

OBSERVACIONES PARA EL EXAMEN.

NOTACIÓN: \mathcal{A} será un alfabeto (conjunto finito no vacío de símbolos).

EJERCICIO 1. *Cifrado de Vigenère.*

Solución. El cifrado de Vigenère consiste en una clave $\alpha \in \exp(\mathcal{A})^*$ y sendas funciones E_α y D_α , para cifrar y descifrar respectivamente. Podemos definir $E_\alpha : \exp(\mathcal{A})^* \rightarrow \exp(\mathcal{A})^*$ como:

$$E_\alpha(s) = \langle f^{-1}((f(s_j) + f(\alpha^{len(s)})_j) \bmod n) \rangle_j.$$

Teniendo en cuenta que:

- f es la inyección que asigna a cada letra un entero.
- Consideramos $\alpha^{len(s)}$ para asegurar la existencia de una letra en la posición j . Es decir, estamos repitiendo la clave hasta alcanzar la longitud de la palabra s (truncando si hace falta). Por ejemplo, si $\alpha = \text{HOLA}$, entonces $\alpha^3 = \text{HOLAHO-LAHOLA}$.
- $\langle \rangle_j$ representa que es una palabra.
- n es el cardinal del alfabeto empleado.

De modo análogo se define $D_\alpha : \exp(\mathcal{A})^* \rightarrow \exp(\mathcal{A})^*$ como:

$$D_\alpha(s) = \langle f^{-1}((f(s_j) - f(\alpha^{len(s)})_j) \bmod n) \rangle_j.$$

Veamos que $D_\alpha \circ E_\alpha = 1_{\exp(\mathcal{A})^*}$. Consideramos $s = \langle s_j \rangle_j$ una expresión de $\exp(\mathcal{A})^*$. Entonces:

$$\begin{aligned} D_\alpha(E_\alpha(s)) &= D_\alpha(\langle f^{-1}((f(s_j) + f(\alpha^{len(s)})_j) \bmod n) \rangle_j) \\ &= \langle f^{-1}((f(f^{-1}((f(s_j) + f(\alpha^{len(s)})_j) \bmod n)) - f(\alpha^{len(s)})_j) \bmod n) \rangle_j \\ &= \langle f^{-1}(((f(s_j) + f(\alpha^{len(s)})_j) \bmod n) - f(\alpha^{len(s)})_j) \bmod n) \rangle_j \\ &= \langle f^{-1}(f(s_j) \bmod n) \rangle_j \\ &= \langle f^{-1}(f(s_j)) \rangle_j \\ &= \langle s_j \rangle_j \\ &= s. \end{aligned}$$

Por último, queda un resultado útil para ver que en realidad ambas funciones son la misma con diferente clave.

Sea α una clave, entonces definiendo $\alpha' = \langle (-\alpha_j) \bmod n \rangle_j$ tenemos que $E_{\alpha'} = D_{\alpha}$.

EJERCICIO 2. *Explicar la transformación SubBytes() que es parte del algoritmo simétrico de cifrado AES.*

EJERCICIO 3. *Limitaciones de los sistemas simétricos de cifrado en la comunicación y cómo la criptografía de clave pública los ha resuelto.*

EJERCICIO 4. *Explicar los fundamentos de la criptografía de clave pública y las líneas fundamentales de la firma a través de la misma.*

EJERCICIO 5. *Enumerar resumidamente las precauciones más destacables a tomar al generar un círculo de comunicación basado en RSA.*

EJERCICIO 6. *Protocolo de intercambio de llaves según el esquema de Diffie-Hellman y explicación de su supuesta fortaleza.*

EJERCICIO 7. *Explicación del criptosistema de ElGamal.*

EJERCICIO 8. *Explicación del algoritmo de firma estándar (DSA).*

EJERCICIO 9. *Rasgos esenciales de SSH: cifrado, funcionamiento, negociación de cifrado para la sesión y autenticación del acceso del usuario al servidor*