INSTITUTO TECNOLÓGICO DE BUENOS AIRES

Informe Trabajo Práctico Especial

Criptografía y Seguridad [72.44] - 2021 1C

Boccardi, Luciano (59518)
lboccardi@itba.edu.ar

Puig, Tamara (59820)
tpuig@itba.edu.ar

Zuberbuhler, Ximena (57287)
xzuberbuhler@itba.edu.ar

14 de junio de 2021

1. Recuperación del Secreto

Figura 1.1: Imágen recuperada a partir de los archivos dados.

1.1. Conclusiones de la ejecución del programa

El archivo asignado al grupo consistía de 4 imágenes BMP. Se recuperó el secreto con un esquema de 4 imágenes portadoras y el resultado fue la imagen mostrada en la Figura1.1. Habiendo seguido el algoritmo de manera correcta, se puede concluir que la recuperación fue efectiva.

2. Cuestiones a Analizar

2.1. Aspectos relativos al documento

El paper analizado tiene una estructura muy bien organizada. Primero se realiza una mención del estado del arte, y trabajos previos del mismo tema. Luego, se comienza a describir la idea y la teoría que la respalda. Se explican las etapas de encripción y desencripción con diagramas de flujo, lo cual ayuda a comprender el procedimiento. Por último, se detalla la carga útil y se realizan comparaciones con los métodos detallado al comienzo del informe.

En cuanto a la descripción de los algoritmos, si bien es sumamente clara, se encontraron algunos problemas en las fórmulas. Muchos de los signos '-' no aparecen, e incluso en la fórmula

7 está mal detallada ya que refiere a s_0 y no a s_{r-1} como debería. No obstante, al ser fórmulas correspondientes a un método de interpolación ampliamente conocido, no hubieron mayores inconvenientes. El resto del detalle es detallado y completo, con un grado de detalle adecuado para poder ser comprendido por personas con una formación correspondiente.

La notación es correcta, no obstante, los índices a los que se refieren suelen entrar en conflicto con los utilizados en las fórmulas matemáticas. Por ejemplo, se utiliza j para denominar el número de bloque, y en la fórmula de interpolación se itera sobre el índice q. Quizás hubiera sido mejor optar por definir otros índices para evitar esos conflictos.

Por último, existe un debate cuestionable entre comenzar a indexar con el número 0 o con el número 1. No nos parece relevante discutir sobre cuál es más adecuado, ya que todo depende del lenguaje en el cual se trabaje. A fines de un paper, es correcto porque se mantiene consistente a lo largo del mismo.

2.2. Optimización de la carga útil

Cuando en el paper se refiere a la carga útil está hablando de cuánta información se guarda en cada sombra. Si asumimos que el bloque (4 píxeles = 4 bytes) es la menor unidad de información, entonces podemos establecer una comparación.

Suponiendo que todas las shadows son del mismo tamaño que coincide con el tamaño del secreto. Sea k el número de sombras y L el tamaño del secreto, la imagen se divide en $\frac{L}{k}$ conjuntos de k elementos. Por cada conjunto, se guarda 1 elemento en un bloque de $2x2$.

Es fácil notar que si $k = 4$, se utilizan $\frac{L}{k} * 4$ píxeles, que es exactamente el mismo tamaño que la imagen original.

En el caso $k > 4$, se puede definir un factor de carga $f = \frac{4}{k}$ que define qué porcentaje de cada imagen se ocupa guardando el secreto. Para $k = 5$, $f = 0{,}8$, y para $k = 6$, $f = 0{,}67$.

No se menciona la optimización de la carga útil en ningún momento. Pero podemos suponer que tiene que ver con el tamaño de bloque escogido. En bloques de $2x2$ se utilizan los 3 bits menos significativos de 3 píxeles para guardar el valor de F. En bloques más grandes se alteran menos bits a cambio de una menor modificación en los datos de la shadow, con el inconveniente de que aumenta el tamaño mínimo requerido.

Puede verse que mientras mayor es k, se necesitan más portadoras pero el tamaño requerido de cada una para guardar el secreto es menor. Si consideramos que L es, en bytes, la cantidad de datos "secretos", como mínimo para recuperarlos se necesita $4 * L$.

