Tajność doskonała

Claude Shannon

1949 Communication theory of secrecy systems

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

$\mathcal{K}$: $\{k_1, k_2, \ldots, k_n\}$ z prawdopodobieństwami $p_1\ p_2\ \ldots\ p_n$, $\sum_i p_i = 1$, $P(K = k_i) = p_i$

$\mathcal{P}$: $\{x_1, x_2, \ldots, x_m\}$ z prawdopodobieństwami $p_1\ p_2\ \ldots\ p_m$, $P(X = x_i) = p_i$

Załóżmy, że X i K są niezależne, to mamy

$$P(X = x, K = k) = P(X = x)P(K = k)$$

$\mathcal{C}$ Y

$$P(Y = y) = \sum_{\{k \in \mathcal{K} : \bigvee_{x \in \mathcal{P}} e_k(x) = y\}} P(K = k, X = d_k(y)) =$$

$$= \boxed{\sum_k P(K = k) P(X = d_k(y))}$$

$$\boxed{P(Y = y | X = x) = \sum_{\{k \in \mathcal{K} : x = d_k(y)\}} P(K = k)}$$

$$P(X = x | Y = y) \overset{\text{wzór Bayesa}}{=} \frac{P(Y = y | X = x) P(X = x)}{P(Y = y)}$$

Def. Kryptosystem ma doskonałą tajność jeżeli

$$\boxed{\bigwedge_{x\in\mathcal{P}} \bigwedge_{y\in\mathcal{C}} P(X=x \mid Y=y) = P(X=x).}$$

$$\underbrace{P(x\mid y)}_{\text{ozn.}} = \underbrace{P(x)}_{\text{ozn.}} \quad !!!$$

Przykład.

$\mathcal{P}=\{a,b\}$, $\mathcal{C}=\{1,2,3,4\}$, $K=\{k_1,k_2,k_3\}$

$P(a)=\frac{1}{4}$ $\qquad$ $P(k_1)=\frac{1}{2}$

$P(b)=\frac{3}{4}$ $\qquad$ $P(k_2)=P(k_3)=\frac{1}{4}$

e_k:

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

$$P(1) = P(a)P(k_1) = \frac{1}{4}\cdot\frac{1}{2} = \frac{1}{8}$$

$$P(2) = P(a)P(k_2) + P(b)\cdot P(k_1) = \frac{1}{4}\cdot\frac{1}{4} + \frac{3}{4}\cdot\frac{1}{2} = \frac{7}{16}$$

$$P(3) = \frac{1}{4}\cdot\frac{1}{4} + \frac{3}{4}\cdot\frac{1}{4} = \frac{4}{16} = \frac{1}{4}$$

$$P(4) = \frac{3}{4}\cdot\frac{1}{4} = \frac{3}{16}$$

$$P(a\mid 1) = \frac{P(1\mid a)\,P(a)}{P(1)} = \frac{\frac{1}{2}\cdot\frac{1}{4}}{\frac{1}{8}} = 1$$

$$P(a) = \frac{1}{4}$$

$$P(a\mid 2) = \frac{\frac{1}{4}\cdot\frac{1}{4}}{\frac{7}{16}} = \frac{1}{7} \neq P(a)$$

$$P(a|3) = \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{1}{4}} = \frac{1}{4} = P(a)$$

$$P(b|3) = \frac{\frac{1}{4} \cdot \frac{3}{4}}{\frac{1}{4}} = \frac{3}{4} = P(b)$$

ONE TIME PAD (szyfr Vernama)

$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$ zbiór ciągów 0-1 o dł. n

$\#\mathcal{P} = \#\mathcal{C} = \#\mathcal{K} = 2^n$

$$e_k(x) = x \text{ XOR } k = x \oplus k =$$
$$= (x+k) \bmod 2$$

$$\begin{array}{rrl} & 0110111 & x \\ \oplus & 1011011 & k \\ \hline & 1101100 & y \end{array}$$

$$d_k(y) = y \oplus k$$

$$d_k(e_k(x)) = d_k(x \oplus k) = (x \oplus k) \oplus k =$$
$$= x \oplus (k \oplus k) = x \oplus 0 = x \; !$$

Tw. Jeżeli w P i K mamy rozkłady jednostajne (dyskretne), to OTP jest doskonale tajny.

Dow. $\bigwedge_{x} \bigwedge_{y} P(x|y) = P(x)$?

$$P(x|y) = \frac{P(y|x)\,P(x)}{P(y)} = \frac{\cancel{\frac{1}{2^n}} \cdot \frac{1}{2^n}}{\cancel{\frac{1}{2^n}}} = \frac{1}{2^n}$$

$$\parallel$$

$$P(x) = \frac{1}{2^n}$$

$$P(y|x) = \sum_{k:\ d_k(y)=x} P(k) = \frac{1}{2^n}$$

$$y \oplus k = x \quad | \oplus y$$

$$y \oplus y \oplus k = y \oplus x$$

$$k = y \oplus x \in P$$

$$P(y) = \sum_{\{k:\ \bigvee_{x} e_k(x) = y\}} P(k)\, P(d_k(y)) =$$

$$= \sum_{k \in K} \frac{1}{2^n} \cdot \frac{1}{2^n} = \cancel{2^n} \cdot \frac{1}{\cancel{2^n}} \cdot \frac{1}{2^n} = \frac{1}{2^n}$$

$e_k(x) = y \qquad x \oplus k = y \quad | \oplus k \qquad x = y \oplus k$

WADY OTP

1) Klucz musi być tak samo długi, jak tekst jawny!

2) Klucz może być użyty tylko raz!
   jeden

1941 – 1946

Projekt Venona

$x_1 \quad x_2 \qquad k$

$e_k(x_1) = x_1 \oplus k = y_1$

$e_k(x_2) = x_2 \oplus k = y_2$

$y_1 \oplus y_2 = (x_1 \oplus k) \oplus (x_2 \oplus k) =$

$= (x_1 \oplus x_2) \oplus \underbrace{(k \oplus k)}_{0} = x_1 \oplus x_2$

znajomość $x_1 \oplus x_2$ pozwala poznać x_1 i x_2.

1) Nadmiarowość języka.

2) Specyfika kodowania (ASCII)