BEZIT – 3. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

29. 2. 2024

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?
  - Dvě (různá) prvočísla p, q

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?
  - Dvě (různá) prvočísla p, q
  - Výpočet $n = p \cdot q$

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?
  - Dvě (různá) prvočísla p, q
  - Výpočet $n = p \cdot q$
  - Výpočet $\varphi(n)$ (jak?)

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?
  - Dvě (různá) prvočísla p, q
  - Výpočet $n = p \cdot q$
  - Výpočet $\varphi(n)$ (jak?)
  - Volba veřejného exponentu e

RSA (1 / 4) – tvorba klíčů

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Krok 1: Tvorba klíčů
  - Co vše potřebujeme?
  - Dvě (různá) prvočísla p, q
  - Výpočet $n = p \cdot q$
  - Výpočet $\varphi(n)$ (jak?)
  - Volba veřejného exponentu e
  - Výpočet inverzního prvku $e^{-1} mod \varphi(n)$ (Rozšířený Euklidův alg)

RSA (2 / 4) – formát zprávy

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Veřejný klíč: $\langle 84001980869843, 5 \rangle$
- Krok 2: Reprezentace zprávy
  - Zprávu chápeme jako čísla
  - Rozdělíme na čísla $x_1, \ldots, x_m$ tak, že $x_i < n$
  - Každé x_i šifrujeme zvlášť

RSA (3 / 4) – šifrování

- Zašifrujte pomocí RSA zprávu: `ahoj`
- Veřejný klíč: $\langle 84001980869843, 5 \rangle$
- Krok 3: Šifrování
  - $e(x_i, \langle n, e \rangle) = x_i^e \, mod \; n$

RSA (4 / 4) – dešifrování

- Vzniklou zprávu zpětně dešifrujte
- Krok 4: Dešifrování
  - $d(y, e^{-1}) = y^{e^{-1}} mod\ n$

Úkol

- Ve vašem oblíbeném programovací jazyce naprogramujte šifrování a dešifrování pomocí RSA
- Můj veřejný klíč (512bit):

```
n=8914059826100449095319934444726061981403199915175561009570828218239477606294983725826465862647017590486021330673184151552488940325281259133274699695424163
e=65537 (0x10001)
```

- Pošlete mi emailem vaše zašifrované (pomocí RSA) osobní číslo bez písmene "R"
- Bonusový úkol: Zjistěte z jakých prvočísel vzniklo číslo n

Úkol

- Ve vašem oblíbeném programovací jazyce naprogramujte šifrování a dešifrování pomocí RSA
- Můj veřejný klíč (512bit):

```
n=8914059826100449095319934444726061981403199915175561009570828218239477606294983725826465862647017590486021330673184151552488940325281259133274699695424163
e=65537 (0x10001)
```

- Pošlete mi emailem vaše zašifrované (pomocí RSA) osobní číslo bez písmene "R"
- Bonusový úkol: Zjistěte z jakých prvočísel vzniklo číslo n (vtip)

Úkol

- Ve vašem oblíbeném programovací jazyce naprogramujte šifrování a dešifrování pomocí RSA
- Můj veřejný klíč (512bit):

```
n=89140598261004490953199344447260619814031999151755610095
  708282182394776062949837258264658626470175904860213306 73
  184151552488940325281259133274699695424163
e=65537 (0x10001)
```

- Pošlete mi emailem vaše zašifrované (pomocí RSA) osobní číslo bez písmene "R"
- Bonusový úkol: Zjistěte z jakých prvočísel vzniklo číslo n (vtip)
- Soukromý klíč:

```
d = 724555544099319351370512699498843892380408714896016196 92
    667961485209419425259578407049913891393094615247605739 48
    880490938182665478769864905020066534910913
```