TEMA
Criptografía. Conceptos generales.

1. OBJETIVOS Y LOGROS DE LA CRIPTOGRAFÍA

El objetivo de este breve capítulo es introducir un vocabulario básico que se emplea de forma habitual al hablar de criptografía. Pretende presentar, de una forma muy resumida, una visión general de las herramientas criptográficas más habituales y los servicios que ofrece cada una de estas herramientas.

El objetivo principal de la criptografía es el cifrado de la información. Existen también otros objetivos que se derivan en gran parte de esa posibilidad del cifrado. Esos objetivos podemos agruparlos, de forma reducida, en cuatro:

1. **Confidencialidad**. Ocultar la información a todo el mundo excepto a aquellos que estén autorizados para acceder a ella. También se habla, en este sentido, de **Secreto**.
2. **Autenticación**. Es un servicio relacionado con la **identificación**. Dos partes que se ponen en comunicación deben inicialmente identificarse mutuamente. Se debe identificar la entidad que comunica, y se debe autenticar el origen de la información comunicada. Una herramienta es la firma digital. Puede emplearse junto a las claves de acceso, o como alternativa a ellas.
3. **Integridad**. Permite verificar que el mensaje o la información no ha sufrido manipulaciones. Manipulaciones son la sustitución, la eliminación y la inserción. Nuestro sistema ha de ser capaz de detectar una de esas manipulaciones y hacerles frente para restituir la información original.
4. **No repudio**. Evitar que el autor de una información o mensaje pueda negar su autoría o envío.

Lo que la criptografía no puede garantizar ni ofrecer es una seguridad total. Se puede trabajar con técnicas criptográficas, pero seguiremos siendo vulnerables.

La criptografía no lo puede todo. Por ejemplo:

1. No puede proteger los **documentos no encriptados**. Se pueden cifrar mensajes para su envío seguro y almacenarlos en nuestro ordenador sin cifrar.
2. No protege contra el **robo de las claves**. Muchas veces la gestión de claves de los usuarios es muy imprudente. La fortaleza de cualquier sistema se mide en su punto más débil.
3. La criptografía no puede proteger contra **ataques de denegación de servicio**. Quizá un atacante no logre acceder a una determinada información, pero sí quizá logre, por ejemplo, eliminar el archivo cifrado donde estaba la información que el atacante no habrá logrado obtener, pero que a partir de ese momento tampoco nosotros podremos acceder a ella.
4. No puede evitar los estudios de **análisis de tráfico**. Podrá ocultar el contenido de una comunicación, pero no el hecho de que esa comunicación haya existido, ni los participantes de esa comunicación.
5. La criptografía es susceptible de **fraude**. Quizá nuestro programa criptográfico tenga sus trampas fraudulentas.
6. Tampoco protege de una **traición** de alguien que tiene acceso lícito a la información, o de un **error en la gestión** de la información.

Es decir, la criptografía ofrece una ayuda importante a la hora de garantizar la seguridad de nuestra información; pero no hemos logrado un sistema invenciblemente seguro sólo con haber acudido a la criptografía.

Junto con la criptografía, otra herramienta necesaria para lograr una amplia seguridad en la información es el control de accesos.

2. CRIPTOSISTEMAS.

El objetivo principal de la criptografía es el cifrado de la información.

Vamos a ver los elementos y nociones principales necesarios para describir cualquier esquema de cifrado.

Un esquema de cifrado, o CRIPTOSISTEMA es un conjunto $(\mathcal{M},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$, con las siguientes propiedades:

1. $\mathcal{M}$ es un conjunto que llamaremos ESPACIO DE TEXTOS PLANOS. Sus

elementos se llaman TEXTOS PLANOS.

