Matematika IV – demonstrační cvičení

Michal Bulant

4. dubna 2011

7. demonstrační cvičení

Polynomiální kód generovaný polynomem $p(x)$ je (n, k)–kód jehož slova jsou polynomy stupně menšího než n dělitelné $p(x)$. Zpráva $m(x)$ je zakódována jako $v(x) = r(x) + x^{n-k}m(x)$, kde $r(x)$ je zbytek po dělení polynomu $x^{n-k}m(x)$ polynomem $p(x)$.

Pozor, konvence: Zprávu $b_0 b_1 \dots b_{k-1}$ reprezentujeme polynomem $m(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1}$.

Příklad 1. *Zakódujte zprávu* 1101 *pomocí* $(6, 4)$ *kódu generovaného polynomem* $1 + x + x^2$.

Matice G typu n/k reprezentující zobrazení $u = G \cdot v$, kde v je zpráva, u odpovídající kódové slovo, ve standardních bazích, se nazývá generující matice kódu.

Je-li g lineární kódování s maticí

$$G = \begin{pmatrix} P \\ \mathbb{E}_{n-k} \end{pmatrix},$$

kde P je matice typu $(n-k)/k$, potom zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^{n-k}$ s maticí

$$H = \begin{pmatrix} \mathbb{E}_{n-k} & P \end{pmatrix}$$

má následující vlastnosti

1. $\operatorname{Ker} h = \operatorname{Im} g$, tj.
2. přijaté slovo u je kódové slovo právě, když je $H \cdot u = 0$

Matice H se nazývá matice kontroly parity kódu. Hodnota $H \cdot u$ se nazývá syndrom slova u.

Příklad 2. *Určete generující matici a matici kontroly parity pro lineární kód $(7, 4)$ generovaný polynomem*

$$x^3 + x^2 + 1.$$

Příklad 3. *a) Určete generující matici a matici kontroly parity pro lineární kód* $(9, 4)$ *generovaný polynomem*

$$1 + x^2 + x^4 + x^5.$$

b) Vypočtěte část tabulky syndromů a vedoucích reprezentantů pro tento kód. Kolik bude mít řádků?

c) Jaký nejvyšší počet chyb detekuje/opravuje tento kód?

d) Dekódujte slova $100110010, 100100101, 111101100$ *a* 000111110.

RSA:

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A;
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat.];
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$;
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$;
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$;
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$.

Příklad 4. *Alice si za parametry svého RSA klíče zvolila* $p = 23, q = 31, e = 17$. *Dopočítejte její soukromý klíč a pomocí modulárního umocňování na druhou (s možným použitím kalkulačky) zašifrujte (a poté dešifrujte) zprávu* $m = 12$.

Diffie-Hellman key exchange, ElGamal

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b
- Společným klíčem pro komunikaci je g^{ab}.
- Původní (a nejobvyklejší) volba G je multipliktivní grupa invertibilních zbytkových tříd modulo prvočíslo p, její generátor bývá také nazývám *primitivní kořen modulo p* .
- Problém diskrétního logaritmu (DLP)
- Nezbytná autentizace (*man in the middle attack*)

Z protokolu DH na výměnu klíčů odvozen šifrovací algoritmus ElGamal:

- Alice zvolí cyklickou grupu G spolu s generátorem g
- Alice zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h)
- šifrování zprávy M: Bob zvolí náhodné y a vypočte $C_1 = g^y$ a $C_2 = M \cdot h^y$ a pošle (C_1, C_2)
- dešifrování zprávy: $OT = C_2/C_1^x$

Příklad 5. *Demonstrujte dohodu Alice a Boba na tajném klíči v DH systému na výměnu klíčů se (všem) známými parametry* $G = (\mathbb{Z}_{23}^{\times}, \cdot)$, $g = 5$.

Příklad 6. *Alice zvolila za parametry v kryptosystému ElGamal* $p = 23, g = 5$*, za svůj soukromý klíč zvolila* $x = 13$ *a zveřejnila veřejný klíč* (p, g, g^x)*. Ukažte, jak Bob zašifruje zprávu* $M = 17$ *určenou Alici a jak tuto zprávu následně Alice dešifruje.*