MA-53G Intr. a la Criptografía	**Semestre Primavera, 1996**

Cátedra No. 4 : 14 de Agosto

Transcriptor: Juan Pablo Alamo E.

1 Seguridad incondicional

En la cátedra anterior digimos que un criptosistema es incondicionalmente seguro si no puede quebrarse frente a un ataque, sin importar cuanta capacidad computacional utilizemos. Queremos formalizar esta noción para un ataque dirigido al texto cifrado.

El estudio de la seguridad incondicional no se puede hacerce en terminos de la capacidad computacional en relación al tiempo necesario en quebar un criptosistema, una forma apropidada es utilizar teoría de probabilidades como base. revisemos brevemente las principales definiciones en relación a esta materia que utilizaremos mas adelante.

Definición 1 *Sean X e Y dos variables aleatorias, denotamos la probabilidad que X tome el valor x por $p(x)$ y la probalilidad que Y tome el valor y por $p(y)$.* **la probabilidad conjunta** *$p(x, y)$ denota la probalilidad que X tome el valor x e Y tome el valor y.* **la probabilidad condicional** *$p(x|y)$ denota la probabilidad que X tome el valor x dado que Y tomo el valor y. Decimos que las variables aleatorias X y Y son independientes si $p(x, y) = p(x)p(y)$ para todo valor x de X e y de Y.*

Es posible expresar la probabilidad conjunta en terminos de probabilidad condicional como $p(x, y) = p(x|y)p(y)$, o bien $p(x, y) = p(y|x)p(x)$. De estas dos expresiones se desprende el em Teorema de Bayes

Teorema 1 Teorema de Bayes *si $p(y) > 0$, entonces*

$$p(x|y) = \frac{p(x)p(x|y)}{p(y)}$$

Corolario 1 *X e Y son variables aleatorias independientes si y solo si $p(x|y) = p(x)$ para todo x, y*

Consideramos un criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ de bloque, donde la clave que se eliga es usada para una sola encripción. Vamos a asumir, salvo que se diga lo contrario, que $|\mathcal{P}|, |\mathcal{C}|, |\mathcal{K}|, |\mathcal{E}|, |\mathcal{D}| < +\infty$, es decir los conjunto $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}$ y $\mathcal{D}$ son finitos.

Tomaremos una distribución de probabilidad sobre el conjunto de textos plano $\mathcal{P}$ denotando la probabilidad a priori de escoger x como $p_{\mathcal{P}}(x)$. Ademas asumimos que la clave k escogida por Alicia y Roberto tiene la misma distribución de probabilidad a priori denotada por $p_{\mathcal{K}}(k)$. Así $(\mathcal{P},2^{\mathcal{P}},p_{\mathcal{P}})$ modela la elección de textos planos comunicados y $(\mathcal{K},2^{\mathcal{K}},p_{\mathcal{K}})$ modela la elección de claves. Donde $2^{\mathcal{P}}$ y $2^{\mathcal{K}}$ son el conjunto de las partes de $\mathcal{P}$ y $\mathcal{K}$ respectivamente.

Vamos a considerar tres variables aleatorias X, Y, K, donde X representa el texto plano que ha sido encriptado, Y el texto cifrado enviado y K la clave escogida. Es natural asumir que X y K son variables aleatorias independientes ya que el texto plano x a enviar es un evento independiente a la elección de la clave k para el proceso de encripción.

Por último, las distribuciones de probabilidad en $\mathcal{P}$ y $\mathcal{K}$ induce una distribución de probabilidad $p_{\mathcal{C}}(y)$ (y es el texto cifrado) en $\mathcal{C}$ que se puede calcular usando los elementos de probabilidades anteriormente vistos.

Estudiemos la siguientes cantidades

(i) $p_{\mathcal{P}}(x) = \Pr[X = x]$, la probabilidad a priori que se envie el texto plano x, donde $x \in \mathcal{P}$

(ii) $p_{\mathcal{K}}(k) = \Pr[K = k]$, la probabilidad que se elija una cierta clave k, donde $k \in \mathcal{K}$

(iii) $p_{\mathcal{C}}(y) = \Pr[Y = y]$, la probabilidad que se envie el texto cifrado y, donde $y \in \mathcal{C}$. Observar que $p_{\mathcal{C}}(y) = \Pr[(X, K) \in \{(x, k) \mid e_k(x) = y\}]$.

