MA-53G Intr. a la Criptografía	**Semestre Otoño, 1998**

Cátedra No. 6 : 31 de Marzo

Transcriptor: Héctor López Moraga

[Continuación de Seguridad Incondicional]

Proposición 1 *Sea $C = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, con $\mathcal{K} = \bigcup_{m \in \mathcal{I}_C} \mathcal{K}_m$, un criptosistema incondicionalmente seguro. Entonces, si $P_X[x] > 0$ $(\forall x \in \mathcal{P}_m)$ y $P_Y[y] > 0$ $(\forall y \in \mathcal{C}_m)$ se cumple que $|\mathcal{C}_m| \leq |\mathcal{K}_m|$.*

Dem: Fijemos $x \in \mathcal{P}_m$. Si $P_Y[y/X = x] = P_Y[y] > 0$, entonces $(\forall y \in \mathcal{C}_m)$ $(\exists K \in \mathcal{K}_m)$ tal que $e_K(x) = y$. Luego la aplicación que va de $\mathcal{K}_m \longrightarrow \mathcal{C}_m$ y que a cada K le asocia $e_K(x)$ es sobreyectiva, y por lo tanto se cumple que $|\mathcal{C}_m| \leq |\mathcal{K}_m|$ $\square$

Observación 1 *Notemos el hecho importante que si las funciones de encripción no son ambiguas, entonces debe cumplirse que $|\mathcal{P}_m| \leq |\mathcal{C}_m|$.*

Lema 1 *Sea $C = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, con $\mathcal{K} = \bigcup_{m \in \mathcal{I}_C} \mathcal{K}_m$, un criptosistema donde $|\mathcal{K}_m| = |\mathcal{C}_m| = |\mathcal{P}_m|$. Entonces el criptosistema provee seguridad incondicional si y solo si cada clave es usada con probabilidad igual a $\frac{1}{|\mathcal{K}_m|}$, y para cada $x \in \mathcal{P}$ e $y \in \mathcal{C}$, hay una única clave K tal que $e_K(x) = y$.*

Dem:

$(\Rightarrow)$

Supongamos que el criptosistema dado provee seguridad incondicional. Entonces por la proposición anterior para cada $x \in \mathcal{P}_m$ e $y \in \mathcal{C}_m$ debe haber al menos una clave K tal que $e_K(x) = y$. Así, obtenemos que

$$\begin{aligned} |\mathcal{C}| &= |\{e_K(x) : K \in \mathcal{K}_m\}| \\ &\leq |\mathcal{K}_m| \end{aligned}$$

Pero estamos asumiendo que $|\mathcal{C}_m| = |\mathcal{K}_m|$. De aquí, debe cumplirse que

$$\{e_K(x) : K \in \mathcal{K}_m\}| = |\mathcal{K}_m|$$

Esto es, no existen dos claves K_1 y K_2, distintas, tal que $e_{K_1}(x) = e_{K_2}(x) = y$. De aquí, hemos mostrado que para algún $x \in \mathcal{P}_m$ e $y \in \mathcal{C}_m$, hay exactamente una clave K tal que $e_K(x) = y$.

Denotando $n = |\mathcal{K}_m|$, sea $\mathcal{P}_m = \{x_i : 1 \leq i \leq n\}$ y fijemos un $y \in \mathcal{C}_m$. Podemos nombrar las claves $K_1, K_2, ..., K_n$ de la forma $e_{K_i}(x_i) = y$ para $1 \leq i \leq n$.

Usando el teorema de Bayes, tenemos que

$$\begin{aligned} P_X(x_i/y) &= \frac{P_Y(y/x_i)P_X(x_i)}{P_Y(y)} \\ &= \frac{P_K(K_i)P_X(x_i)}{P_Y(y)} \end{aligned}$$

Consideramos la condición de seguridad incondicional $P_X(x_i/y) = P_X(x_i)$. De esto sigue que $P_K(K_i) = P_Y(y)$, para $1 \leq i \leq n$. Esto dice que las claves K_i son equiprobables, pero ya que el núnero de claves es $|\mathcal{K}_m|$ tenemos que $P_K(K) = \frac{1}{|\mathcal{K}_m|}$ para todo $K \in \mathcal{K}_m$.

