LibreIM

Seguridad y Protección de Sistemas Informáticos
Grado en Ingeniería Informática
Universidad de Granada

24 de diciembre de 2019

Observaciones para el examen.

Ejercicio 1. *Cifrado de Vigenere.*

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

$$E_\alpha(s) =< f^{-1}((f(s_j) + f(\alpha^l en(s))_j) mod n) >_j$$

Teniendo en cuenta que:

- f es la inyección que asigna a cada letra un entero.
- Consideramos $\alpha^l en(s)$ para tener claro que existe una letra en la posición j. Es decir en verdad solo estamos repitiendo muchas veces la clave (sea α = HOLA, pues α^3 =HOLAHOLAHOLA).
- $<>_j$ representa que es una palabra.
- n es el cardinal del alfabeto empleado.

De modo análogo se define $E_\alpha : exp(\mathscr{A})^* \longrightarrow exp(\mathscr{A})^*$ como:

$$D_\alpha(s) =< f^{-1}((f(s_j) - f(\alpha^l en(s))_j) mod n) >_j$$

Se puede comprobar fácil que D es la inversa de E por izquierda y derecha.

Como último queda un resultado útil para ver que en realidad ambas funcione son solo un mismo sistema con diferente clave.

Sea α una clave, entonces definiendo $\alpha' =< (-\alpha_j) mod n >_j$

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 criptografíade clave pública los ha resuelto.*

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

Ejercicio 5. *Enumerar resumidamente las precauciones más destacables a tomar al generar un cículo decomunicación basado en RSA.*

Ejercicio 6. *Protocolo de intercambio de llaves según el esquema de Diffie-Hellman y explicación de susupuesta 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 yautenticación del acceso del usuario al servidor*