Profesor: Alejandro Hevia
Auxiliar: Bryan Ortiz
Ayudante: David Contreras

CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE CHILE

Tarea 3

Hashing, MACs, Encriptación Autenticada y Diffie-Hellman

Fecha de Entrega: 22 de Noviembre

P1. En los protocolos de red, resulta útil aplicar encriptación autenticada para proteger el cuerpo de los paquetes transmitidos. Sin embargo, los headers deben permanecer en texto plano para que los routers puedan acceder a su información y enviar los paquetes a su destino. Aún así, nos interesa garantizar que el header (o buena parte de él) no haya sido modificado en el camino, esto es, asegurar su integridad de algún modo. En esta pregunta, extendemos la sintaxis y seguridad de los esquemas de encriptación autenticada con el fin de cubrir este caso de uso.

Definición (*Encriptación Autenticada con Datos Asociados*): extendemos la definición de un esquema de encriptación autenticada para permitir que los algoritmos de encriptación y desencriptación reciban un conjunto de datos asociados $d \in \mathcal{D}$, cuya integridad es protegida por el esquema de cifrado, no así su confidencialidad. La sintaxis de un esquema de encriptación autenticada con datos asociados es la siguiente:

- $\mathcal{G}$: Algoritmo probabilístico que genera una clave k.
- $\mathcal{E}(k, m, d)$: Algoritmo de encriptación que toma como entrada una clave k, un mensaje m, y un conjunto de datos asociados d, a partir de los cuales produce un texto cifrado c.
- $\mathcal{D}(k, c, d)$: Algoritmo de desencriptación que toma como entrada una clave k, un texto cifrado c, y un conjunto de datos asociados d, y retorna un mensaje m o $\perp$ en caso de error (en cuyo caso decimos que (c, d) no es auténtico).

Proceda como sigue:

a) Adapte los juegos y definiciones utilizados para definir la seguridad (tanto la confidencialidad como la integridad) de un esquema de autenticación autenticada, para el caso de un esquema de encriptación autenticada con datos asociados.

b) Plantee un esquema de encriptación autenticada con datos asociados apropiado, y demuestre que es seguro bajo las definiciones de seguridad que propuso en el ítem anterior.
Hint: recuerde el comportamiento de EtM *cuando el tanto el sistema de encriptación como el MAC utilizados son seguros.*

P2. Sea $\mathbb{G}$ un grupo cíclico de orden q, para q primo de k bits, donde k es un parámetro de seguridad, y sea $g \in \mathbb{G}$ un generador de $\mathbb{G}$. Sea además, $n \in \mathbb{N}$ un parámetro polinomialmente acotado en k, esto es, $n = k^c$ para c constante. Se define la siguiente función de hash $H : \mathbb{Z}_q^n \to \mathbb{G}$ como:

$$H(x_1, x_2, \ldots, x_n) = g_1^{x_1} \cdot g_2^{x_2} \cdot \ldots \cdot g_3^{x_n}$$

donde $g_1, g_2, \ldots, g_n$ son elementos aleatorios de $\mathbb{G}$. El objetivo de esta pregunta es demostrar que H es resistente a colisiones bajo el supuesto de que calcular el logaritmo discreto en $\mathbb{G}$ es computacionalmente difícil. Para ello, considere lo siguiente:

Definición: Sea $\mathbb{G}^n$ un grupo cíclico de orden q generado por $g \in G$, y sea $n \in \mathbb{N}$ un parámetro polinomialmente acotado. Un algoritmo *busca-relaciones* $\mathcal{A}_{rf}$ recibe como input la tupla $(g_1, g_2, \ldots, g_n) \in \mathbb{G}^n$, y devuelve otra tupla $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_q^n$ tal que:

$$g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \ldots \cdot g_n^{\alpha_n} = 1$$

donde $\alpha \neq (0, 0, \ldots, 0)$, y es llamado una *relación no trivial* para $g_1, g_2, \ldots, g_n \in \mathbb{G}$. Luego, se define la ventaja de un adversario *busca-relaciones* $\mathcal{A}_{rf}$ como:

$$\mathbf{Adv}_{G,g}^{\mathsf{rf}}(\mathcal{A}_{rf}) = Pr\left[g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \ldots \cdot g_n^{\alpha_n} = 1\right]$$

Teorema ♣: Para todo algoritmo eficiente $\mathcal{A}_{rf}$ que busca relaciones no triviales en $\mathbb{G}^n$, existe un algoritmo eficiente $\mathcal{B}_{dl}$ que resuelve el problema del logaritmo discreto en $\mathbb{G}$, tal que:

$$\mathbf{Adv}^{\mathsf{rf}}_{G,g}(\mathcal{A}_{rf}) \leq \mathbf{Adv}^{\mathsf{dl}}_{G,g}(\mathcal{B}_{dl}) + \frac{1}{q}$$

Finalmente:

a) Demuestre que para todo adversario eficiente $\mathcal{A}$ que intenta encontrar una colisión para H, existe un adversario eficiente $\mathcal{B}$ que resuelve el problema del logaritmo discreto en $\mathbb{G}$, tal que:

$$\mathbf{Adv}^{\mathsf{cr}}_{H}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{dl}}_{G,g}(\mathcal{B}) + \frac{1}{q}$$

b) **[Bonus, 1pt]** demuestre el teorema ♣.