2. $\mathcal{C}$ es un conjunto que llamaremos ESPACIO DE TEXTOS CIFRADOS. Sus elementos se llaman TEXTOS CIFRADOS o CRIPTOGRAMAS.
3. $\mathcal{K}$ es un conjunto que llamaremos ESPACIO DE CLAVES. Sus elementos se llaman CLAVES.
4. $\mathcal{E} = \{E_e : e \in \mathcal{K}\}$ es una familia de funciones $E_e : \mathcal{M} \longrightarrow \mathcal{C}$. Cada clave $e \in \mathcal{K}$ determina de forma única una biyección de $\mathcal{M}$ en $\mathcal{C}$, E_e, que llamamos FUNCIÓN DE CIFRADO o transformación de cifrado. El hecho de que E_e sea una biyección implica que este proceso se puede invertir, y que de cada mensaje plano de $\mathcal{M}$ llegamos a un único mensaje cifrado de $\mathcal{C}$. El proceso que resulta de aplicar la transformación E_e al mensaje $m \in \mathcal{M}$ se llama CIFRADO de m.
5. $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ es una familia de funciones $D_k : \mathcal{C} \longrightarrow \mathcal{M}$. Cada clave $d \in \mathcal{K}$ determina una biyección de $\mathcal{C}$ en $\mathcal{M}$, D_d, que llamamos FUNCIÓN DE DESCIFRADO.
6. Un sistema de cifrado, o criptosistema, consiste en un conjunto $\{E_e : e \in \mathcal{K}\}$ de funciones de cifrado y un correspondiente conjunto $\{D_d : d \in \mathcal{K}\}$ de funciones de descifrado con la propiedad de que para cada $e \in \mathcal{K}$, existe una única clave $d \in \mathcal{K}$ tal que $D_d = E_e^{-1}$, es decir, $D_d\big(E_e(m)\big) = m$, para todo $m \in \mathcal{M}$.

La construcción de un criptosistema requiere pues de la selección de un espacio de mensajes $\mathcal{M}$, un espacio de mensajes cifrados $\mathcal{C}$, un espacio de claves $\mathcal{K}$, un conjunto de funciones de cifrado $\mathcal{E} = \{E_e : e \in \mathcal{K}\}$, y su correspondiente conjunto de funciones de descifrado $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$.

Una característica necesaria y no suficiente para un criptosistema es que su espacio de claves sea lo suficientemente amplio para evitar que una búsqueda exhaustiva por parte de un atacante pueda tener éxito.

Un emisor (por ejemplo Alicia) puede usar un criptosistema para enviar de forma confidencial un mensaje m a un receptor, por ejemplo a Bob. Ella usará la clave de cifrado e. Bob usará la correspondiente clave de descifrado d. Alicia obtendrá el texto cifrado a partir de (1) el texto plano, (2) la transformación elegida y (3) su clave: $c = E_e(m)$, y así lo enviará a Bob. Bob, a su vez, podrá obtener el texto plano inicial con (1) su transformación, (2) su clave y (3) el texto cifrado: $m = D_d(c)$.

Para todo este proceso se asume que no es posible en la práctica descifrar un mensaje si sólo se dispone del texto cifrado y del conocimiento del algoritmo de

cifrado y descifrado.

3. CRIPTOSISTEMAS SIMÉTRICOS Y ASIMÉTRICOS

Si Alicia quiere enviar un mensaje cifrado a Bob, entonces ella usará su clave de cifrado y Bob usará su correspondiente clave de descifrado.

Si en un criptosistema se cumple que la clave de cifrado, e, es siempre igual a la clave de descifrado, d, o bien la clave d es sencilla de deducir a partir del conocimiento de la clave e, entonces a ese criptosistema se le llama SIMÉTRICO. Si Alicia y Bob usan un criptosistema simétrico, ellos deberán intercambiarse sus claves antes de comenzar su comunicación de forma cifrada: el intercambio de las claves de forma segura es la parte más comprometida de un criptosistema simétrico. Nadie debe conocer la clave e, excepto Alicia y Bob, porque de lo contrario, un tercero podrá interceptar el mensaje y descifrarlo para obtener el mensaje plano.

En los criptosistemas ASIMÉTRICOS, las claves e y d son diferentes, y la relación computacional entre ambas imposible de averiguar. En estos sistemas, la clave de cifrado e puede ser pública. Si Bob quiere recibir un mensaje cifrado, basta con que haga pública una clave de cifrado e, y guarde a buen recaudo la clave de descifrado d correspondiente. Cualquiera podrá usar la clave e y enviar un mensaje cifrado a Bob. Por eso, a la clave e se le llama CLAVE PÚBLICA. Y sólo Bob puede descifrar el mensaje cifrado recibido, porque sólo él dispone de la clave de descifrado d: a esa clave se la llama CLAVE PRIVADA. A los criptosistemas asimétricos se les llama también CRIPTOSISTEMAS DE CLAVE PÚBLICA.

