2 Dokonalá bezpečnost

V ideálním světě bychom o každém kryptografickém primitivu uměli dokázat, že je bezpečné. To je mnohem těžší, než se zdá, ale přeci jen existují konstrukce, pro které takový důkaz známe. V této kapitole si několik těchto výjimečných případů předvedeme. Ukáže se ale, že mají dost omezené využití.

2.1 Jednorázové klíče

Uvažujme následující symetrickou šifru. Jejím vstupem bude zpráva $\mathbf{x} \in \{0,1\}^n$ a stejně dlouhý klíč $\mathbf{k} \in \{0,1\}^n$. Zašifrovanou zprávu $\mathbf{y} \in \{0,1\}^n$ spočítáme jako XOR původní zprávy s klíčem, tedy $y_i = x_i \oplus k_i$ pro všechna i. Dešifrovat můžeme druhým vyxorováním s klíčem: $y_i \oplus k_i = (x_i \oplus k_i) \oplus k_i = x_i \oplus (k_i + k_i) = x_i \oplus 0 = x_i$.

Věta: Pakliže klíč zvolíme jako rovnoměrně náhodnou posloupnost bitů, je zašifrovaná zpráva také rovnoměrně náhodná posloupnost bitů.

Důkaz: Jelikož různé bity zprávy spolu neinteragují, stačí větu dokázat pro jediný bit:

- Pokud $x_i = 0$, pak s pravděpodobností 1/2 nastane $k_i = 0$, a tedy $y_i = 0 \oplus 0 = 0$, nebo $k_i = 1$, a tedy $y_i = 0 \oplus 1 = 1$.
- Pokud $x_i = 1$, pak s pravděpodobností 1/2 nastane $k_i = 0$, a tedy $y_i = 1 \oplus 0 = 1$, nebo $k_i = 1$, a tedy $y_i = 1 \oplus 1 = 0$.

V obou případech tedy y_i nabývá hodnot 0 a 1 se stejnou pravděpodobností. □

Z toho plyne, že zašifrovaný text nenese vůbec žádnou informaci o původním textu kromě jeho délky. Takové šifře se říká *dokonale bezpečná.* Ovšem pozor – takhle silnou záruku bezpečnosti dostáváme pouze tehdy, když jeden klíč použijeme pro jedinou zprávu. Takovým klíčům se říká *jednorázové klíče (one-time pad).*

Podívejme se, co se stane, pokud stejný klíč $\mathbf{k}$ použijeme pro dvě zprávy $\mathbf{x}$ a $\mathbf{x}'$. Víme, že $y_i = x_i \oplus k_i$ a $y'_i = x'_i \oplus k_i$. Pokud zašifrované zprávy vyxorujeme, dostaneme $y_i \oplus y'_i = (x_i \oplus k_i) \oplus (x'_i \oplus k_i) = (x_i \oplus x'_i) \oplus (k_i \oplus k_i) = (x_i \oplus x'_i) \oplus 0 = x_i \oplus x'_i$. Zašifrované zprávy se tedy liší přesně tam, kde se liší původní zprávy. Vzhledem k tomu, jak velkou redundanci mají přirozené jazyky, tato informace obvykle postačí k rekonstrukci většiny obsahu zpráv. Jen nerozlišíme jejich pořadí.

Vypadá to tedy, že jsme si nepomohli – místo bezpečného přenosu zprávy teď potřebujeme bezpečně přenést stejné dlouhý klíč. To přesto může být praktické. Pokud vysíláme do

ciziny tajného agenta, můžeme ho vybavit knížkou s jednorázovými klíči. Každou stránku použije na jednu zprávu, a pak ji zničí.

Také časem sestrojíme zajímavé šifry tak, že dokonale náhodnou posloupnost nahradíme výstupem pseudonáhodného generátoru. To už ovšem nebude dokonale bezpečné.

Kromě toho si všimněme, že změna jednoho bitu zašifrované zprávy způsobí změnu příslušného bitu dešifrované zprávy. Zbytek dešifrované zprávy zůstane nezměněn. Tato vlastnost nám komplikovala život už v první kapitole a zde vidíme, že se může projevit i u dokonale bezpečných šifer. Proto zopakujeme: šifra zaručuje utajení, nikoliv integritu.

Dodejme ještě, že šifru s jednorázovým klíčem poprvé popsal Frank Miller v roce 1882, znovu ji objevil Gilbert Vernam v roce 1917 (proto se této šifře často říká Vernamova) a dokonalou bezpečnost dokázal Claude Shannon v roce 1945 (proto místo dokonale bezpečné někdy říkáme shannonovsky bezpečné).