(iv) $p_{\mathcal{P}}(x|y) = \Pr[X{=}x \mid Y{=}y]$, la probabilidad que x se haya encriptado dado que y fue enviado. Notar que $p_{\mathcal{P}}(x|y) = \Pr[X = x, K \in \{k \mid e_k(x) = y\}]$

(v) $p_{\mathcal{P}}(y|x) = \Pr[K \in \{k \mid e_k(x) = y\}]$, la probabilidad que y se envie dado que x se encripto. De la definición de probalilidades condicionales sigue que

$$p_{\mathcal{P}}(y|x) = \frac{p_{\mathcal{P}}(x|y)\, p_{\mathcal{C}}(y)}{p_{\mathcal{P}}(x)}$$

luego se tiene que

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x) p_{\mathcal{C}}(y|x)}{p_{\mathcal{C}}(y)}$$

De la independencia de las variables aleatorias X e Y se deduce que

$$p_{\mathcal{C}}(y) = \sum_{\substack{\{x\in\mathcal{P},k\in\mathcal{K} \\ :\, e_{\mathcal{K}}(x)=y\}}} \Pr[X{=}x, K{=}k] = \sum_{\substack{\{x\in\mathcal{P},k\in\mathcal{K} \\ :\, e_{\mathcal{K}}(x)=y\}}} p_{\mathcal{P}}(x)\, p_{\mathcal{K}}(k)$$

Ahora podemos formalizar la noción de ciptosistema perfectamente secreto.

Definición 2 *Criptosistema perfectamente secreto*
El criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ es perfectamente secreto si $p_{\mathcal{P}}(x|y) = p_{\mathcal{P}}(x)$ para todo $x \in \mathcal{P}, y \in \mathcal{C}$. Esto es, La probabilidad a posteriori que el texto plano sea x, dado que se obtiene el texto cifrado y, es identica a la probabilidad a priori que el texto plano sea x.

Estudiemos la seguridad del criptosistema Afín.

Recordemos que en el criptosistema Afín teniamos que $\mathcal{P} = \mathcal{C} = \mathcal{Z}_m$ y $\mathcal{K} = \{(a, b) \in (\mathcal{Z}_m)^2 \mid mcd(a, m) = 1\}$. Ahora calculemos $p_{\mathcal{P}}(x|y)$ usando el *teorema de Bayes*

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x) p_{\mathcal{C}}(y|x)}{p_{\mathcal{C}}(y)}$$

La probabilidad $p_{\mathcal{C}}(y|x) = \Pr[ax + b = y \ mod \ m]$ es sobre la elección de la tupla $(a, b) \in (\mathcal{Z}_m)^2$ sujeto a que $mcd(a, m) = 1$. Suponiendo que la claves se eligen uniformemente y fijamos a, sólo hay un valor $b \in \mathcal{Z}_m$ tal que $ax + b = y \ mod \ m$, por otro lado, si fijamos b entonces hay un valor de a que cumple la misma condición pero el rango en que varia a esta acotado por $mcd(a, m) = 1$, luego

$$p_{\mathcal{C}}(y|x) = \frac{1}{\phi(m)m}.$$

donde $\phi(m)$ es la cardinalidad del conjunto $\{a \in \mathcal{Z}_m : mcd(a, m) = 1\}$ que depende del valor m

Por otro lado como las variables aleatorias X e Y son independientes se tiene que

$$p_{\mathcal{C}}(y) = \sum_{\substack{\{x\in\mathcal{P},k\in\mathcal{K} \\ :\, e_{\mathcal{K}}(x)=y\}}} p_{\mathcal{P}}(x)\, p_{\mathcal{K}}(k)$$

Usando el supuesto de la uniformidad de la distribución de probabilidades $p_{\mathcal{K}}$ sobre $\mathcal{K}$, la expresión anterior se puede escribir como

$$p_{\mathcal{C}}(y) = \frac{1}{\phi(m)m} \sum_{x \in \mathcal{P}} p_{\mathcal{P}}(x)$$

entonces; cada vez que se fija una clave, existe un solo texto plano que cumple la condición $e_k(x) = y$, o bien, cada vez que se fija un texto plano, existe una sola clave que cumple la misma condición, luego $\sum_{x \in \mathcal{P}} p_{\mathcal{P}}(x) = 1$ entonces

$$p_{\mathcal{C}}(y) = \frac{1}{\phi(m)m}.$$

Hemos probado que $P_{\mathcal{P}}(x|y) = P_{\mathcal{P}}(x)$ esto significa que si utilizamos una clave distinta para encriptar cada texto plano, el criptosistema Afín es perfectamente secreto.

