PROBABILIDAD Y CRIPTOGRAFÍA

Espacio de Mensajes: $\mathcal{M}$

- Probabilidad de que un mensaje emitido sea x:
  $P[M = x]$

Espacio de Claves: $\mathcal{K}$

- Probabilidad de que una clave elegida sea k:
  $P[K = k]$

Espacio de Cifrados: C= $\{Enc_k(x) / x \in M \wedge k \in K\}$

Las claves se eligen independientemente de los mensajes planos, por lo que:

$$P[M = x, K = k] = P[M = x] \cdot P[K = k]$$

Por lo tanto:

- Probabilidad de que aparezca el texto cifrado y:
  $$P[C = y] = \sum_{k:y \in C(k)} P[K = k] \cdot P[M = Dec_k(y)]$$

- Probabilidad de aparición del texto cifrado y, dado el texto plano x:
  $$P[C = y \mid M = x] = \sum_{k:x=Dec_k(y)} P[K = k]$$

- Probabilidad de que un texto plano sea x dado que el texto cifrado es y:
  $$P[M = x \mid C = y] = \frac{P[M = x] \sum_{k:x=Dec_k(y)} P[K = k]}{P[C = y]}$$

Ejemplo 1:

Espacio de Mensajes: $\mathcal{M}$={a,b}

$$P[M = a] = P[M = b] = 0{,}5$$

Espacio de Claves: $\mathcal{K}$={k1,k2}

$$P[K = k1] = P[K = k2] = 0{,}5$$

Espacio de Cifrados: C= $\{Enc_k(x) / x \in M \wedge k \in K\}$={c,d}

Donde Enc está dado por la tabla:

	a	b
k1	c	d
k2	d	c

$P[C = c] = P[K = k1] \cdot P[M = a] + P[K = k2] \cdot P[M = b]$ =0,5.0,5+0,5.0,5 = 0,5

$P[C = d] = P[K = k1] \cdot P[M = b] + P[K = k2] \cdot P[M = a]$ =0,5.0,5+0,5.0,5 = 0,5

$P[C = c \mid M = a] = P[K = k1] = 0{,}5$

$P[C = c \mid M = b] = P[K = k2] = 0{,}5$

$P[C = d \mid M = a] = P[K = k2] = 0{,}5$

$P[C = d \mid M = b] = P[K = k1] = 0{,}5$

Se observa que se cumple $P[C = y \mid M = x] = P[C = y] \ \forall y \forall x$, por lo que **hay secreto perfecto**

$P[M = a \mid C = c] = (P[M = a]P[K = k1]) / P[C = c] = 0{,}5$

$P[M = a \mid C = d] = (P[M = a]P[K = k2]) / P[C = d] = 0{,}5$

$P[M = b \mid C = c] = (P[M = b]P[K = k2]) / P[C = c] = 0{,}5$

$P[M = b \mid C = d] = (P[M = b]P[K = k1]) / P[C = d] = 0{,}5$

Se observa que se cumple $P[M = x \mid C = y] = P[M = x] \ \forall y \forall x$, por lo que **hay secreto perfecto**

Ejemplo 2:

Espacio de Mensajes: $\mathcal{M}=\{a,b\}$

$$P[M=a]=0{,}25;\ P[M=b]=0{,}75$$

Espacio de Claves: $\mathcal{K}=\{k1,k2,k3\}$

$$P[K=k1]=0{,}5;\ P[K=k2]=P[K=k3]=0{,}25$$

Espacio de Cifrados: $C=\{Enc_k(x)/\ x\in M\wedge k\in K\}=\{1,2,3,4\}$

Donde Enc está dado por la tabla:

	a	b
k1	1	2
k2	2	3
k3	3	4

$$P[C=1]=P[K=k1]\cdot P[M=a]=\frac{1}{2}\cdot\frac{1}{4}=\frac{1}{8}$$

$$P[C=2]=P[K=k1]\cdot P[M=b]+P[K=k2]\cdot P[M=a]=\frac{1}{2}\cdot\frac{3}{4}+\frac{1}{4}\cdot\frac{1}{4}=\frac{7}{16}$$

$$P[C=3]=P[K=k2]\cdot P[M=b]+P[K=k3]\cdot P[M=a]=\frac{1}{4}\cdot\frac{3}{4}+\frac{1}{4}\cdot\frac{1}{4}=\frac{1}{4}$$

$$P[C=4]=P[K=k3]\cdot P[M=b]=\frac{1}{4}\cdot\frac{3}{4}=\frac{3}{16}$$

$$P[C=1\mid M=a]=P[K=k1]=\frac{1}{2}$$

$$P[C=1\mid M=b]=0$$

$$P[C=2\mid M=a]=P[K=k2]=\frac{1}{4}$$

$$P[C=2\mid M=b]=P[K=k1]=\frac{1}{2}$$

$$P[C=3\mid M=a]=P[K=k3]=\frac{1}{4}$$

$$P[C=3\mid M=b]=P[K=k2]=\frac{1}{4}$$

$$P[C=4\mid M=a]=0$$

$$P[C=4\mid M=b]=P[K=k3]=\frac{1}{4}$$

Se observa que <u>NO se cumple</u> $P[C=y\mid M=x]=P[C=y]\ \ \forall y\forall x$, por lo que **NO hay secreto perfecto**

$$P[M=a\mid C=1]=\left(P[M=a]P[K=k1]\right)/\ P[C=1]=\frac{\left(\frac{1}{4}\cdot\frac{1}{2}\right)}{\frac{1}{8}}=1$$

$$P[M=a\mid C=2]=\left(P[M=a]P[K=k2]\right)/\ P[C=2]=\frac{\left(\frac{1}{4}\cdot\frac{1}{4}\right)}{\frac{7}{16}}=\frac{1}{7}$$

$$P[M=a \mid C=3]=\left(P[M=a]P[K=k3]\right)/\,P[C=3]=\frac{\left(\frac{1}{4}\cdot\frac{1}{4}\right)}{\frac{1}{4}}=\frac{1}{4}$$

$$P[M=a \mid C=4]=\left(P[M=a]0\right)/\,P[C=4]=\frac{\left(\frac{1}{4}\cdot 0\right)}{\frac{1}{8}}=0$$

$$P[M=b \mid C=1]=\left(P[M=b]0\right)/\,P[C=1]=\frac{\left(\frac{3}{4}\cdot 0\right)}{\frac{1}{8}}=0$$

$$P[M=b \mid C=2]=\left(P[M=b]P[K=k1]\right)/\,P[C=2]=\frac{\left(\frac{3}{4}\cdot\frac{1}{2}\right)}{\frac{7}{16}}=\frac{6}{7}$$

$$P[M=b \mid C=3]=\left(P[M=b]P[K=k2]\right)/\,P[C=3]=\frac{\left(\frac{3}{4}\cdot\frac{1}{4}\right)}{\frac{1}{4}}=\frac{3}{4}$$

$$P[M=b \mid C=4]=\left(P[M=b]P[K=k3]\right)/\,P[C=4]=\frac{\left(\frac{1}{4}\cdot\frac{1}{4}\right)}{\frac{1}{8}}=1$$

Se observa que NO se cumple $P[M=x \mid C=y]=P[M=x]\ \ \forall y \forall x$, por lo que **NO hay secreto perfecto**