MB104 – 5. demonstrovaná cvičení
RSA algoritmus

Masarykova univerzita
Fakulta informatiky

27.3. 2012

Příklad 1. *Zakódujte zprávu* 10011 *pomocí* $(8,5)$ *kódu generovaného polynomem* $1 + x + x^3$.

Řešení. 11110011. □

Příklad 2. *Určete generující matici a matici kontroly parity pro lineární kód generovaný polynomem z předchozího příkladu.*

Řešení.

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$\square$

Příklad 3. *Metodou vedoucích reprezentantů dekódujte slovo* 10001111 *přijaté v kódu z předchozích příkladů za předpokladu, že došlo k minimálnímu počtu chyb při přenosu.*

Řešení. syndrom $S = 001$ vedoucí reprezentant: 00100000, pravděpodobně posílané kódové slovo 10101111.

$\square$

1. Řešení domácích úloh z minulého týdne

2. Návodné úlohy
   - RSA algoritmus
   - Algoritmus ElGamal

Martin zveřejnil svoje RSA klíče N=143 a e=17. Honza mu chce poslat zprávu 3. Jak to pomocí RSA algoritmu provede? Jak Martin posléze zprávu dešifruje?

Řešení. Martin zná rozklad čísla $143 = 11 \cdot 13$ (faktorizace je těžký problém pro velká N).

Martin zveřejnil svoje RSA klíče N=143 a e=17. Honza mu chce poslat zprávu 3. Jak to pomocí RSA algoritmu provede? Jak Martin posléze zprávu dešifruje?

Řešení. Martin zná rozklad čísla $143 = 11 \cdot 13$ (faktorizace je těžký problém pro velká N).
Díky tomuto rozkladu spočítá $\varphi(N) = 120$ a dopočítá inverzi k číslu 17 v okruhu Z_{120}: $[17]_{120}^{-1} = [113]$.

Martin zveřejnil svoje RSA klíče N=143 a e=17. Honza mu chce poslat zprávu 3. Jak to pomocí RSA algoritmu provede? Jak Martin posléze zprávu dešifruje?

Řešení. Martin zná rozklad čísla $143 = 11 \cdot 13$ (faktorizace je těžký problém pro velká N).
Díky tomuto rozkladu spočítá $\varphi(N) = 120$ a dopočítá inverzi k číslu 17 v okruhu Z_{120}: $[17]_{120}^{-1} = [113]$.
Honza pošle $3^{17} \equiv 9 \pmod{143}$

Martin zveřejnil svoje RSA klíče N=143 a e=17. Honza mu chce poslat zprávu 3. Jak to pomocí RSA algoritmu provede? Jak Martin posléze zprávu dešifruje?

Řešení. Martin zná rozklad čísla $143 = 11 \cdot 13$ (faktorizace je těžký problém pro velká N).
Díky tomuto rozkladu spočítá $\varphi(N) = 120$ a dopočítá inverzi k číslu 17 v okruhu Z_{120}: $[17]_{120}^{-1} = [113]$.
Honza pošle $3^{17} \equiv 9 \pmod{143}$
Martin dešifruje $9^{113} \equiv 3 \pmod{143}$. □

- Odesílatel zvolí cyklickou grupu G spolu s generátorem g.

- Odesílatel zvolí cyklickou grupu G spolu s generátorem g.
- Odesílatel zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h).

- Odesílatel zvolí cyklickou grupu G spolu s generátorem g.
- Odesílatel zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h).
- Šifrování zprávy Z: Bob zvolí náhodně y a vypočte $S_1 = g^y$ a $S_2 = Z \cdot h^y$ a pošle (S_1, S_2).