4. CRIPTOANÁLISIS

Para hacer aún más difícil un posible ataque de espionaje, se podría pensar en hacer secreto también el criptosistema utilizado en nuestras comunicaciones, y no solamente hacer secretas las claves. Sin embargo, en las comunicaciones por internet, y en las redes públicas, este procedimiento no es viable. Por eso, asumimos siempre que el único secreto en las comunicaciones es el texto plano y

las claves privadas. Se entiende que en un criptosistema simétrico todas las claves son privadas. El criptosistema o esquema de cifrado utilizado en nuestras comunicaciones es siempre de dominio público.

Para determinar la real seguridad de un criptosistema, hemos de saber los medios y habilidades que tiene cualquier potencial atacante.

Un atacante que disponga del texto cifrado, deseará conocer lo máximo posible del contenido del texto plano. Un camino inmediato es averiguar la clave de descifrado. En ese caso, el atacante ha roto nuestra comunicación y todo lo que transmitamos quedará abierto.

Pero un atacante puede pretender averiguar información sobre el texto plano aunque no disponga de la clave de descifrado. Quizá pudiera obtener información parcial. Con frecuencia no se necesita toda la información transmitida, sino simplemente una parte de ella.

Existen los siguientes tipos de ataque (en todos ellos, el atacante conoce el criptosistema al que se enfrenta):

1. **Ciphertext–only attack**: El atacante únicamente conoce un mensaje de texto cifrado. Este es el camino de ataque más débil. Un posible ataque de esta forma es el de **fuerza bruta** o de **búsqueda exhaustiva**: probar con todas las posibles claves del espacio de claves de descifrado. Este es un camino posible si nuestro criptosistema dispone de un espacio de claves reducido, teniendo en cuenta que el concepto “reducido” depende de la potencia de cálculo de que disponga el atacante.
   Otro ataque de esta forma es el ataque estadístico, basado en el conocimiento de las propiedades del lenguaje utilizado en el texto plano.
2. **Known plaintext attack**: El atacante conoce un texto plano y su correspondiente texto cifrado, o varias parejas de estos. El atacante tratará de descifrar otros textos cifrados de los que no conoce su correspondiente texto plano.
3. **Chosen plaintext attack**: Al atacante le es permitido obtener el cifrado de algunos textos planos por él seleccionados, pero sigue sin conocer la clave de cifrado. De nuevo lo que intenta es descifrar algunos textos cifrados obtenidos, de los que desconoce su significado. Desde luego, este método es siempre posible en los criptosistemas de clave pública, porque todo el mundo puede cifrar con la clave pública cualquier mensaje plano. Este ataque puede

ser útil si el **espacio de mensajes planos posibles es reducido**: pueden cifrarse todos ellos y comparar luego resultados.

4. **Chosen Ciphertext attack**: El atacante puede ahora obtener el descifrado de algunos textos cifrados por él elegidos. De esa manera intenta obtener la clave de descifrado.

En general el criterio para decidir que un criptosistema es válido para la comunicación que deseo establecer, o para almacenar cifrada una información cifrada, se basa en dos parámetros:

1. Que el costo económico de romper la cifra exceda al valor de la información cifrada.
2. Que el tiempo requerido para lograr descifrar por ataque la información sea mayor que el tiempo de vida de la información.

Diremos que un criptosistema es computacionalmente seguro si cumple con estos dos criterios enunciados.

5. ALFABETOS Y PALABRAS

Para escribir textos necesitamos un conjunto de símbolos, que llamamos alfabeto. Un ALFABETO es un conjunto no vacío Σ. La LONGITUD de Σ es el número de elementos de Σ. Los elementos de Σ se llaman SÍMBOLOS o LETRAS.

Un alfabeto bastante común es el abecedario:

$\Sigma = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, \tilde{N}, O, P, Q, R, S, T, U, V, X, Y, Z\}$.

En las computadoras (y habitualmente en los algoritmos criptográficos) se usa frecuentemente el alfabeto binario: $\Sigma = \{0,1\}$.

Como los alfabetos son conjuntos finitos, se puede establecer una relación entre sus elementos y los enteros no negativos. Si el alfabeto tiene m elementos, podemos identificarlo con los números $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

Una PALABRA o CADENA sobre Σ es una secuencia finita de símbolos de Σ, incluyendo la cadena vacía, que suele denotarse como ε. La LONGITUD DE UNA PALABRA w sobre Σ es el número de sus componentes, y la denotamos como $|w|$. El conjunto de todas las posibles palabras sobre Σ, incluyendo la cadena vacía, la llamamos Σ^*.