($\Leftarrow$)

La otra parte de la demostración se deja propuesta. Es fácil ver, con las dos condiciones de hipótesis, que un criptosistema que las cumple debe ser incondicionalmente seguro. $\square$

1 Criptosistemas Productos

Shannon [1949] introdujo la idea de iterar un criptosistema con la esperanza que esto condujese a criptosistemas más difíciles de quebrar. Esta idea a afectado el diseño de criptosistemas en uso actualmente, como *DES*.

Definición 1 (Criptosistema Producto) *Sean $C_i = (\mathcal{K}_i, \mathcal{E}_i, \mathcal{D}_i)$ con $i = 0, 1$ dos criptosistemas tales que $\exists \mathcal{I}_{C_0}, \mathcal{I}_{C_1} \subseteq N$ y una función $\varphi : \mathcal{I}_{C_0} \longrightarrow \mathcal{I}_{C_1}$ donde además* *(i)* $\mathcal{K}_i = \bigcup_{m \in \mathcal{I}_{C_i}} \mathcal{K}_{m,i}$, $i \in \{0,1\}$

(ii) $\forall K \in \mathcal{K}_i$, $Dom(e_K) = \mathcal{P}_{m,i}$, $Rec(e_K) = \mathcal{C}_{m,i}$ $i \in \{0,1\}$.

(iii) $\forall m_0 \in \mathcal{I}_{C_0}$, *si* $m_1 = \varphi(m_0) \Longrightarrow \mathcal{C}_{m_0,0} = \mathcal{P}_{m_1,1}$

Se define el criptosistema producto *como la tupla*

$$C \times C' = (\mathcal{K}, \mathcal{E}, \mathcal{D})$$

donde

$$\mathcal{K} = \bigcup_{m \in \mathcal{I}_C} \mathcal{K}_{m,0} \times \mathcal{K}_{\varphi(m),1}$$

para

$$\begin{aligned} K &= (K_0, K_1) \in \mathcal{K} \\ e_K &= e_{K_1} \circ e_{K_0} \\ d_K &= d_{K_0} \circ d_{K_1} \end{aligned}$$

2 DES (Data Encription Standard)

2.1 Un poco de Historia

En 1972 la NBS (National Bureau of Standards), hoy en día conocida como NIST (National Institute of Standards and Technology), inició un programa para proteger computadores y comunicaciones. En 1973 la NBS publicó una solicitud pública para proposiciones conducentes a establecer algoritmos criptográficos. Entre los criterios de diseño de estos mecanismos se encontraban:

- el algoritmo debe proveer un alto grado de seguridad.
- el algoritmo debe estar completamente especificado y ser fácil de entender.
- la seguridad del algoritmo debe residir en la clave, es decir, la seguridad no puede depender del mantenimiento en secreto del método.

- el algoritmo debe estar disponible para todos los usuarios.
- el algoritmo debe poder implementarse económicamente a nivel de hardware.
- el algoritmo debe ser eficiente.
- el algoritmo debe ser exportable.
- el algoritmo debe poder validarse.

IBM desarrolló DES (Data Encryption Standard) como una modificación de un sistema conocido bajo el nombre de LUCIFER. La NBS para poder analizar las distintas propuestas pidió ayuda a la NSA (National Security Agency) para evaluar los algoritmos. DES se publicó en 1975, y se adoptó como un standard después de un intenso debate en 1976. Este debate se centraba en las modificaciones sugeridas por la NSA, las que consistieron básicamente en:

- Reducción del tamaño de la clave de 128 a 56 bits.
- Modificación de ciertas partes del algoritmo que en la época se vieron misteriosas pero a comienzos de 1990 los académicos advirtieron la trascendencia de ellas.

La NBS (NIST) evalúa DES aproximadamente cada cinco años. La próxima evaluación es este año (1998), en donde se espera sea descartado.