Zobecnění

Stejný princip můžeme použít v libovolné grupě. Kdykoliv máme nějakou komutativní grupu $(G, +, \mathbf{0}, -)$, můžeme zprávu $x \in G$ zašifrovat náhodným[1] klíčem $k \in G$ jako $y = E(x, k) = x + k$, a tedy dešifrovat jako $D(y, k) = y - k = (x + k) - k = x$. Předchozí „xorovací“ verzi dostaneme volbou $G = \mathbb{Z}_2^n$.

Opět nahlédneme, že sečtením libovolného prvku grupy s rovnoměrně náhodným prvkem dostaneme rovnoměrně náhodný prvek. (Pro každé $a \in G$ je $x \mapsto a + x$ permutace na G.) Proto je i tato šifra dokonale bezpečná.

Dokonalou bezpečnost můžeme interpretovat i takto: Nechť Alice vybere zprávu $X \in G$ z nějakého neznámého pravděpodobnostního rozdělení $\mathcal{D}$ a rovnoměrně rozdělený klíč $K \in G$. My jsme zpozorovali nějakou konkrétní hodnotu y náhodné veličiny $Y = E(X, K) = X + K$ a ptáme se, jaká je za této podmínky pravděpodobnost, že X je rovno nějaké konkrétní zprávě x. Zajímá nás tedy $\Pr[X = x \mid Y = y] = \Pr[X = x \mid X + K = y] = \Pr[X = x \mid K = y - X]$. Ovšem K je zvoleno nezávisle na X, takže jevy $X = x$ a $K = y - x$ jsou nezávislé, a tudíž je podmíněná pravděpodobnost rovna nepodmíněné $\Pr[X = x]$. Pozorování $Y = y$ tedy nepřináší vůbec žádnou informaci o hodnotě X.

Délka klíče

Kromě toho, že se klíče nesmí opakovat, je nešikovné i to, že jsou dlouhé. To je bohužel také nevyhnutelné.

Věta: Žádná šifra, jejíž prostor klíčů je menší než prostor zpráv, není dokonale bezpečná.

[1] Měli bychom samozřejmě říkat *rovnoměrně náhodným,* ale dohodněme se, že kdykoliv nezmíníme konkrétní rozdělení, budeme myslet rovnoměrné.

Důkaz: Nechť X je množina zpráv, K množina klíčů a $E : X \times K \to X$ šifrovací funkce.

Rovnoměrně náhodně vybereme zprávu $x \in X$ a klíč $k \in K$. Zprávu zašifrujeme: $y = E(x, k)$. Pokud ji zkoušíme dešifrovat všemi klíči $k' \in K$, dostáváme množinu možných originálů $O = \{D(y, k') \mid k' \in K\}$. Jistě je $x \in O$. Jelikož ale platí $|O| \leq |K| < |X|$, musí existovat nějaká zpráva $x' \in X \setminus O$.

Pro zašifrovanou zprávu y je tedy x možným originálem, zatímco x' nikoliv. Všechny originály tedy nejsou stejně pravděpodobné, takže šifra není dokonale bezpečná. □

2.2 Rozdělování tajemství

Alice a Bob si do trezoru uložili svou soukromou korespondenci, aby v důchodu mohli vzpomínat na časy dávných dobrodružství. Chtějí ale, aby trezor mohli otevřít pouze oba společně. Klíč k trezoru tedy potřebují rozdělit na dvě části tak, aby se z obou dohromady dal spočítat celý klíč, ale žádná jedna z nich nedávala o klíči žádné informace kromě délky.

Princip one-time padu se dá použít i k jiným věcem než šifrování. Máme nějaké tajemství $\mathbf{x} \in \{0,1\}^n$. Vygenerujeme náhodný řetězec $\mathbf{a} \in B^n$ a spočítáme $\mathbf{b} = \mathbf{x} \oplus \mathbf{a}$. Víme, že jak $\mathbf{a}$, tak $\mathbf{b}$ jsou n-bitové náhodné řetězce, ale jejich xor je roven $\mathbf{x}$. To je možné díky tomu, že jsou sice náhodné, ale nikoliv nezávislé.

Dokázali jsme tedy rozložit tajemství $\mathbf{x}$ na dvě části tak, že žádná z částí sama o sobě neprozradí o $\mathbf{x}$ nic než délku, ale pokud známe obě, dokážeme $\mathbf{x}$ rekonstruovat přesně. O rozdělování tajemství můžeme uvažovat i obecněji: klíč od trezoru chceme rozdělit mezi k lidí tak, aby libovolných ℓ mohlo trezor otevřít.