Si $v,w \in \Sigma^*$, entonces $vw = v \circ w$ es una cadena que se obtiene por concatenación de v y w. A esta operación la llamamos concatenación de v y w. En particular, se verifica que $v \circ \varepsilon = \varepsilon \circ v = v$.

Si n es un entero no negativo entonces Σ^n es el conjunto de todas las palabras de longitud n sobre Σ.

6. PERMUTACIONES

Sea $\mathcal{X}$ un conjunto finito de elementos. Diremos que p es una PERMUTACIÓN DE $\mathcal{X}$ si es una aplicación biyectiva de $\mathcal{X}$ sobre sí misma, $p: \mathcal{X} \longrightarrow \mathcal{X}$. Al conjunto de todas las permutaciones de $\mathcal{X}$ lo llamamos $S(\mathcal{X})$.

Supongamos que $\mathcal{X} = \{0,1,2,3,4,5\}$. Un modo de representar una permutación es mediante una matriz de dos filas: en ambas filas están recogidos todos los elementos de $\mathcal{X}$. La fila de abajo indica dónde ha ido a parar cada elemento de la fila de arriba tras la permutación. Por ejemplo:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 & 0 \end{pmatrix}$$

El conjunto $S(\mathcal{X})$ con todas sus permutaciones, junto con la operación composición tiene estructura de grupo. Si $n \geq 0$ es un entero, entonces al grupo formado por todas las permutaciones del conjunto $\{1,2,\dots,n\}$ lo llamamos S_n. El orden del grupo S_n es $n!$

7. CIFRADO DE BLOQUE

Un algoritmo de cifrado de bloque cifra bloques de texto plano de longitud fija en bloques cifrados también de longitud fija.

Un criptosistema se llama de CIFRADO DE BLOQUE si su espacio de texto plano y su espacio de texto cifrado es el conjunto Σ^n de palabras de longitud fija n (n entero positivo) sobre el alfabeto Σ. Es decir, $\mathcal{M} = \mathcal{C} = \Sigma^n$.

Las funciones de cifrado de un algoritmo de cifrado de bloque son **permutaciones**: biyecciones de Σ^n en Σ^n. Por tanto, el espacio de claves de un cifrado de bloque es el de todas las permutaciones de Σ^n: $S(\Sigma^n)$.

La función de cifrado para una determinada clave $\pi \in S(\Sigma^n)$ será, pues, $E_\pi: \Sigma^n \to \Sigma^n: \ v \to \pi(v)$. La correspondiente función de descifrado será $D_\pi: \Sigma^n \to \Sigma^n: \ v \to \pi^{-1}(v)$.

El espacio de claves es muy amplio: contiene $|\Sigma^n|!$ elementos. El esquema de cifrado o criptosistema parece, por tanto, bastante seguro.

8. SUSTITUCIÓN Y TRANSPOSICIÓN

Los cifrados por SUSTITUCIÓN son cifrados de boque que realiza cambio de símbolos o de grupo de símbolos por otros símbolos o grupo de símbolos.

Sea Σ un alfabeto de q elementos o símbolos, y $\mathcal{M}$ el conjunto de todas las cadenas de longitud t sobre Σ. Sea $\mathcal{K}$ el conjunto de todas las permutaciones del conjunto Σ. (Ya hemos dicho que el numero de permutaciones posibles es $q!$, y es un valor independiente del tamaño del bloque de cifrado, t.) Definimos para cada $e \in \mathcal{K}$ una trasformación o función de cifrado E_e tal que $E_e(m) = \big(e(m_1)\, e(m_2) \dots\ e(m_t)\big) = (c_1 c_2 \dots c_t) = c$, donde $m = (m_1 m_2 \dots m_t) \in \mathcal{M}$ (cada m_i y cada c_i es un elemento del alfabeto Σ). En otras palabras, para cada símbolo en una cadena de t símbolos, se sustituye o reemplaza éste por otro símbolo de Σ de acuerdo con una permutación fija e.

Para descifrar $c = (c_1 c_2 \dots c_t)$ se computa la permutación inversa $d = e^{-1}$ y se aplica la transformación de descifrado correspondiente: $D_d(c) = \big(d(c_1) d(c_2) \dots d(c_t)\big) = (m_1 m_2 \dots m_t) = m$.

La transformación E_e se llama CIFRADO DE SUSTITUCIÓN SIMPLE o CIFRADO DE SUSTITUCIÓN MONOALFABÉTICA.