El ataque de la clase pasada (#3), radica en el hecho que las claves se utilizan reiterativamente para encriptar distintos textos plano.

Proposición 1 *El criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ es perfectamente secreto si se cumple que $p_{\mathcal{C}}(y|x) = p_{\mathcal{C}}(y)$, para todo $x \in \mathcal{P}$ y para todo $y \in \mathcal{C}$.*

Dem: De la Definición 2, perfectamente secreto significa que $p_{\mathcal{P}}(x|y) = p_{\mathcal{P}}(x)$. Luego del teorema de Bayes se puede escribir

$$p_{\mathcal{P}}(x) = p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{C}}(y|x) p_{\mathcal{P}}(x)}{p_{\mathcal{C}}(y)}$$

Cancelando $p_{\mathcal{P}}(x)$ y reordenando términos en la expresion anterior se desprende que

$$p_{\mathcal{C}}(y) = p_{\mathcal{C}}(y|x)$$

$\square$

Es natural asumir que $p_{\mathcal{C}}(y) > 0$ para todo $y \in \mathcal{C}$, de lo contrario el texto cifrado nunca se genera, entonces puede ser omitido del conjunto $\mathcal{C}$. Luego en un criptosistema perfectamente secreto $p_{\mathcal{C}}(y|x) = p_{\mathcal{C}}(y) > 0$, por lo tanto para cada $y \in \mathcal{C}$ debe haber por lo menos una clave $k \in \mathcal{K}$ tal que $e_k(x) = y$ luego $|\mathcal{C}| \leq |\mathcal{K}|$ (no se puede ocupar las mismas claves). Si la regla de encripción no es ambigua entonces $|\mathcal{P}| \leq |\mathcal{C}|$. En el caso límite donde $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ la siguiente proposición no da una caracterización alternativa de lo que es un criptosistema perfectamente secreto.

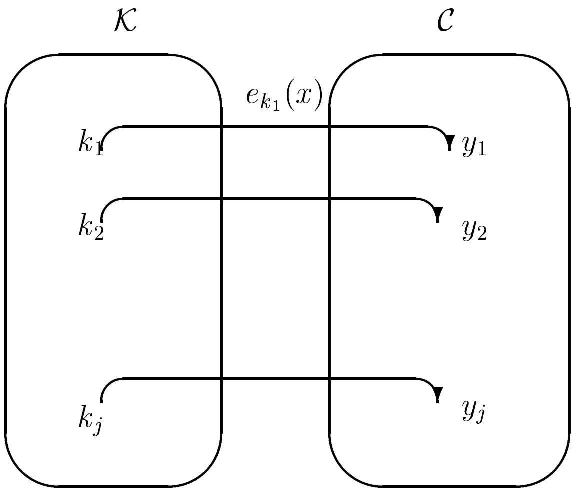

Figure 1: Biyección entre los conjunto $\mathcal{K}$ y $\mathcal{C}$

Proposición 2 *Sea* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *un criptosistema donde* $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$*, entonces es perfectamente secreto si y sólo si cada clave es usada con igual probabilidad* $1/|\mathcal{K}|$*, y para todo* $x \in \mathcal{P}, y \in \mathcal{C}$ *existe por lo menos una clave* $k \in \mathcal{K}$ *tal que* $e_k(x) = y$.

Dem: Haremos la demostración en los dos sentidos separadamente

$\boxed{\Rightarrow}$ De la definición de criptosistema perfectamente secreto se sabe que $\forall x \in \mathcal{P}, \forall y \in \mathcal{P}$ existe $k \in \mathcal{K}$ tal que $e_k(x) = y$, luego $\forall x \in \mathcal{P}$, se tiene que

$$|\mathcal{C}| = |\{e_k(x) \,:\, k \in \mathcal{K}\}| = |\mathcal{K}|,$$

entonces no existen dos claves distintas $k_1, k_2 \in \mathcal{K}$ tal que $e_{k_1}(x) = e_{k_2}(x) = y$, luego $\forall x \in \mathcal{P}, \forall y \in \mathcal{C}$ existe una sola clave $k \in \mathcal{K}$ que cumple $e_k(x) = y$. De esta forma hemos probado que hay una biyección entre el conjunto $\mathcal{K}$ y $\mathcal{C}$, (ver Figura 1) formalmente

$$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}\ \exists! k \in \mathcal{K} \text{ que cumple } e_k(x) = y.$$