2.3. Trabajar en GF(2^8) en lugar de Operaciones Modulares

La principal ventaja que ofrece trabajar con campos de Galois GF(2^8) es que no tiene problema para generar valores en el rango $[0,255]$, lo cual es fundamental para la recuperación de los datos. Es por esto que el algoritmo se puede aplicar para recuperar cualquier tipo de archivo binario, no solo imágenes, sin pérdida de información. Si trabajáramos con congruencias Mod 251 o Mod 257 que son los dos primos más cercanos al rango, es explícita la pérdida de datos.

Las desventaja más importante tiene que ver con la dificultad de operar en los campos de Galois, lo cual aumenta la complejidad de las operaciones y hace mucho más difícil el debugging del código. Además, para operar en el campo se necesita conocer el polinomio generador correspondiente. Por ende, dos personas que operen con el mismo algoritmo pero empleen un polinomio distinto, van a obtener resultados inconclusos entre sí.

2.3.1. Suppose "chuckïmplies vomiting.

A woodchuck can ingest 361.92 cm^3 (22.09 cu in) of wood per day. Assuming immediate expulsion on ingestion with a 5% retainment rate, a woodchuck could chuck **343.82 cm^3** of wood per day.

BONUS: SUPPOSE THERE IS NO WOODCHUCK. Fusce varius orci ac magna dapibus porttitor. In tempor leo a neque bibendum sollicitudin. Nulla pretium fermentum nisi, eget sodales magna facilisis eu. Praesent aliquet nulla ut bibendum lacinia. Donec vel mauris vulputate, commodo ligula ut, egestas orci. Suspendisse commodo odio sed hendrerit lobortis. Donec finibus eros erat, vel ornare enim mattis et.

3. INTERPRETING EQUATIONS

3.1. Identify the author of Equation 3.1 below and briefly describe it in English.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{3.1}$$

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent porttitor arcu luctus, imperdiet urna iaculis, mattis eros. Pellentesque iaculis odio vel nisl ullamcorper, nec faucibus ipsum molestie. Sed dictum nisl non aliquet porttitor. Etiam vulputate arcu dignissim, finibus sem et, viverra nisl. Aenean luctus congue massa, ut laoreet metus ornare in. Nunc fermentum nisi imperdiet lectus tincidunt vestibulum at ac elit. Nulla mattis nisl eu malesuada suscipit.

3.2. Try to make sense of some more equations.

$$\begin{aligned}(x+y)^3 &= (x+y)^2(x+y)\\ &= (x^2+2xy+y^2)(x+y)\\ &= (x^3+2x^2y+xy^2)+(x^2y+2xy^2+y^3)\\ &= x^3+3x^2y+3xy^2+y^3\end{aligned} \tag{3.2}$$

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

$$A = \begin{bmatrix} A_{11} & A_{21} \\ A_{21} & A_{22} \end{bmatrix} \tag{3.3}$$

Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem.

4. Viewing Lists

4.1. Bullet Point List

- First item in a list
  - First item in a list
    - First item in a list
    - Second item in a list
  - Second item in a list
- Second item in a list

4.2. Numbered List

1. First item in a list
2. Second item in a list
3. Third item in a list

5. Interpreting a Table

Per 50g	**Pork**	**Soy**
Energy	760kJ	538kJ
Protein	7.0g	9.3g
Carbohydrate	0.0g	4.9g
Fat	16.8g	9.1g
Sodium	0.4g	0.4g
Fibre	0.0g	1.4g

Cuadro 5.1: Sausage nutrition.

5.1. The table above shows the nutritional consistencies of two sausage types. Explain their relative differences given what you know about daily adult nutritional recommendations.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent porttitor arcu luctus, imperdiet urna iaculis, mattis eros. Pellentesque iaculis odio vel nisl ullamcorper, nec faucibus ipsum molestie. Sed dictum nisl non aliquet porttitor. Etiam vulputate arcu dignissim, finibus sem et, viverra nisl. Aenean luctus congue massa, ut laoreet metus ornare in. Nunc fermentum nisi imperdiet lectus tincidunt vestibulum at ac elit. Nulla mattis nisl eu malesuada suscipit.