También se puede definir el CIFRADO DE SUSTITUCIÓN POLIALFABÉTICA, que es un cifrado de bloque, con bloques de longitud t sobre un alfabeto Σ, y que tiene las siguientes propiedades:

1. El espacio de claves $\mathcal{K}$ consiste en todos los conjuntos ordenados de t permutaciones $(p_1, p_2, \dots, p_t)$ donde cada permutación p_i está definida en el conjunto Σ.
2. El cifrado del mensaje $m = (m_1 m_2 \dots m_t)$ bajo a clave $e = (p_1, p_2, \dots, p_t)$ viene dado por la transformación $E_e(m) = (p_1(m_1) p_2(m_2) \dots p_t(m_t))$; y
3. La clave de descifrado asociada a $e = (p_1, p_2, \dots, p_t)$ es $d = (p_1^{-1}, p_2^{-1}, \dots, p_t^{-1})$

Los cifrados por TRANSPOSICIÓN son otra clase de cifrado simétrico, que simplemente permuta los símbolos de cada bloque.

Supongamos un criptosistema de clave simétrica, de cifrado por bloques con bloques de longitud t. Sea $\mathcal{K}$ el conjunto de todas las permutaciones en el conjunto $\{1, 2, \dots, t\}$. Para cada $e \in \mathcal{K}$ definimos la función de cifrado $E_e(m) = (m_{e(1)} m_{e(2)} m_{e(t)})$, donde $m = (m_1 m_2 \dots m_t) \in \mathcal{M}$. Al conjunto de todas las transformaciones definidas de esta forma lo llamamos CIFRADO DE TRASPOSICIÓN SIMPLE. La clave de descifrado correspondiente a la de cifrado e es $d = e^{-1}$. Para descifrar $c = (c_1 c_2 \dots c_t)$ computamos $D_d(c) = (c_{d(1)} c_{d(2)} c_{d(t)})$.

Los cifrados de trasposición simple preserva el número de símbolos de un tipo dado dentro del bloque, y por eso es fácilmente criptoanalizable.

9. COMPOSICIÓN DE CIFRADOS

La composición es un camino conveniente para construir funciones más complicadas a partir de otras más simples.

Sean $\mathcal{S}$, $\mathcal{T}$ y $\mathcal{U}$ conjuntos finitos, y sean las funciones $f: \mathcal{S} \rightarrow \mathcal{T}$ y $g: \mathcal{T} \rightarrow \mathcal{U}$. La COMPOSICIÓN de g con f, que se escribe como $g \circ f$ (o simplemente gf), es una función de $\mathcal{S}$ en $\mathcal{U}$, y definida como $g \circ f(x) = g(f(x))$, para todo $x \in \mathcal{S}$.

La composición es fácilmente extendible para más de dos funciones. Para las funciones $f_1, f_2, \dots, f_t$, se puede definir $f_t \circ \dots \circ f_2 \circ f_1$, siempre que el dominio inicial de f_t sea el mismo que el dominio final de f_{t-1}, y así con todos.

Los cifrados de simple sustitución y de transposición, individualmente, no ofrecen un alto nivel de seguridad. Sin embargo, combinando estas transformaciones sí es posible lograr una transformación de cifrado fuerte. Llamamos CIFRADO PRODUCTO a una composición de $t \geq 2$ transformaciones $E_{k_1}, E_{k_2}, \dots, E_{k_t}$, donde cada E_{k_i}, $1 \leq i \leq t$ o es una cifra de sustitución, o es una cifra de transposición.

Llamamos ROUND, o VUELTA a la composición de una transposición y una sustitución.

10. CIFRADO DE FLUJO

Ya hemos visto cómo emplear el cifrado de bloque para cifrar un texto plano de longitud arbitraria. También los cifrados de flujo permiten cifrar textos planos de cualquier longitud, pero ahora la construcción del algoritmo es diferente.

Los cifrados de flujo forman una clase importante dentro de los cifrados simétricos. Por una parte pueden considerarse como cifrados de bloque en el que la longitud del bloque se toma igual a la unidad ($n = 1$). Lo que hace que esta singularidad sea útil es el hecho de que la función de cifrado puede cambiar cada vez que un símbolo del texto plano queda cifrado.