Definice: (k, ℓ)*-prahové schéma* pro množinu zpráv X je randomizovaný algoritmus, který z $x \in X$ spočítá části $y_1, \ldots, x_k$ takové, že z libovolných alespoň ℓ částí lze rekonstruovat x, zatímco pro libovolnou podmnožinu méně než ℓ částí jsou všechna $x \in X$ stejně pravděpodobná.

Příklad ((k,k)-schéma): Naše první konstrukce je tedy $(2,2)$-schéma pro $X = \{0,1\}^n$. Podobně můžeme sestrojit (k,k)-schéma pro $X = \{0,1\}^n$ s libovolným $k > 1$: pro zprávu $\mathbf{x} \in \{0,1\}^n$ zvolíme náhodně $\mathbf{y}_1$ až $\mathbf{y}_{k-1}$ z $\{0,1\}^n$ a položíme $\mathbf{y}_k = \mathbf{y}_1 \oplus \mathbf{y}_2 \oplus \ldots \oplus \mathbf{y}_{k-1} \oplus \mathbf{x}$. Mohou nastat následující případy:

- Známe-li všechny části $\mathbf{y}_i$, stačí spočítat $\mathbf{y}_1 \oplus \ldots \oplus \mathbf{y_k} = (\mathbf{y}_1 \oplus \mathbf{y}_1) \oplus \ldots \oplus (\mathbf{y}_{k-1} \oplus \mathbf{y}_{k-1}) \oplus \mathbf{x} = \mathbf{x}$.
- Pokud by jednou z chybějících částí bylo $\mathbf{y}_k$, byly by všechny známé části nezávislé jak mezi sebou, tak na $\mathbf{x}$, takže o $\mathbf{x}$ bychom nevěděli vůbec nic.

- Ve zbývajícím případě $\mathbf{y}_k$ nechybí, takže chybí alespoň jedna náhodně vygenerovaná část $\mathbf{y}_i$ $(i < k)$. Pro každou hodnotu $\mathbf{x}$ a hodnoty ostatních chybějících částí přitom existuje právě jedna hodnota $\mathbf{y}_i$, s níž vyjde pozorované $\mathbf{y}_k$. Všechna $\mathbf{x}$ jsou tedy stejně pravděpodobná.

Příklad (neefektivní (k,ℓ)-schéma): Obecné (k,ℓ) schéma lze odvodit tak, že pro každou ℓ-prvkovou podmnožinu osob použijeme (ℓ,ℓ)-schéma. To provedeme $\binom{k}{\ell}$-krát, pokaždé vytvoříme ℓ částí, takže celkem vznikne $\binom{k}{\ell}\ell$ částí, z nichž každý dostane $\binom{k}{\ell}\frac{\ell}{k} = \binom{k-1}{\ell-1}$. Pokud se sejde alespoň ℓ lidí, tak pro alespoň jednu ℓ-tici známe všechny části a tajemství rekonstruujeme. Pokud se sejde méně než ℓ, v každé ℓ-tici nějaká část chybí, takže z žádné ℓ-tice se nic nedozvíme.

Shamirovo schéma

Efektivní konstrukci (k,ℓ)-schémat popsal v roce 1979 Adi Shamir. Začneme triviálním případem.

Příklad (pokus o $(k,2)$-schéma): Nechť x je zpráva a y_1 nějaké náhodné číslo. Vedeme přímku body $(0,x)$ a $(1,y_1)$ a najdeme body $(2,y_2)$ až (k,y_k) na této přímce. To nám dá části $y_1,\ldots,y_k$. Kdykoliv známe alespoň dvě části y_i a y_j, vedeme jednoznačně určenou přímku body (i,y_i) a (j,y_j) a najdeme její průsečík s osou y, tedy bod $(0,x)$. Známe-li jen jednu část y_i, pro každou potenciální zprávu x existuje právě jedna přímka procházející body $(0,x)$ a (i,y_i), takže všechny zprávy jsou stejně pravděpodobné.

Příklad (opravdové $(k,2)$-schéma): Předchozí pokus selže na tom, že nelze vybrat rovnoměrně náhodně racionální číslo. Místo toho se budeme na zprávy dívat jako na prvky nějakého dostatečně velkého konečného tělesa $\mathbf{F}$, pro které navíc musí platit $|\mathbf{F}| > k$. Pevně zvolíme prvky tělesa $a_0,\ldots,a_k$. Nechť $x \in \mathbf{F}$ je zpráva. Zvolíme $y_1 \in \mathbf{F}$ náhodně a najdeme (jednoznačně určenou) lineární funkci $f(t) = \alpha t + \beta$ takovou, že $f(a_0) = x$ a $f(a_1) = y_1$. Spočítáme další části $y_2 = f(a_2)$ až $y_k = f(a_k)$. Nyní dokážeme:

