1 Absolútne bezpečná šifra

Teoretické základy kryptografie možno datovať do roku 1949, keď Claude Shannon publikoval svoju prácu „Communication Theory of Secrecy Systems“. V tejto časti sa bližšie pozrieme na pojem absolútne (resp. nepodmienene) bezpečnej šifry.

Bezpečnosť šifrovacieho systému môže byť dvoch druhov: výpočtová a nepodmienená. Prvá počíta s tým, že útočníkova výpočtová kapacita je obmedzená. Pri nepodmienenej bezpečnosti si takúto podmienku nekladieme.

Prirodzene, bezpečnosť šifrovacieho systému závisí aj od typu útoku (COA, KPA, ...) a ďalších predpokladov. Teda aj pojem absolútne (nepodmienene) bezpečnej šifry bude obmedzený niekoľkými predpokladmi.

1.1 Označenia predpoklady

Pripomeňme, že šifrovací systém je dvojica funkcií (algoritmov) $E : P \times K \to C$ a $D : C \times K \to P$, s vlastnosťou

$$\forall k \in K\, \forall p \in P : \quad D_k(E_k(p)) = p,$$

kde P, C a K sú konečné množiny otvorených textov, šifrových textov a kľúčov.

Označme $p(x)$ pravdepodobnosť, že náhodná premenná $\mathbf{X}$ nadobudne hodnotu x. Podobne $p(y)$ označuje pravdepodobnosť, že náhodná premenná $\mathbf{Y}$ nadobudne hodnotu y. Potom $p(x, y)$ označuje simultánne nastatie oboch spomínaných udalostí a $p(x|y)$ pravdepodobnosť že $\mathbf{X} = x$, ak už $\mathbf{Y}$ nadobudla hodnotu y. Ak platí

$$\forall x\, \forall y : \quad p(x|y) = p(x)p(y),$$

tak $\mathbf{X}$ a $\mathbf{Y}$ sa nazývajú nezávislé náhodné premenné.

Ľahko vidieť, že $p(x, y) = p(x|y)p(y)$ a zároveň $p(x, y) = p(y|x)p(x)$. Dáme oba vzťahy do rovnosti a dostaneme známu Bayesovu vetu:

$$p(x|y) = \frac{p(x)p(y|x)}{p(y)}, \qquad \text{ak } p(y) > 0.$$

Pojem absolútne bezpečného šifrovacieho systému sa opiera o nasledujúce predpoklady:

1. Budeme predpokladať fixnú distribúciu pravdepodobností nad P a nad K. Označíme $p_P(x)$ pravdepodobnosť, že otvorený text je x ($x \in P$). Podobne označíme $p_K(k)$ pravepodobnosť, že zvolený kľúč je k ($k \in K$).

2. Predpokladáme, že konkrétny kľúč je zvolený (použitý) na jedno šifrovanie.

3. Voľba kľúča k je nezávislá na voľbe otvoreného textu x.

Zároveň označíme $p_C(y)$ pravdepodobnosť, že šifrový text je (bude) $y \in C$.

Definícia 1. Šifrovací systém (E, D) je absolútne bezpečný, ak

$$\forall x \in P\, \forall y \in C : \quad p_P(x|y) = p_P(x).$$

Teda absolútne bezpečný šifrovací systém je taký, kde (apriórna) pravdepodobnosť otvoreného textu sa nezmení ani keď máme k dispozícii šifrový text.

Poznamenajme, že pojem absolútne bezpečnej šifry je definovaný v situácii útoku len so znalosťou šifrového textu (COA).

1.2 Vlastnosti

Majme nejaký absolútne bezpečný šifrovací systém. Predpokladajme, že $\forall y \in C$ je $p_C(y) > 0$, inak môžeme C zúžiť. Potom pre ľubovoľné $x \in P$ a $y \in C$ máme

$$p_P(x) = p_P(x|y) = \frac{p_P(x)p_C(y|x)}{p_C(y)},$$

odkiaľ dostávame

$$p_C(y|x) = p_C(y).$$

Teda $p_C(y|x) > 0$. To znamená, že pre ľubovoľné y a ľubovoľné x existuje aspoň 1 kľúč k taký, že $E_k(x) = y$. Odtiaľ vyplýva, že $|K| \geq |C|$. Keďže každá funkcia E_k musí byť invertovateľná (injektívna), máme $|C| \geq |P|$. Ak dáme tieto vzťahy dokopy, dostaneme pre absolútne bezpečný šifrovací systém

$$|K| \geq |P|.$$

Veta 1. *Nech (E, D) je šifrovací systém, v ktorom $|P| = |C| = |K|$. Potom je tento systém absolútne bezpečný práve vtedy, keď $p_K(k) = 1/|K|$ ($\forall k \in K$) a $\forall x \in P\, \forall y \in C$ existuje práve jeden kľúč k taký, že $E_k(x) = y$.*

Dôkaz.
($\Rightarrow$) Nech je (E, D) absolútne bezpečný. Podľa predchádzajúcich úvah potom $\forall x \in P$, $\forall y \in C$ existuje aspoň jeden kľúč k taký, že $E_k(x) = y$. Keďže $|C| = |K|$, tak taký kľúč môže byť maximálne jeden (inak by sa nedostalo na iné šifrové texty). Teda existuje práve jeden kľúč s požadovanou vlastnosťou.

Označme $n = |K|$ a fixujme ľubovoľné $y \in C$. Nech $P = \{x_1, \ldots, x_n\}$. Potom pre $\forall i = 1, \ldots, n$ dostávame:

$$p_P(x_i) = p_P(x_i|y) = \frac{p_P(x_i)p_C(y|x_i)}{p_C(y)}$$
$$p_C(y) = p_C(y|x_i) = p_K(k_i),$$

kde k_i je práve ten jeden kľúč, pre ktorý $E_{k_i}(x_i) = y$. Teda $p_K(k_i)$ je konštanta pre ľubovoľné i a preto $p_K(k_i) = 1/|K|$.

($\Leftarrow$) Vypočítame $p_P(x|y)$. Vieme, že

$$p_P(x|y) = \frac{p_P(x)p_C(y|x)}{p_C(y)}.$$

Postupne určme jednotlivé pravdepodobnosti.

$$\begin{aligned} p_C(y) &= \sum_{k \in K} p_K(k) p_P(D_k(y)) \\ &= \frac{1}{|K|} \sum_{k \in K} p_P(D_k(y)). \end{aligned}$$

Keďže $\forall x \in P$ a $\forall y \in C$ existuje práve jeden kľúč k taký, že $E_k(x) = y$, je $\{D_k(y) \mid k \in K\} = P$. Preto

$$p_C(y) = \frac{1}{|K|} \sum_{x \in P} p_P(x) = \frac{1}{|K|}.$$

Ľahko vidieť, že $p_C(y|x) = p_K(k) = 1/|K|$ (k je ten jediný kľúč, pre ktorý $E_k(x) = y$). Dosadením do pôvodného vzťahu dostaneme

$$p_P(x|y) = \frac{p_P(x) \cdot \frac{1}{|K|}}{\frac{1}{|K|}} = p_P(x).$$

□

Príklad. Uvažujme Vernamovu šifru. Teda $P = C = K = \{0,1\}^n$ pre nejaké $n \geq 1$. Šifrovanie a dešifrovanie je dané vzťahmi $E_k(x) = x \oplus k$ a $D_k(y) = y \oplus k$. Potom dôsledkom predchádzajúcej vety je, že ak sú vo Vernamovej šifre kľúče volené rovnako pravdepodobne, je táto šifra absolútne bezpečná.