En situaciones donde los errores de transmisión son altamente probables, los cifrados de flujo ofrecen una ventaja porque no tienen errores de propagación. Otras circunstancias donde este tipo de criptosistema es útil es cuando los datos deben ser procesados en un símbolo cada vez.

Sea $\mathcal{K}$ el espacio de claves para un conjunto de transformaciones o funciones de cifrado. Llamamos clave de la cadena a una secuencia de símbolos $e_1 e_2 e_3 \dots e_i \in \mathcal{K}$.

Sea Σ un alfabeto de q elementos, y sea E_e una función de cifrado por sustitución de longitud 1, donde $e \in \mathcal{K}$. Sea $m_1 m_2 m_3 \dots$ una cadena de texto plano, y sea $e_1 e_2 e_3 \dots$ una clave de flujo de $\mathcal{K}$. Un cifrado de flujo toma la cadena de texto plano y produce una cadena de texto cifrado $c_1 c_2 c_3 \dots$, donde $c_i = E_{e_i}(m_i)$. Si d_i es la clave inversa a e_i, entonces $D_{d_i}(c_i) = m_i$ descifra la cadena de texto cifrado.

11. FIRMA DIGITAL

Una herramienta fundamental para la autenticación, la autorización y el no repudio es la firma digital. Su propósito es proveer un medio para que una entidad vincule su identidad a un trozo de información. El proceso de firmado supone transformar el mensaje y alguna información secreta que posee la entidad en una etiqueta, llamada firma.

Sea $\mathcal{M}$ el conjunto de mensajes que pueden ser firmados. Sea $\mathcal{S}$ un conjunto de elementos llamados FIRMAS. Habitualmente serán cadenas binarias de longitud fija: eso se entenderá mejor cuando se haya llegado a la explicación de las funciones hash.

$\mathcal{S}_A$ es una transformación que va desde el conjunto de mensajes $\mathcal{M}$ al conjunto de firmas $\mathcal{S}$, y se llama TRASNFORMACIÓN DE FIRMA para la entidad A. La

transformación $\mathcal{S}_A$ es algo que A debe mantener en secreto, y será usada para crear las firmas para los mensajes de $\mathcal{M}$.

V_A es una transformación que va desde el conjunto $\mathcal{M} \times \mathcal{S}$ al conjunto $\{true, false\}$. La transformación V_A se llama TRANSFORMACIÓN DE VERIFICACIÓN para las firmas de A; es públicamente conocida, y la emplean todas las entidades que quieran verificar las firmas creadas por A.

Ambas transformaciones $\mathcal{S}_A$ y V_A forman el criptosistema de firma digital.

Un ejemplo (muy simple) podría ser el siguiente: $\mathcal{M} = \{m_1, m_2, m_3\}$, y $\mathcal{S} = \{s_1, s_2, s_3\}$. En la figura 1 se recoge la función de firmado $\mathcal{S}_A$ y la función de verificación V_A.

El procedimiento para la firma es el siguiente. La entidad A firmante crea una firma para el mensaje $m \in \mathcal{M}$ realizando los siguientes pasos:

1. Computo de $s = \mathcal{S}_A(m)$.
2. Transmisión del par (m, s). s es la firma del mensaje m.

El procedimiento para la verificación es el siguiente: La entidad B, receptora del mensaje m y de la firma s creada por A, realiza los siguientes pasos:

1. Solicita a A la función de verificación V_A.
2. Computa $u = V_A(m, s)$.
3. Aceptará la firma que le ha entregado A si se verifica que $u = true$, y la rechazará si $u = false$.

Lo normal es que los algoritmos de firma y verificación sean públicamente conocidos: existe una clase de algoritmos de firma y verificación, y cada algoritmo dentro de la clase se caracteriza por una clave. Así, el algoritmo $\mathcal{S}_A$ de firmado vendrá determinado por la clave k_A, y A únicamente debe mantener el

