Cátedra No. 2 : 7 de Agosto

Transcriptor: Marcos Kiwi

1 Cifrados de Chorro

En los criptosistemas que hemos estudiado hasta ahora, hemos encriptado el texto plano utilizando la misma clave K de forma que el texto cifrado $y = y_1y_2\ldots = e_K(x_1)e_K(x_2)\ldots$. Los criptosistemas que se obtienen utilizando esta forma de encriptar se conocen como *cifrados en bloque*.[1] En este curso nos remitiremos principalmente al estudio de este tipo de criptosistemas. Sin embargo hay otras alternativas. Por completitud discutiremos una de ellas en esta sección, los *cifrados de chorro*.[2]

La idea básica de este tipo de cifrados es generar una secuencia de claves $K = z_1z_2\ldots$, y usarla para encriptar el texto plano $x = x_1x_2\ldots$, como sigue:

$$y \;=\; y_1y_2\ldots \;=\; e_{z_1}(x_1)e_{z_2}(x_2)\ldots$$

Formalmente,

Definición 1 *Un cifrado de chorro es una tupla $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{L},\mathcal{F},\mathcal{E},\mathcal{D})$ tal que:*

- *$\mathcal{P}$ es un conjunto de posibles textos planos.*
- *$\mathcal{C}$ es un conjunto de posibles textos cifrados.*
- *$\mathcal{K}$ es un conjunto de posibles claves.*
- *$\mathcal{L}$ es un conjunto denominado alfabeto de claves de chorro.*
- *$\mathcal{F} = (f_1, f_2, \ldots)$ es tal que $\forall\, i \geq 1,\ f_i\colon\ \mathcal{K}\times\mathcal{P}^{i-1} \to \mathcal{L}$.*
- *Para cada $z \in \mathcal{L}$, hay una* función de encripción *$e_z \in \mathcal{E}$ y una correspondiente* función de decripción *$d_z \in \mathcal{D}$, donde $e_z\colon\ \mathcal{P}\to\mathcal{C}$, $d_z\colon\ \mathcal{C}\to\mathcal{P}$ y $d_z(e_z(x)) = x$, cualquiera sea $x \in \mathcal{P}$.*

---

[1] *Block chiphers.*
[2] *Stream ciphers.*

A continuación discutimos la forma en que Alicia y Roberto emplean un criptosistema como el anterior. Primero eligen una clave $K \in \mathcal{K}$ (cuando no pueden ser observados por Eva). Más tarde, cuando Alicia quiere enviar a Roberto el texto plano $x = x_1 x_2 \ldots$, $x_i \in \mathcal{P}$, $i = 1, 2, \ldots$, esta determina $z_i = f_i(K, x_1, \ldots, x_{i-1})$, y envía $y_i = e_{z_i}(x_i)$. En general, Alicia determinará $z_1, y_1, z_2, y_2, \ldots$ secuencialmente. (Es importante notar, que la encripción de x_i depende no sólo de K sino que también de $x_1 x_2 \ldots x_{i-1}$.) Una vez que Roberto recibe el texto cifrado $y = y_1 y_2 \ldots$, este obtiene el texto plano calculando secuencialmente $z_1, x_1, z_2, x_2, \ldots$ determinando primero $z_i = f_i(K, x_1, \ldots, x_{i-1})$ y luego $x_i = d_{z_i}(y_i)$.

Claramente, los cifrados en bloque son un caso especial de los cifrados de chorro donde $z_i = K$, para todo $i \geq 1$.

La utilidad de los cifrados de chorro radica en que usualmente se pueden implementar a nivel de hardware en forma muy eficiente.

Veamos un ejemplo de este tipo de cifrados. Consideremos $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathcal{Z}_2$ y $\mathcal{K} = (\mathcal{Z}_2)^m \setminus \{(0, \ldots, 0)\}$. Supongamos que comenzamos con $K = (z_1, \ldots, z_m) \in \mathcal{K}$ y hacemos que

$$z_{i+m} = (\sum_{j=0}^{m-1} c_j \, z_{i+j}) \bmod 2 \,,$$

donde $c_0, \ldots, c_{m-1} \in \mathcal{Z}_2$ estan fijos. Finalmente hacemos

$$\begin{aligned} e_z(x) &= (x + z) \bmod 2 \,, \\ d_z(y) &= (y - z) \bmod 2 \,. \end{aligned}$$

Más adelante en el curso, cuando estudiemos DES (*Data Encryption Standard*), veremos otros ejemplos del tipo de encripción discutido en esta sección.

2 Divisibilidad y el Algoritmo de Euclides

En esta sección recordaremos algunas definiciones y repasaremos algunos resultados que conciernen a los números enteros.

Dados dos enteros a y b decimos que *a divide a b*, o *b es divisible por a*, y escribimos $a|b$ si existe un entero k tal que $b = ak$. En este caso decimos que a es un divisor de b. Si a no es un divisor de b escribimos $a \not| b$.

