IIC3253: Criptografía y Seguridad Computacional **2018-01**

Tarea 2: 17/05/2018

Entrega Final: 01/06/2018

Reglas

TODOS LOS PROBLEMAS SON OBLIGATORIOS

Las tareas se pueden discutir de a 2 estudiantes. Sin embargo, cada uno tiene la obligación de escribir su propia solución. La entrega final de la tarea se realiza mediante correo electrónico firmado a `gnmonsalve@uc.cl`, `masanmartin@uc.cl`, `faflorenzano@uc.cl` y a `fekrell@uc.cl` con el asunto `[IIC3253] Entrega Tarea 3` a las 22:00 del día de la entrega. Cada estudiante sólo puede asumir que su tarea ha sido correctamente entregada si recibe un correo electrónico de respuesta correctamente firmado por algún miembro del cuerpo docente. Usted debe entregar un archivo pdf generado en LaTeX. Se sugiere utilizar el template publicado en la página web del curso, y que la solución para cada pregunta quede en una hoja distinta.

HINT: UTILICE HORARIOS DE CONSULTA Y FORO PIAZZA

Problema 1 [15pts]

Calcule a mano lo siguiente (puede ocupar el teorema del resto chino).

1. **[5 pts]** Los últimos 2 dígitos de 7^{35688}. Hint: $\phi(\prod P_i^{e_i}) = \prod P_i^{e_i-1}(P_i - 1)$, para P_i primo y $e_i \in \mathbb{N}$.
2. **[5 pts]** $[233^{230000022} \mod 35]$
3. **[5 pts]** $[46^{51} \mod 55]$

Problema 2 [15pts]

Sea $\mathbb{G}$ es un grupo cíclico de orden n y generador g.

- **[4 pts]** Demuestre que $\mathbb{Z}_n$ y $\mathbb{G}$ son isomorfos.
- **[8 pts]** Asumiendo que $n = p \cdot q$, en donde p y q son primos distintos ¿Cuántos generadores tiene $\mathbb{G}$? Demuestre su resultado.
- **[3 pts]** Generalice el resultado anterior para n entero positivo cualquiera.

Problema 3 [15pts]

Sean N, e tales que $\mathsf{mcd}(e, \phi(N)) = 1$ y asuma que existe un adversario probabilista $\mathcal{A}$ que corre en tiempo t tal que

$$\Pr[\mathcal{A}(e, N, x^e \mod N) = x] = 0{,}01$$

en donde x es uniforme en $\mathbb{Z}_N^*$. Construya un adversario probabilista $\mathcal{A}'$ que corra en tiempo polinomial en t y $||N|| = \log N$ tal que:

$$\Pr[\mathcal{A}'(e, N, x^e \mod N) = x] = 0{,}99$$

para todo x (es decir, x no es necesariamente elegido uniformemente, por lo que no hay ninguna garantía de que $\mathcal{A}$ retorne x con probabilidad 0.01).

Hint: dado $x^e \mod N$ para cualquier x en $\mathbb{Z}_N^*$, genere un elemento y^e tal que y sea uniformemente aleatorio en $\mathbb{Z}_N^*$.

Problema 4 [15pts]

Imaginen que Alice y Bob intercambian llaves utilizando el protocolo de Diffie-Hellman, y luego utilizan la llave acordada para comunicarse privadamente mediante un esquema de cifrados simétrico autenticado. Muestre cómo un adversario que escucha *y modifica* mensajes en el canal de comunicación durante el protocolo Diffie-Hellman puede escuchar la conversación privada entre Alice y Bob ¿Qué más puede el adversario hacer?