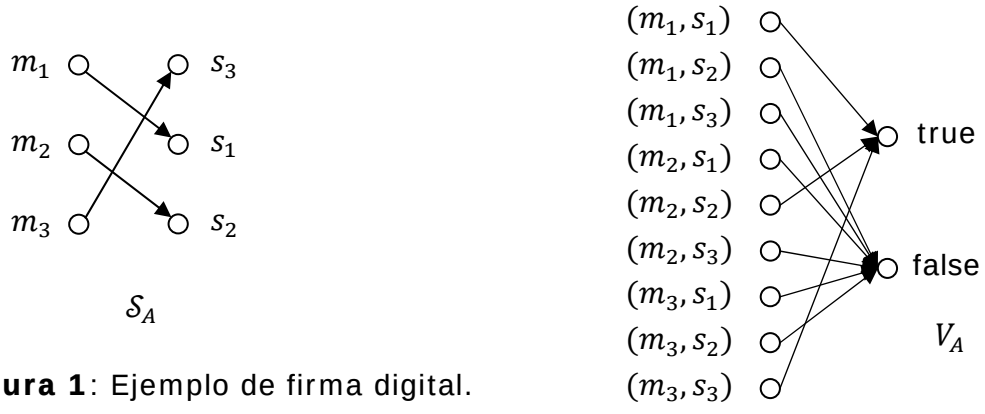

Figura 1: Ejemplo de firma digital.

secreto de esa clave. De igual manera, la verificación V_A de A puede depender de una clave l_A, que además puede hacerse pública.

Una firma manual como las que conocemos de siempre puede ser interpretada como una clase de firma digital: tomamos el conjunto $\mathcal{S}$ de firmas que contiene un solo elemento que es la firma manuscrita de A, y que denotamos s_A. Sea cual sea el mensaje a firmar, el resultado de $S_A(m) = s_A$, para todo $m \in \mathcal{M}$. La función de verificación chequea si la firma recibida junto al mensaje m es, efectivamente, s_A.

Como se ve, una diferencia capital entre el proceso de firmado tradicional y el proceso de firmado digital es que en el tradicional la firma obtenida depende siempre y únicamente del firmante y no de lo que se firma; en el criptosistema de firma digital, la firma obtenida depende tanto de la clave de firmado que tenga el firmante como del mensaje a firmar.

Hay dos propiedades exigibles a cualquier criptosistema de firma digital:

1. s será una firma válida de A para el mensaje m si y sólo si $V_A(m,s) = true$.
2. Debe ser computacionalmente imposible para cualquier entidad distinta de A encontrar, para cada $m \in \mathcal{M}$, un $s \in \mathcal{S}$ tal que $V_A(m,s) = true$.

La clave pública ofrece una vía muy eficaz para lograr firmas digitales. Supongamos E_e una transformación de cifrado de clave pública, con su espacio de mensajes planos $\mathcal{M}$ y su espacio de mensajes cifrados $\mathcal{C}$. Supongamos además que $\mathcal{M} = \mathcal{C}$. Si D_d es la transformación de descifrado correspondiente a E_e, entonces tendremos que E_e y D_d son permutaciones, y tenemos además que $D_d\big(E_e(m)\big) = E_e\big(D_d(m)\big) = m$, para todo $m \in \mathcal{M}$.

Un criptosistema de clave pública de este tipo se llama REVERSIBLE. Desde luego es esencial que $\mathcal{M} = \mathcal{C}$ para que esta expresión sea válida para todo $m \in \mathcal{M}$. De lo contrario la expresión $D_d(m)$ carece de sentido para $m \notin \mathcal{C}$.

Para construir una firma digital, el esquema es el siguiente:

1. Sea $\mathcal{M}$ el espacio de mensajes para el criptosistema de firma.
2. Sea $\mathcal{C} = \mathcal{M}$, el espacio de firma $\mathcal{S}$.
3. Sea (e,d) el par de claves del criptosistema de clave pública.
4. Definimos la función de firmado S_A que sea D_d. Esto es, la firma del mensaje $m \in \mathcal{M}$ es $s = D_d(m)$.
5. Definimos la función de verificación, V_A como:

$$V_A(m,s) = \begin{cases} verdadero, si\ E_e(s) = m \\ falso, en\ otro\ caso \end{cases}$$

12. FUNCIONES HASH

Uno de los elementos más importantes de la criptografía moderna son las funciones hash, llamadas también de forma habitual funciones hash de una vía.

Un FUNCIÓN HASH es una función computacionalmente eficiente que transforman cadenas binarias de longitud arbitraria en otras cadenas binarias de longitud fija. A estas cadenas de longitud fija las llamamos VALORES HASH.

Para una función hash de valores hash de longitud n (por ejemplo, valores típicos $n = 128$, ó $n = 160$) y una serie de propiedades deseables (que ya veremos más adelante) la probabilidad de que una cadena tomada aleatoriamente tenga una imagen en la función hash de predeterminada es 2^{-n}.

