LibreIM

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

26 de diciembre de 2019

Observaciones para el examen.

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

Ejercicio 1. *Cifrado de Vigenère.*

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

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

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 α = HOLA, entonces α^3 =HOLAHOLAHOLA.
- $\langle\rangle_j$ representa que es una palabra.
- n es el cardinal del alfabeto empleado.

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

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

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

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

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.*

El algoritmo de cifrado de AES realiza en cada ronda una serie de transformaciones a nivel de bytes. La primera de estas transformaciones es `SubBytes()`, que consiste en sustituir los bytes del estado según una tabla de sustitución, llamada S-box. Así, la sustitución se hace de forma no lineal e independiente.

La tabla de sustitución es una matriz (no simétrica) que contiene en cada posición un byte (en hexadecimal). La construcción de la tabla se realiza de la siguiente forma, dada una entrada xy:

1. Si $xy = 00$, se mantiene igual. Si $xy \neq 00$, se calcula el inverso de xy en $\mathrm{GF}(2^8)$, que será otro byte $b = b_7 \dots b_0$.
2. El bit i-ésimo del byte b, b_i, se transformará en b'_i de la siguiente forma:

   $$b'_i = b_i + b_{(i+4) \bmod 8} + b_{(i+5) \bmod 8} + b_{(i+6) \bmod 8} + + b_{(i+7) \bmod 8} + c_i,$$

   donde c_i es el i-ésimo bit del byte $\{63\}$ o $\{01100011\}$ para todo $0 \leq i \leq 8$. El byte b' resultante ocupará la posición (x, y) de la tabla.

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 cículo 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*