Se tienen las siguientes propiedades:

- Si $a|b$ y c es un entero, entonces $a|b\,c$.
- Si $a|b$ y $b|c$, entonces $a|c$.
- Si $a|b$ y $a|c$, entonces $a|(b \pm c)$.

Cada entero mayor que 1 tiene al menos dos divisores; 1 y b. Un divisor no trivial de b es un divisor de b distinto a 1 y a b. Un número *primo* es, por definición, un número mayor que 1 que no tiene divisores no triviales. Un número es *compuesto* si es mayor que 1 y tiene al menos un divisor no trivial.

Por el Teorema Fundamental de la Aritmética se tiene que cualquier número entero positivo se puede expresar de manera única (salvo el orden de los factores) como un producto de primos. Dos consecuencias de este importante teorema son:

- Si p es primo y $p|(ab)$, entonces $p|a$ o $p|b$.
- Si $m|a$ y $n|a$, y m, n no tienen divisores comunes mayores que 1, entonces $(mn)|a$.

El *maximo común divisor* de dos enteros a y b no ambos nulos, se denota por $\mathrm{mcd}(a,b)$, y es el mayor entero d tal que $d|a$ y $d|b$. Equivalentemente, $d = \mathrm{mcd}(a,b)$ si cualquiera sea el entero positivo c tal que $c|a$ y $c|b$ se tiene que $c|d$.

El *minimo común multiplo* de dos enteros no nulos a y b, denotado $\mathrm{mcm}(a,b)$, es el menor entero positivo divisible por a y b. No es dificil probar que $\mathrm{mcm}(a,b) = |a\,b|/\mathrm{mcd}(a,b)$.

Si se conoce la factorización de a y b es relativamente simple calcular $\mathrm{mcd}(a,b)$ y $\mathrm{mcm}(a,b)$. Si a y b son grandes lo más probable es que no conozcamos su factorización. A continuación veremos un algoritmo eficiente para calcular el máximo común divisor de dos números desconocida su factorización.

2.1 Algoritmo de Euclides

Sean a y b dos enteros no ambos nulos, $a > b$, y sea $r_0 = a$, $r_1 = b$. El algoritmo de Euclides consiste en calcular

$$\begin{aligned} r_0 &= q_1\, r_1 + r_2\,, \qquad 0 < r_2 < r_1 \\ r_1 &= q_2\, r_2 + r_3\,, \qquad 0 < r_3 < r_2 \end{aligned}$$

$$\begin{aligned}
&\vdots \\
r_{m-2} &= q_{m-1}\, r_{m-1} + r_m\,, \qquad 0 < r_m < r_{m-1} \\
r_{m-1} &= q_m\, r_m\,.
\end{aligned}$$

En cursos anteriores se demuestra que $r_m = \mathrm{mcd}(a, b)$.

Ejercicio 1 *El objetivo de este ejercicio es encontrar una cota para el número de divisiones que requiere el algoritmo de Euclides.*
(i) Pruebe que si $a > b > 0$, y al algoritmo de Euclides le toma k divisiones encontrar $\mathrm{mcd}(a, b)$ entonces $a \geq f_{k+2}$ (donde f_n es el n-ésimo número de Fibonacci, i.e. $f_1 = 1$, $f_2 = 1$, $f_{n+1} = f_n + f_{n-1}$ para todo $n \geq 2$.)
(ii) Pruebe que

$$f_n = \frac{1}{\sqrt{5}}\,(\phi^n - \varphi^n)\,, \qquad \text{donde } \phi = \frac{1}{\sqrt{2}}\,(1+\sqrt{5})\,, \quad \varphi = \frac{1}{\sqrt{2}}\,(1-\sqrt{5})\,.$$

Luego, para n suficientemente grande f_n es el entero más cercano a $\phi^n/\sqrt{5}$.

Sigue que el número de iteraciones, k, que le toma al algoritmo de Euclides determinar $\mathrm{mcd}(a, b)$, donde $a > b$, es tal que $a \geq \phi^{k+2}/\sqrt{5} - 1$ (si k es suficientemente grande como para que $|\varphi|^{k+2}/\sqrt{5} < 1$), i.e. $k = O(\log a)$.