Ahora definimos la biyección $\Pi_y : \mathcal{P} \longrightarrow \mathcal{K}$ tal que para cada $x \in \mathcal{P}$ se asocia $k \in \mathcal{K}$ que cumple $e_{\Pi_y(k)}(x) = y$. Queremos calcular $\Pr[K = \Pi_y(x)]$, utilizando el hecho que el criptosistema es perfectamente secreto, de la Proposición 1 se tiene que $p_{\mathcal{C}}(y|x) = p_{\mathcal{C}}(y)$ luego como $\Pr[K = \Pi_y(x)] = p_{\mathcal{C}}(y|x)$ se cumple que

$$\Pr[K = \Pi_y(x)] = p_{\mathcal{C}}(y), \forall x \in \mathcal{P}$$

considerando que existe una biyección entre el conjuto $\mathcal{K}$ y $\mathcal{C}$ la distribución de $p_{\mathcal{C}}$ es igual a la de $p_{\mathcal{K}}$ entonces se deduce que

$$\Pr[K = k] = \frac{1}{|\mathcal{K}|}$$

$\boxed{\Leftarrow}$
Sabemos que $p_{\mathcal{C}}(y|x) = p_{\mathcal{K}}(k \in \{k : e_k(x) = y\})$, luego como cada clave se usa con igual probabilidad se tiene que $p_{\mathcal{C}}(y|x) = 1/|\mathcal{K}|$. Por otro lado, como vimos anteriormente, del *Teorema Bayes* se sabe que

$$p_{\mathcal{C}}(y) = \sum_{\substack{\{x \in \mathcal{P}, k \in \mathcal{K} \\ : e_k(x) = y\}}} p_{\mathcal{P}}(x) p_{\mathcal{K}}(k)$$

Ya que la elección de claves tiene una distribución uniforme se puede separar la suma de la expresión anterior sacando un término común como sigue

$$p_{\mathcal{C}}(y) = \frac{1}{|\mathcal{K}|} \sum_{x \in \mathcal{P}} p_{\mathcal{P}}(x) \sum_{\substack{\{k \in \mathcal{K} \\ : e_k(x) = y\}}} 1$$

De la expresión anterior se puede concluir que la suma $\sum_{x \in \mathcal{P}} p_{\mathcal{P}}(x)$ representa todos los posibles valores que toma la variable aleatoria X, luego tiene el valor 1. La siguiente suma sólo tiene un término que cumple la condición $e_k(x) = y$ luego también su valor es 1. Así se obtiene que

$$p_{\mathcal{C}}(y) = \frac{1}{|\mathcal{K}|}$$

entonces, de esta última ecuación se concluye que

$$p_{\mathcal{C}}(y|x) = p_{\mathcal{C}}(y)$$

Así, de la Proposición 1, el cirtosistema es perfectamente secreto. □

Un criptosistema que cumple la condición de ser perfectamente secreto es el llamado **one-time Pad** inventado por Vernam (1917), quien lo utilizó para la encripción y decripción de mensajes telegráficos. Ahora lo describiremos formalmente

Definición 3 *Criptosistema One-time Pad*
Sea el criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *done* $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathcal{Z}_2)^n$ *con* $n \geq 1$ *entero, y una clave* $k \in (\mathcal{Z}_2)^n$*. Se define* $e_k(x)$ *como la suma del vector* k *y* x *modulo 2 (o equivalentemente el OR-exclusivo entre estas cadenas de bit). De este modo, si* $x = (x_1, ..., x_n)$ *y* $k = (k_1, ..., k_n)$ *entonces, la función de encripción es*

$$e_k(x) = (x_1 + k_1, ..., x_n + k_n) \bmod 2$$

y la función de decripción, si $y = (y_1, ..., y_n)$ *es*

$$d_k(y) = (y_1 + k_1, ..., y_n + k_n) \bmod 2$$

Este criptosistema tiene seria limitaciones, por ejemplo; hay un serio manejo de claves ya que hay problemas de sincronización, se necesita generar una gran cantidad de bits aleatorios, lo que es costoso. Si la clave se genera utilizando bits pseudo-aleatorios entonces se habre la posibilidad de atacar el criptosistema atacando el generador de bits pseudo-aletorios. Por último, $|\mathcal{K}| \geq |\mathcal{P}|$, i.e. la clave es por lo menos tan larga como toda la comunicación, sin enbargo la propiedad de ser incondicionalmente seguro lo hace muy útil en el contexto diplomatico o militar.