- Známe-li libovolné dvě části y_i a y_j, najdeme jednoznačně určenou funkci f procházející body (a_i,y_i) a (a_j,y_j), takže můžeme spočítat $x = f(a_0)$.
- Znalost samotného y_1 nám nepomůže, protože je rovnoměrně náhodné a nezávislé na x.
- Znalost jednoho y_i pro $i > 1$ nám také nepomůže, protože bodem (a_i,y_i) prochází $|\mathbf{F}|$ možných přímek odpovídajících bodům (a_1,y_1) pro jednotlivá $y_1 \in \mathbf{F}$. Stejné přímky můžeme také určit pomocí bodů (a_0,x) pro možné zprávy x. Jelikož všechna y_1 jsou stejně pravděpodobná, jsou stejně pravděpodobné i zprávy x.

Obecné Shamirovo schéma využívá místo přímek polynomy. Proto si nejdříve zopakujeme několik zásadních vlastností polynomů, které platí nad libovolným tělesem.

Lemma: Nechť p je polynom s kořeny $\alpha_1, \ldots, \alpha_t$. Pak platí $p(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_t)\cdot q(x)$, kde q je polynom bez kořenů.

Myšlenka důkazu: Budeme polynom opakovaně dělit monomy $(x - \alpha_i)$ a všimneme si, že to vždy vyjde beze zbytku. □

Důsledek: Nenulový polynom stupně d má nejvýše d kořenů.

Věta: Jsou-li p a q polynomy stupně menšího než d a platí-li $p(x_i) = q(x_i)$ pro nějaká navzájem různá $x_1, \ldots, x_d$, pak $p = q$.

Důkaz: Uvažme polynom $r = p-q$. Pro všechna i platí $r(x_i) = p(x_i)-q(x_i) = 0$. Polynom r má tedy alespoň d kořenů, ale jeho stupeň musí být menší než d. Podle předchozího důsledku je tedy všude nulový, tudíž $p = q$. □

Věta: Pro každé $x_1, \ldots, x_d$ navzájem různé a $y_1, \ldots, y_d$ existuje právě jeden polynom p stupně menšího než d, který splňuje $p(x_i) = y_i$ pro všechna i.

Důkaz: Jednoznačnost plyne z předchozí věty, existenci dokážeme *Lagrangeovou interpolací.* Nejprve si všimneme, že polynom $q_i(x) = \prod_{j\neq i}(x - x_j)$ splňuje $q_i(x_j) = 0$ pro $j \neq i$ a $q_i(x_i) = \prod_{j\neq i}(x_i - x_j) \neq 0$. Polynom

$$q_i'(x) = \frac{\prod_{j\neq i}(x - x_j)}{\prod_{j\neq i}(x_i - x_j)}$$

tedy splňuje $q'(x_j) = 0$ pro $j \neq i$ a $q'(x_i) = 1$. Nyní stačí zvolit p jako lineární kombinaci těchto q_i':

$$p(x) = \sum_i y_i \cdot q_i'(x).$$

Dosadíme-li $x = x_j$, budou všechny sčítance nulové až na $y_j \cdot q_j(x_j) = y_j \cdot 1 = y_j$. □

Nyní konečně odvodíme Shamirovo schéma. Zvolme nějaké $k, \ell > 1$, konečné těleso $\mathbf{F}$ s více než k prvky a nějaké jeho navzájem různé prvky $a_0, \ldots, a_k$.

Pro zprávu $x \in \mathbf{F}$ vygenerujeme náhodně části $y_1, \ldots, y_{\ell-1} \in \mathbf{F}$ a najdeme jednoznačně určený polynom p procházející body (a_0, x) a (a_1, y_1) až $(a_{\ell-1}, y_{\ell-1})$. Zbývající části dopočítáme jako $y_\ell = p(a_\ell)$ až $y_k = p(a_k)$.

- Známe-li libovolných ℓ částí, Lagrangeovou interpolací jednoznačně určíme polynom p a vyhodnocením $p(a_0)$ získáme x.

- Leží-li všechny známé části mezi $y_1, \ldots, y_{\ell-1}$, dozvěděli jsme se jen rovnoměrně náhodné prvky tělesa, které jsou nezávislé jak mezi sebou, tak na x. O x tedy nevíme vůbec nic.
- Ve zbývajících případech nám chybí alespoň jedno z náhodně zvolených y_i. I kdybychom znali všechny ostatní části, možnými volbami y_i získáme $|\mathbf{F}|$ různých polynomů p, stejně jako možnými volbami x. Proto je-li y_i rovnoměrně náhodné, jsou i všechna x stejně pravděpodobná.