LibreIM

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

30 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.*

Solución. 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.*

Solución. En la criptosistemas de clave simétrica, emisor y receptor acuerdan una clave k que marca como funcionarán las funciones E_k y D_k, y cualquier persona que tenga esta clave puede entrar en la comunicación.

Esto conlleva diferentes problemas:

- El intercambio inicial de la clave se tiene que hacer de algún modo seguro antes de poder establecer el canal encriptado. Esto es uno de los mayores problemas de la criptografía clásica. Si bien, se pudieron vadear en un inicio por medios militares y personas de confianza, esto se hace imposible cuando, por ejemplo, estamos hablando de encriptar transacciones comerciales donde los involucrados son completos desconocidos. Además el coste de este intercambio es demasiado alto considerando la posibilidad de que no se vuelva a necesitar nunca más el canal.

- Cuando consideramos una red de usuarios, hemos de tener una clave para cada par de usuarios para tener máxima seguridad. Esto hace que tengamos un ratio de crecimiento del número de claves cuadrático en relación al tamaño de la red. Claramente no es un sistema escalable. Por ejemplo, con 10

usuarios necesitamos 45 claves diferentes y con 100 usuarios necesitaremos 4950 claves.

Por este motivo no es fácil añadir un usuario a la red y actualizar la base de datos. Este gran número de claves es también un problema de seguridad al ser necesario que cada usuario guarde sus claves.

- Estos sistemas también adolecen de falta de crédito, ya que ambos usuarios tienen la misma clave en cada pareja emisor receptor.

  Si Alice y Bob comparten una clave secreta y se da que Carol la descubre, esta puede interceptar los mensajes de Alice a Bob y modificarlos sin que Bob lo descubra. También es posible que Bob envíe mensajes falsos y después se encubra en esta posibilidad para eximirse de las culpas.

A raiz de esto, necesitamos un nuevo criptosistema que satisfaga: autenticación, integridad y no repudiabilidad. El criptosistema de clave pública soluciona estos problemas:

- Al tener una función E pública y una D privada deja de haber problema con el intercambio de claves en un canal seguro, dado que este intercambio inicial no se produce.

- Solo se mantienen dos claves por usuario del círculo, lo que es mucho más clave. Más aún, en la base de datos solo se guarda la clave pública de cada usuario.

- Se implementa un sistema de autenticación y no repudio del siguiente modo: Como E y D son biyecciones e inversas. Sean $A = \{E_a, D_a\}$ las funciones de Alice y $B = \{E_b, D_b\}$ las funciones de Bob. Para que Alice envíe un mensaje a Bob encripta el mensaje m con $E_b(D_a(m))$. Cuando Bob lo recibe, primeramente lo desencipta con su función privada, y posteriormente para comprobar que efectivamente es de Alice lo desencripta con su función pública. Así se sabe que es de Alice y solo puede ser suyo pues es la única que posee la función inversa de E_a.En la criptosistemas de clave simétrica, emisor y receptor acuerdan una clave k que marca como funcionaran las funciones E_k y D_k, y cualquier persona que tenga esta clave puede entrar en la comunicación.

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*