# Moderní kryptografické systémy

*Petr Chovanec*

## Motivační úlohy

**Úloha.** Chcete si s kamarádem hodit mincí, ale on je v České Republice a vy v Botswaně.

**Úloha.** Jste mezinárodní pozorovatelé a máte uspořádat volby v jedné nejmenované africké zemi. Může volit pouze občan nejmenované země a to pouze jednou. Také hlasování je tajné.

**Úloha.** Firma Seznámení úchylů™ provozuje chat, na kterém jsou právě Alice a Bob. Alice se ráda mazlí s plyšovými medvídky a Bob rád hladí mramorové bloky. Chtějí zkusit, jestli ten druhý nemá stejnou zálibu. Ale současně nechtějí, aby ten druhý věděl, co mají za zálibu.

Když v roce 1972 vyučující kryptografie označil myšlenky R. Merkleho za bláboly, tak asi netušil, že za čtyři roky tyto bláboly dobudou svět. V roce 1976 pánové Hellman a Diffie publikovali konkrétní algoritmus s veřejným klíčem, což byla revoluce v kryptografii. Již nebylo potřeba utajovat klíč, ale naopak ho zveřejnit.

## Hlavní druhy šifer

• Symetrické šifry: Na zašifrování i rozšifrování se používá stejný klíč. Například *Caesarova šifra, Enigma, DES, RC?, IDEA, Skipjack.*

• Asymetrické šifry: Na zašifrování se používá veřejný klíč, který je volně širitelný, a na rozšifrováni se využije soukromý klíč. Jsou založeny na jednocestných funkcích. Například *RSA, Diffie-Hellman, ElGamal, Knapsack alg. (Ruksakový algoritmus).*

• Hashovací funkce: používají se pro ověření totožnosti, digitální podpis ... Výsledkem jsou řadově menší čísla, která se připojí k původní zprávě. Jsou většinou také založeny na jednocestných funkcích. Například *MD?, DSA, XOR.*

Použili jsme některé neznámé pojmy:

*Jednocestná funkce* je funkce, která se jedním směrem vypočítá snadno, ale naopak těžce. Například $f(x) = x^2 + x + 1$. Pro $x = 1$ snadno zjistíme, že $f(x) = 3$. Ale když víte, že $f(x) = 3$, pak není stejně jednoduché zjistit, že $x_1 = 1,\ x_2 = -2$.

*Jednocestná hashovací funkce* jednocestná funkce, ale ze vstupu udělá konstantní počet bitů. Příklad: Na začátku je výsledek 0. Vezme se další byte zprávy a vyXORuje se s předchozím výsledkem. Nakonec se připojí ke zprávě.

V tomto příkladu lze jednoduše najít zprávy, které dávají stejný výsledek. Jiné algoritmy to umí řešit. Jak, to se dozvíte na přednášce.

## Popis některých algoritmů

### IDEA (International Data Encryption Standard)

Dílo Xuejia Lai a Jamese Masseyho, které spatřilo světlo světa ve Švýcarsku. Je to bloková šifra s klíčem délky 128 bitů. Zde popíšu algoritmus, ale proč to funguje se dozvíte na přednášce.

Vždy se vezme blok délky 64 bitů a rozdělí se na čtyři části po 16 bitech ($X_{1,\ldots,4}$). Pak se osmkrát provede (násobení i sčítání je $\pmod{2^{16}}$), ($N$) je výsledek $n$-tého kroku):

(1) = $X_1 \cdot K_1$.
(2) = $X_2 \cdot K_2$.
(3) = $X_3 \cdot K_3$.
(4) = $X_4 \cdot K_4$.
(5) = (1) `xor` (3).
(6) = (2) `xor` (4).
(7) = (5) $\cdot K_5$.
(8) = (6) + (7).
(9) = (8) $\cdot K_6$.
(10) = (7) + (9).
(11) = (1) `xor` (9).
(12) = (3) `xor` (9).
(13) = (2) `xor` (10).
(14) = (4) `xor` (10).

Výstupem je (11)(13)(12)(14). A nyní se tento postup opakuje ještě sedmkrát. $K_1, \ldots, K_N$ se dostane, jako rozdělení klíče na 16-bitové podklíče, když dojdou, tak se klíč rotuje o 25 bitů a znovu se rozdělí.

Rozšifrování se provádí stejným postupem, jen s opačně vybíranými klíči a násobením a přičítáním inverzních prvků.

### Diffie-Hellman

(1) Alice (Bob, Certifikační autorita) si zvolí číslo $n$ tak, aby $n$ bylo prvočíslo a aby $\frac{n-1}{2}$ bylo taky prvočíslo. K tomu si zvolí libovolný primitivní kořen $g$ k $n$. A zveřejní je.

(2) Alice si vybere velké číslo $x$ a spočítá $X = g^x \pmod{n}$.
(3) Bob si také vybere velké číslo $y$ a spočítá $Y = g^y \pmod{n}$.
(4) Vymění si tato čísla.
(5) Alice spočítá $k = Y^x \pmod{n}$.
(6) Bob spočítá $k' = X^y \pmod{n}$.

$$k = k' = g^{xy}.$$

Toto se nedá použít k přímé komunikaci, ale jen jako výměna klíče k nějaké symetrické šifře. Toto už napravuje ElGamal. V praxi se používá spíše $n = 2^m$, pro rychlé počítání na počítači. U.S. patent vypršel 29. dubna 1997, proto to můžete používat bez omezení.

**Příklad.** (Za Studentskou pečeť) Mějme grafy $G_1$ a $G_2$. Alice říká, že zná izomorfismus mezi $G_1$ a $G_2$, a Bob ho strašlivě potřebuje. Ale má i jiné nabídky a neví, jestli Alice neblafuje. Alice mu ho samozřejmě nechce ukázat. Vyřešte tento problém tak, aby Bob na 99.9% věděl, že Alice má vysněný izomorfismus.