Timing attack on RSA cipher

FIT ČVUT v Praze
andryma1@fit.cvut.cz

June 21, 2018

Úvod

- Použité principy RSA
- Druhy útoků
- Realizace
- Problémy realizace

RSA I

- Šifrování:

$$c = |m^e|_n$$

- Dešifrování:

$$m = |c^d|_n$$

Square and Multiply

Algorithm 1 Square & Multiply algorithm

```
1:  function SQUARE_AND_MULTIPLY(m, e, n)
2:      c ← 1
3:      k ← BitLen(e)
4:      for i ← k − 1, 0 do
5:          c ← Mon_Mult(c, c)                    ▷ square
6:          if e[i] == 1 then                     ▷ ith bit of exponent e
7:              c ← Mon_Mult(c, m)                ▷ multiply
8:          end if
9:      end for
10:     return c
11: end function
```

RSA III

Montgomeryho násobení

Algorithm 2 Montgomery Multiplication

1: **function** MON_MULT($\bar{a}, \bar{b}, N$)
2: $t \leftarrow \bar{a} * \bar{b}$
3: $m \leftarrow N^{-1} * t \pmod{r}$
4: $\bar{u} \leftarrow (t + mN)/r$
5: **if** $\bar{u} > N$ **then**
6: $\bar{u} \leftarrow \bar{u} - N$
7: **end if**
8: **return** $\bar{u}$
9: **end function**

Realizace

- Python - dlouhá čísla
- modul *timeit*
- Potřeba vlastní RSA
- 50 000 zpráv

Orákulum

```
def square_and_multiply(ot, n, e):

 for i in "{0:b}".format(int(e)):
  st, sq = mont_product(st, st, n, r, n_inv)
  if i == '1':
   st, mult = mont_product(st, ot, n, r, n_inv)

 return mont_product(st, 1, n, r, n_inv), sq, mult
```

Útoky I

- Attack on Multiply

```
for i in message_times:
    dummy, sq, mult = counted_sq_mul(i, n, exp)
    if mult:
        reduced_dict[i] = message_times[i]
    else:
        unreduced_dict[i] = message_times[i]
```

Útoky II

- Attack on Square

```
for i in message_times:
 dummy, sq, mult = counted_sq_mul(i, n, exp * 2)
 if sq:
  m1_dict[i] = message_times[i]
 else:
  m2_dict[i] = message_times[i]
 dummy,sq,mult=counted_sq_mul(i, n, (exp - 1) * 2)
 if sq:
  m3_dict[i] = message_times[i]
 else:
  m4_dict[i] = message_times[i]
```

Úspěchy

- RSA
- Orákulum
- 40-80 bitů na 50 000 vzorků
- 3 dny

Problémy

- Míra šumu
- Jeden "špatný" bit kazí další výpočet
- Velká časová náročnost (domácí úkol?)

Závěr

- Attack on Multiply
- Attack on Square
- Průměrné měření
- Nejlepší měření

Děkuji za pozornost.

Otázky oponenta I

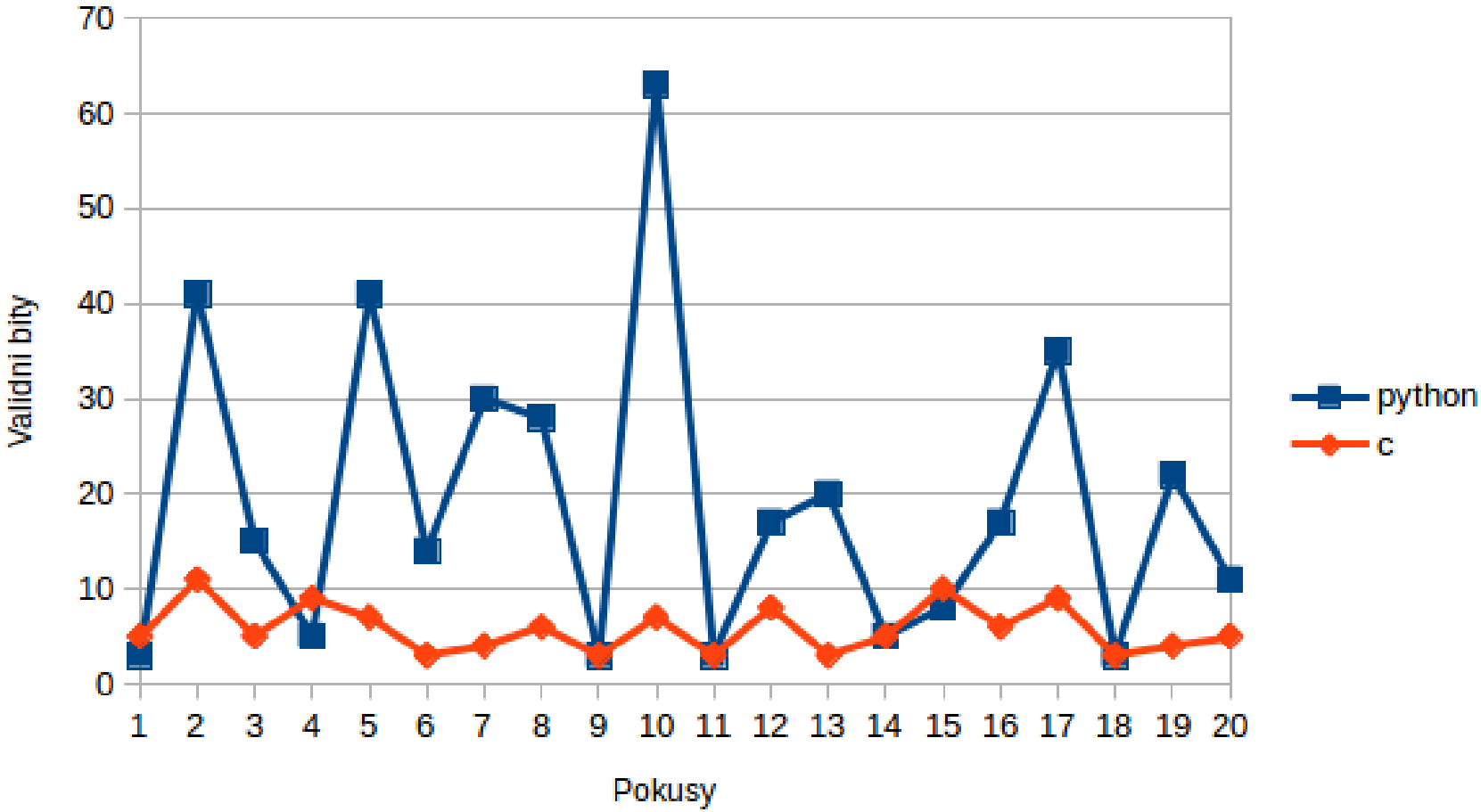

Figure: Průběh algoritmu

Otázky oponenta II

- Rešerše
- Chyby