El objetivo básico de las funciones hash es que los valores hash sirvan como un valor compacto representativo de una cadena de entrada. Se habla de que la función hash ofrece un "resumen" de la cadena de entrada. Para su uso criptográfico, una función hash h se toma de forma que sea computacionalmente imposible encontrar dos cadenas de entrada distintas con un valor hash común (imposible encontrar intencionalmente dos cadenas x e y tales que $h(x) = h(y)$). También se exige que dado el valor hash y, es computacionalmente imposible encontrar una cadena x tal que $h(x) = y$.

Los usos más habituales de las funciones hash en criptografía son los siguientes:

1. Como una herramienta de uso conjunto con la firma digital. A la hora de firmar, habitualmente no se firma el mensaje o el documento entero, sino únicamente un resumen de él, obtenido mediante una función hash. El receptor del mensaje completo puede aplicar al mensaje recibido la misma función hash y verificar si la firma recibida se corresponde con el resumen o valor hash obtenido.
2. Como medio para garantizar integridad de la información. En un momento determinado se obtiene el resumen o valor hash de un documento. Si más adelante se vuelve a calcular el valor hash del documento y éste no coincide con el valor hash previo, entonces es inmediato deducir que el documento ha

sido modificado.

13. VENTAJAS E INCONVENIENTES DE LOS CRIPTOSISTEMAS SIMÉTRICO Y ASIMÉTRICO

Ambas tipos de criptosistemas gozan de sus respectivas ventajas y adolecen de sus respectivos defectos. Resumidamente, recogemos unas y otras para cada uno de los dos grupos de criptosistemas. Más adelante, al terminar la presentación de todos los conceptos de este capítulo, la lectura de estas listas de ventajas y desventajas será más clara.

Ventajas de los criptosistemas simétricos.

1. Alta velocidad de transformación, especialmente en implementaciones hardware.
2. Las claves simétricas son relativamente cortas.
3. Se emplean para muchas aplicaciones criptográficas.
4. El cifrado simétrico es fácilmente componible para producir cifrados más robustos.
5. Tiene ya una larga historia ampliamente conocida, comenzando por las máquinas de rotor, entre las que se encuentra la máquina enigma. Con la llegada de las computadores digitales se han desarrollado muchos algoritmos, entre los que destaca, en particular, el algoritmo DES.

Desventajas de los criptosistemas simétricos.

1. En una comunicación de dos partes, la clave debe permanecer secreta en ambos extremos.
2. En una red amplia de comunicantes se requiere gestionar un alto número de claves.
3. En la práctica está recomendado que en una comunicación a dos partes la clave de cifrado y descifrado se cambie con frecuencia, incluso dentro de la misma comunicación.

Ventajas de los criptosistemas asimétricos.

1. Sólo se ha de mantener oculta una de las dos claves.
2. En una red amplia de comunicantes el número de claves requeridas es sensiblemente menor que en el caso del uso de criptosistema simétricos.

3. Las claves pueden usarse y ser válidas en periodos largos y en diferentes comunicaciones.
4. Muchas claves públicas ofrecen medios para la fira digital.

Desventajas de los criptosistemas asimétricos.

1. La velocidad de cifrado es mucho menor que en el cifrado simétrico.
2. El tamaño de las claves es sensiblemente mayor que en el cifrado simétrico.
3. Los criptosistemas de clave pública deben su seguridad a la presumible dificultad de resolver un pequeño grupo de problemas de la teoría de números.
4. Su historia es mucho más reciente que la del cifrado simétrico.

Resumen y comparación.

El cifrado simétrico y el asimétrico tienen ventajas complementarias. Actualmente las técnicas criptográficas procuran aprovechar los beneficios de cada una de ellas.

En la práctica el uso de ambos sistemas es el siguiente:

1. La criptografía de clave pública facilita herramientas para la firma digital (particularmente útiles para evitar el no repudio) y para la gestión e intercambio de claves simétricas.
2. La criptografía de clave simétrica es eficiente para el cifrado de la información y para algunas aplicaciones de integridad de la información.

REFERENCIAS

[1] "Handbook of Applied Cryptography". A. Menezes, P. van Oorschot, and S. Vanstone. CRC Press, Inc. 1997.

[2] "Cryptography and Network Security. Principles and practices". William Stallings. Prentice Hall. Pearson Education. Third edition. 2003.

[3] "Introduction to Cryptography". Johannes A. Buchmann. Springer Verlag, 2004. Second Edition.