritmo descrito en la literatura especializada, pudiendo incluir cualquier propuesta que se considere interesante pese a no estar incluída en el temario. En este último caso deberá justificarse adecuadamente la conveniencia de la solución. Como se ha comentado, el código desarrollado deberá probarse experimentalmente utilizando como mínomo el conjunto de problemas disponible en Poliformat.

Debido a que algunos algoritmos necesitan disponer de un conjunto de números primos, hay disponible en el sitio de la asignatura de Poliformat un listado de números primos clasificados en función de su tamaño (número de bits necesarios para codificarlo). En el mismo sitio Poliformat se pueden encontrar casos para el cálculo del logaritmo discreto que pueden ser la base de una experimentación y obtención de resultados.

La descripción de los trabajos realizados deberá incluir una descripción de, al menos, los siguientes aspectos:

- Características del ordenador utilizado en la experimentacion (procesador, velocidad, número de núcleos, cantidad de memoria RAM).
- El/los algoritmos implementados y las razones para haber considerado estos.
- Para cada problema resuelto (cada clave pública atacada con éxito) se indicará:
  - El/los algoritmos que consiguieron realizar el cálculo con éxito.
  - Los tiempos máximos (timeouts) considerados y una justificación del valor escogido.
  - El tiempo y memoria utilizados en el proceso.
- El código implementado en un apéndice. En caso que se considere necesario, una descripción de la estructura de este código y la relación entre sus componentes.

Aunque la evaluación del trabajo no considerará una comparativa entre los resultados empíricos obtenidos por distintos grupos. En cualquier caso, deberá incluirse en la memoria una discusión de los resultados obtenidos,

la aproximación con mejor comportamiento comparado y las razones de un posible comportamiento anómalo.

Por supuesto, dependiendo de las características de cada trabajo, podría ser necesario incluir la descripción de aspectos no enumerados.

# 3. Factorización de enteros

Como sucede para el cálculo del logaritmo discreto, existen distintas aproximaciones para obtener la factorización de enteros que no se incluyen en el temario de la asignatura. En este caso será necesario implementar, al menos, dos algoritmos, pudiendo ser estos los vistos en el temario o cualquier otra propuesta que se considere interesante, justificando adecuadamente la consideración de esta inclusión.

En la elección hay que tener presente que hay algoritmos que únicamente garantizan un comportamiento aceptable si el problema de entrada cumple determinadas características. En el listado de retos no se indicará ninguna de las posibles características que facilitarían el ataque a estas *claves*.

Como se ha comentado, el código desarrollado deberá probarse experimentalmente utilizando el conjunto de problemas disponible en Poliformat.

La descripción de los trabajos realizados deberá incluir una descripción de, al menos, los siguientes aspectos:

- Características del ordenador utilizado en la experimentacion (procesador, velocidad, número de núcleos, cantidad de memoria RAM).
- Los algoritmos implementados y las razones para haber considerado estos.
- Para cada problema resuelto (cada clave pública atacada con éxito) se indicará:
  - El/los algoritmos que consiguieron realizar el cálculo con éxito.
  - El tiempo y memoria utilizados en el proceso.

El código implementado se incluirá en un apéndice. En caso que se considere necesario, una descripción de la estructura de este código y la relación entre sus componentes. El código deberá estar a disposición (no es necesario

aportarlo en primera instancia) para que, en caso que se considere necesario por el profesorado, se puedan replicar las pruebas enumeradas en la memoria.

Aunque la evaluación del trabajo no considerará una comparativa entre los resultados empíricos obtenidos por distintos grupos. En cualquier caso, deberá incluirse en la memoria una discusión de los resultados obtenidos, la aproximación con mejor comportamiento comparado y las razones de un posible comportamiento anómalo.

Por supuesto, dependiendo de las características de cada trabajo, podría ser necesario incluir la descripción de aspectos no enumerados.

