Cvičení 7: Aplikace: kódování a kryptografie

Teorie:

(n,k)–**kódy**: přenášíme slova o k bitech, přičemž potřebujeme rozpoznávat/opravovat přenosové chyby a za tím účelem přidáváme dodatečných $n-k$ bitů informace pro pevně zvolené $n > k$.

Hammingova vzdálenost (bitových slov): počet bitů, v nichž se dvě bitová slova liší. Kód odhaluje r a méně chyb právě, když je minimální Hammingova vzdálenost kódových slov právě $r+1$. Kód opravuje r a méně chyb právě, když je minimální Hammingova vzdálenost kódových slov právě $2r+1$.

Polynomiální kódy: 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 $p(x)$.

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

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

Věta 1. *Je-li g lineární kódování s maticí*

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

potom zobrazení $h : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^k$ 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. Hoidnota $H \cdot u$ se nazývá syndrom slova u.

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 zprávy C: $OT = D_d(C) \equiv C^d \pmod{n}$

Obdobně je možné zprávy podepisovat – vytvoří se tzv. hash zprávy (my v příkladech budeme pro jednoduchost používat krátké zprávy, které budou svým vlastním hashem), ten se „zašifruje“ pomocí d a připojí ke zprávě. Ověření podpisu se děje analogicky jako při dešifrování zprávy.

Výměna klíčů Diffie-Hellman

- Dohoda stran na **cyklické grupě** G (obvykle Z_p) 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}.

Šifrování ElGamal:

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí velké prvočíslo p, generátor g grupy $\mathbb{Z}_p^\times$, dále náhodné $1 < a < p-1$ a vypočte $e = g^a \pmod{p}$. Zveřejní $[p, g, e]$, tajný klíč je a.
- zašifrování numerického kódu zprávy M: zvolí náhodně $1 < k < p-1$ a vypočte $c = g^k \pmod{p}$ a $C = M \cdot e^k \pmod{p}$. Pošle $[c, C]$.
- dešifrování zprávy $[c, C]$: $OT = c^{-a} \cdot C$.

Příklad 112. Určete polynom, který generuje $(4, 1)$–kód opakování bitů.

Příklad 113. Určete nějaký ireducibilní polynom stupně 4 nad $\mathbb{Z}_2$ a zákodujte pomocí něj zprávu 11010.

Příklad 114.
1. Určete matici lineárního kódu generovaného polynomem $p(x) = 1 + x^2 + x^3$. Zapište příslušnou kontrolní matici.
2. Dekódujte zprávu 111101, předpokládáte-li, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Příklad 115. Binární slovo délky 11 je zakódováno pomocí polynomu $p(x) = x^4 + x^3 + 1$. Příjemce obdržel slovo 011101110111001.

1. Ukažte, že při přenosu došlo k chybě.
2. Určete původní slovo za předpokladu, že chyba při přenosu byla jediná.

Příklad 116. Uživatel Adam si zvolil prvočísla $p = 31, q = 83$, vypočetl $n = 31 \cdot 83 = 2573$ a veřejný klíč $e = 77$.

1. Zašifrujte zprávu $m = 14$ pro Adama.

2. Adam poslal zprávu $m = 5$, kterou podepsal číslem 56. Ověřte, že je to jeho podpis a že zpráva nebyla pozměněna.

3. V pozici Adama vypočtěte tajný klíč d a zprávu z 1. dešifrujte.

Příklad 117. Martin a Honza chtějí komunikovat, přestože se dosud neměli šanci potkat. Veřejně se domluvili na cyklické grupě $\mathbb{Z}_{41}^{\times}$. Martin si zvolil generátor grupy 11 a číslo 10 a zveřejnil trojici $(41, 11, e)$, kde $e \equiv 11^{10} \pmod{41}$.

1. V roli Honzy dokončete DH protokol výměny klíče a určete klíč pro následnou komunikaci.

2. Honza poslal Martinovi dvojici $[22, 6]$. V roli Martina zprávu zašifrovanou protokolem ElGamal dešifrujte.

3. Se znalostí zprávy (viz výsledek předchozího úkolu) ukažte, jak Honza šifroval (možností šifrování zprávy je více, pracujte s $k = 23$; dokázali byste toto k snadno určit se znalostí c a g?).