Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 6. Firma digital. Protocolos criptográficos.

---

1. Jugando a piedra, papel o tijera. Supongamos que Alice y Bob quieren jugar a piedra, papel o tijera a través de un sistema de mensajería, y lo hacen usando una función hash H – definida en el dominio apropiado – siguiendo el siguiente protocolo:

   Paso 1. Alice elige $s_A \in \{\texttt{piedra}, \texttt{papel}, \texttt{tijera}\}$. Elige una cadena de bits al azar r_a y envía a Bob el resumen $h_A = H(r_a || s_a)$

   Paso 2. Bob elige $s_B \in \{\texttt{piedra}, \texttt{papel}, \texttt{tijera}\}$ y se lo envía a Alice,

   Paso 3. Alice envía a Bob r_a, s_a. Ahora, Bob comprueba que el hash de los valores recibidos coincide con h_A y, si es correcto, ambos aceptan el resultado del juego.

   ¿Con qué tipo de protocolo criptográfico asocias esta construcción? ¿qué propiedad de este protocolo garantizaría que es justo para Alice? ¿Y para Bob? ¿qué hemos de pedir a la función hash H para que esas propiedades se cumplan?

2. Trabajaremos en $\mathbb{Z}_{17}^*$ y vamos a compartir un secreto $S = 2$ usando un esquema de Shamir con umbral 3, es decir, para que se requiera un mínimo de 3 "shares"de la forma $s_i = (i, f(i))$ de cara a recuperar el secreto. Recordemos que éste se calcula obteniendo un poninomio f, que en este caso será de grado 2, cuyo término independiente es el secreto.

   Escribe los valores que recibirá un conjunto de $n = 6$ participantes, estudia cómo recuperan el secreto los participantes del conjunto $\{P_1, P_2, P_3\}$ y justifica que un conjunto (cualquiera, de tu elección) de dos participantes no aprende nada sobre S.

3. Una firma de Lamport es una esquema de firma seguro para un sólo uso que se puede construir a partir de una función $f : X \to Y$ de una vía. A continuación describimos la generación de claves y el algortimo de firma del esquema de firma de Lamport para firmar un mensaje m consistente en una cadena de v bits, es decir, $m \in \{0,1\}^v$.

   Generación de claves: Para cada $i \in \{0,1\}$ y para cada $j \in \{1, 2, 3, \ldots, v\}$ se genera uniformemente al azar un valor $x_{i,j} \in X$ y se calcula $y_{i,j} = f(x_{i,j}) \in Y$. Se obtienen $2v$ valores en X, que constituyen la clave secreta, y otros $2v$ valores en Y, que constituyen la clave pública. Representados más visualmente, en forma de matriz, tenemos:

$$sk := \begin{pmatrix} x_{0,1} & x_{0,2} & x_{0,3} & \ldots & x_{0,v} \\ x_{1,1} & x_{1,2} & x_{1,3} & \ldots & x_{1,v} \end{pmatrix}$$

$$pk := \begin{pmatrix} y_{0,1} & y_{0,2} & y_{0,3} & \ldots & y_{0,v} \\ y_{1,1} & y_{1,2} & y_{1,3} & \ldots & y_{1,v} \end{pmatrix}$$

   Algoritmo de firma: Dado un mensaje $m = b_1 b_2 \ldots b_v \in \{0,1\}^v$ donde cada b_j es un bit. La firma de m se calcula eligiendo, para cada j, uno de los dos posibles valores $x_{i,j}$ dependiendo del valor del bit b_j, el de la fila superior si $b_j = 0$ y el de la fila inferior si $b_j = 1$. Más formalmente:

$$\sigma = (x_{b_1,1}, x_{b_2,2}, x_{b_3,3}, \ldots, x_{b_v,v}) \in X^v$$

   a) Trata de describir el algoritmo de verificación.

   b) Da una idea informal de por qué el esquema es seguro cuando se utiliza una única vez.

   c) Explica por qué el esquema es completamente inseguro cuando se utiliza varias veces.