- Odesílatel zvolí cyklickou grupu G spolu s generátorem g.
- Odesílatel zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h).
- Šifrování zprávy Z: Bob zvolí náhodně y a vypočte $S_1 = g^y$ a $S_2 = Z \cdot h^y$ a pošle (S_1, S_2).
- Dešifrování zprávy:
  $M = S_2/S_1^x = Z \cdot h^y/(g^y)^x = Z \cdot h^y/(g^x)^y = Z \cdot h^y/(h^y) = Z.$

Příklad *Martin a Honza chtějí komunikovat šifrou ElGamal Domluvili se na cyklické grupě* $\mathbb{Z}_{41}^{+}$ *a Martin si náhodně zvolil generátor grupy* 11 *a číslo* 10 *a zveřejnil trojici* $(\mathbb{Z}_{41}, 11, 9)$, *(*$9 \equiv 11^{10} \pmod{41}$*). Honza mu pošle veřejně dvojici* $(22, 6)$. *Jakou zprávu Honza poslal?*

Příklad *Martin a Honza chtějí komunikovat šifrou ElGamal Domluvili se na cyklické grupě* $\mathbb{Z}_{41}^{+}$ *a Martin si náhodně zvolil generátor grupy* 11 *a číslo* 10 *a zveřejnil trojici* $(\mathbb{Z}_{41}, 11, 9)$, *(*$9 \equiv 11^{10} \pmod{41}$*). Honza mu pošle veřejně dvojici* $(22, 6)$. *Jakou zprávu Honza poslal?*

Řešení. Zprávu Z dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$.

Příklad *Martin a Honza chtějí komunikovat šifrou ElGamal Domluvili se na cyklické grupě* $\mathbb{Z}_{41}^{+}$ *a Martin si náhodně zvolil generátor grupy* 11 *a číslo* 10 *a zveřejnil trojici* $(\mathbb{Z}_{41}, 11, 9)$, *(*$9 \equiv 11^{10} \pmod{41}$*). Honza mu pošle veřejně dvojici* $(22, 6)$. *Jakou zprávu Honza poslal?*

Řešení. Zprávu Z dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$. Spočtěme nejprve $22^{10} \equiv 22^2 \cdot (22^2)^2 \cdot ((22^2)^2) \equiv (-8) \cdot (-8)^2 \cdot (-8)^2 \equiv (-8) \cdot 23 \cdot 23 \equiv -9 \pmod{41}$,

Příklad *Martin a Honza chtějí komunikovat šifrou ElGamal Domluvili se na cyklické grupě* $\mathbb{Z}_{41}^{+}$ *a Martin si náhodně zvolil generátor grupy* 11 *a číslo* 10 *a zveřejnil trojici* $(\mathbb{Z}_{41}, 11, 9)$, *(*$9 \equiv 11^{10} \pmod{41}$*). Honza mu pošle veřejně dvojici* $(22, 6)$*. Jakou zprávu Honza poslal?*

Řešení. Zprávu Z dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$. Spočtěme nejprve $22^{10} \equiv 22^2 \cdot (22^2)^2 \cdot ((22^2)^2) \equiv$ $(-8) \cdot (-8)^2 \cdot (-8)^2 \equiv (-8) \cdot 23 \cdot 23 \equiv -9 \pmod{41}$, $(-9)^{-1} = 9$,

Příklad *Martin a Honza chtějí komunikovat šifrou ElGamal Domluvili se na cyklické grupě* $\mathbb{Z}_{41}^{+}$ *a Martin si náhodně zvolil generátor grupy* 11 *a číslo* 10 *a zveřejnil trojici* $(\mathbb{Z}_{41}, 11, 9)$*,* *(*$9 \equiv 11^{10} \pmod{41}$*). Honza mu pošle veřejně dvojici* $(22, 6)$*. Jakou zprávu Honza poslal?*

Řešení. Zprávu Z dostaneme jako $Z \equiv (6/22^{10}) \pmod{41}$.
Spočtěme nejprve $22^{10} \equiv 22^2 \cdot (22^2)^2 \cdot ((22^2)^2) \equiv$
$(-8) \cdot (-8)^2 \cdot (-8)^2 \equiv (-8) \cdot 23 \cdot 23 \equiv -9 \pmod{41}$,
$(-9)^{-1} = 9$,
$Z = 9 \cdot 6 \equiv 13 \pmod{41}$. $\square$