Proposición 1 *Sea $d = \mathrm{mcd}(a, b)$, Entonces, existen enteros u y v tales que $d = u\,a + v\,b$. Los valores u y v se puden determinar en el tiempo que toma calcular el máximo común divisor de a y b mediante el algoritmo de Euclides.*

Dem: Observar que re-ordenando las igualdades del algoritmo de Euclides obtenemos que

$$\begin{aligned}
d &= r_{m-2} - q_{m-1}\, r_{m-1}\,, \\
r_{m-1} &= r_{m-3} - q_{m-2}\, r_{m-2}\,, \\
&\vdots \\
r_3 &= r_1 - q_2\, r_2\,, \\
r_2 &= r_0 - q_1\, r_1\,.
\end{aligned}$$

Recordando que $r_0 = a$ y $r_1 = b$ las identidades anteriores proveen una forma de expresar d como una combinación lineal de a y b, puesto que cada r_i, $i \in \{2, \ldots, m-1\}$, es una combinación lineal de r_{i-1} y r_{i-2}. $\square$

Decimos que dos enteros a y b son *primos relativos* si $\mathrm{mcd}(a, b) = 1$, i.e. si no tienen divisores comunes mayores que 1.

Corolario 1 *Si a y b son primos relativos, entonces existen enteros u y v tales que $1 = u\,a + v\,b$.*

3 Congruencias

En esta sección repasaremos algunos resultados básicos que conciernen a las congruencias.

Dados tres enteros a, b y m, decimos que *a es congruente a b módulo m*, y escribimos $a \equiv b \pmod{b}$, si $m|(a-b)$. Se puede verificar que congruencia módulo m es una relación de equivalencia.

Sea $\mathcal{Z}_m$ el conjunto $\{0, \ldots, m-1\}$ dotado de dos leyes de composición interna: suma $(+)$ y multiplicación $(\cdot)$, donde la suma y multiplicación son exactamente iguales a la suma y multiplicación de enteros pero donde los resultados son reducidos módulo m. Se verifica que $\mathcal{Z}_m$ así definido forma un anillo conmutativo con unidad.

A continuación enumeramos algunas propiedades de las congruencias.

- Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a \pm c \equiv b \pm d \pmod{m}$ y $ac \equiv bd \pmod{m}$.
- Si $a \equiv b \pmod{m}$ entonces $a \equiv b \pmod{d}$ para cualquier divisor d de m.
- Si $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$ y m, n son relativamente primos, entonces $a \equiv b \pmod{mn}$.

Proposición 2 *Los elementos de $\mathcal{Z}_m$ que tienen inversos multiplicativos son aquellos que son relativamente primos a m. De hecho, de existir el inverso de $a \in \mathcal{Z}_m$ este se puede calcular en el tiempo que toma el algoritmo de Euclides en determinar $\mathrm{mcd}(a, m)$.*

Dem: Si $a \in \mathcal{Z}_m$ no es relativamente primo a m entonces $d = \mathrm{mcd}(a, m) > 1$. Supongamos que existe un $b \in \mathcal{Z}_m$ tal que $ab \equiv 1 \pmod{m}$. Luego $ab - 1$ es divisible por d, pero $d|a$, por lo tanto concluimos que 1 es divisible por d, contradicción.

Si $a \in \mathcal{Z}_m$ es relativamente primo a m entonces por el Corolario 1 existen enteros u y v tales que $1 = au + mv$. Eligiendo $b = u$, sigue que $m|(1 - ab)$, i.e. $ab \equiv 1 \pmod{m}$. Luego, $b \bmod m \in \mathcal{Z}_m$ es inverso multiplicativo de a. □

Corolario 2 *La ecuación $ax \equiv b \pmod{m}$ en la indeterminada x tiene solución en $\mathcal{Z}_m$ si a y m son primos relativos y el tiempo que toma calcular sus soluciones esta dominado por el tiempo que toma encontrar inversos en $\mathcal{Z}_m$. Si $d = \mathrm{mcd}(a, m) > 1$ entonces $ax \equiv b \pmod{m}$ tiene solución en $\mathcal{Z}_m$ ssi $d|b$ y sus soluciones son las mismas que las de la ecuación $a'x \equiv b' \pmod{m'}$ donde $a' = a/d$, $b' = b/d$ y $m' = m/d$.*

Dem: Claramente la solución en $\mathcal{Z}_m$ de la ecuación $ax \equiv b \pmod{m}$ es $x = a^{-1}b \bmod m$ donde a es el inverso multiplicativo de $a \in \mathcal{Z}_m$ que existe puesto que a y m son primos relativos y por la Proposición 2.

Si x es solución de $ax \equiv b \pmod{m}$ y $d = \mathrm{mcd}(a, b)$ entonces $ax \equiv b \pmod{d}$. Luego $d|(ax - b)$. Pero como además $d|a$ se concluye que $d|b$. Por otro lado, $ax \equiv b \pmod{m}$ implica que $ax = b + km$ para algń entero k. Luego, $a'x = b' - km'$, i.e. $a'x \equiv b' \pmod{m'}$. En el sentido inverso, tenemos que si $d|b$ entonces b' es un entero y como a' y m' son primos relativos existe un x solución de $a'x \equiv b' \pmod{m'}$. Luego, $a'x = b' - km'$ para algún entero k. Sigue que $ax = b - km$, i.e. $ax \equiv b \pmod{m}$. □