# 4. Evaluación

El trabajo supone un 20 % de la nota final de la asignatura. Para ofrecer distintas alternativas de conseguir la máxima nota (100 puntos) en el trabajo se considerarán los siguientes hitos:

**Factorización de enteros**

- Implementación base de los algoritmos de Fermat, Pollard-rho, Pollard $p-1$. Experimentación base considerando los tres algoritmos, distintas tallas de problema y un mínimo de 10 factorizaciones por cada una. Exposición gráfica de los resultados obtenidos. Discusión de resultados obtenidos. ..... (20 puntos)
- Implementación base del algoritmo de Lenstra para la factorización de enteros. Experimentación base considerando distintas tallas de problema y un mínimo de 10 factorizaciones por cada una. Discusión (y comparación si procede) de los resultados obtenidos. ..... (40 puntos)
- Implementación base del algoritmo de criba cuadrática para la factorización de enteros, no considerando implementaciones que no se ajusten a los parámetros del algoritmo. Experimentación base considerando distintas tallas de problema y un mínimo de 10 factorizaciones por cada una. Discusión y compativa de de los resultados obtenidos. (40 puntos)
- Implementación base de otros algoritmos de factorización en la literatura científica. Descripción del método. Experimentación base considerando distintas tallas de problema y un mínimo de 10 factorizaciones por cada una. Discusión de resultados. ..... (20 puntos c.u.)

- Experimentación extendida considerando uno o ambos puntos siguientes:
  - Un conjunto de test que considere el tiempo de resolución en función del tamaños de problema (número de bits del valor a factorizar) para problemas no considerados en la experimentación base. La experimentación deberá analizar resultaos de más de 50 números factorizados de cada uno de los tamaños de problema.
  - (Si fuera aplicable) Estudio del comportamiento del algoritmo en función de los parámetros internos de este.

  En cualquier caso, estudio estadístico en función de la talla de los números. Exposición gráfica de los resultados obtenidos. Discusión de resultados ..... (35 puntos)

- Implementación alternativa de un método original o modificación de uno ya descrito. Descripción y justificación de la hipótesis. Implementación y experimentación comparada con el/los algoritmos base (al menos uno). Exposición gráfica de los resultados obtenidos. Discusión de resultados ..... (30 puntos)

**Logaritmo discreto**

- Implementación de los algoritmos Baby-step Giant-step y Pollard-rho para el cálculo del logaritmo discreto. Experimentación base considerando ambos algoritmos, obteniendo tiempos de cálculo para distintas tallas de problema y un mínimo de 10 problemas por cada una de las tallas. Representación gráfica de los resultados obtenidos. Discusión de resultados. ..... (40 puntos)

- Implementación base del algoritmo Index-calculus para el cálculo del logaritmo discreto. Experimentación base obteniendo tiempos de cálculo para distintas tallas de problema y un mínimo de 10 problemas por cada una de las tallas. Representación gráfica de los resultados obtenidos. Discusión, comparando si procede los resultados con otros métodos implementados, de los resultados obtenidos. ..... (40 puntos)

- Implementación base de otros algoritmos para el cálculo del logaritmo discreto en la literatura científica. Descripción del método. Experimentación base considerando distintas tallas de problema y un mínimo de

10 problemas por cada una de las tallas. Exposición gráfica de los resultados obtenidos.Discusión (y comparación si procede) de los resultados obtenidos. ..... (35 puntos)

- Experimentación extendida considerando distintas tallas de problema no analizadas en el previo y un mínimo de 50 casos por cada una de las tallas del problema. Alternativamente, estudio del comportamiento de los algoritmos considerando distintas configuraciones de estos. Estudio estadístico en función de la talla de los números. Exposición gráfica de los resultados obtenidos.Discusión (y comparación si procede) de los resultados obtenidos. ..... (30 puntos)
- Implementación alternativa. Descripción y justificación de la hipótesis. Implementación y experimentación comparada con el/los algoritmos base (al menos uno). Exposición gráfica de los resultados obtenidos. Discusión de resultados ..... (35 puntos)

En todos los apartados considerados se muestra la puntuación máxima a obtener. Una puntuación de 100 o mayor supone una puntuación máxima en el trabajo.