Příklad na RSA algoritmus

Karel má *veřejný klíč* $(e, n) = (13, 77)$ (e je šifrovací exponent).
Zašifrujte vzkaz pro Karla, jímž je číslo $m = 26$.

Příklad na RSA algoritmus

Karel má *veřejný klíč* $(e, n) = (13, 77)$ (e je šifrovací exponent).
Zašifrujte vzkaz pro Karla, jímž je číslo $m = 26$.
Označme zašifrovaný text jako c. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

Příklad na RSA algoritmus

Karel má *veřejný klíč* $(e, n) = (13, 77)$ (e je šifrovací exponent).
Zašifrujte vzkaz pro Karla, jímž je číslo $m = 26$.
Označme zašifrovaný text jako c. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

$$c \equiv m^e (\mod n)$$

Příklad na RSA algoritmus

Karel má *veřejný klíč* $(e, n) = (13, 77)$ (e je šifrovací exponent).
Zašifrujte vzkaz pro Karla, jímž je číslo $m = 26$.
Označme zašifrovaný text jako c. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

$$c \equiv m^e (\mod n)$$

$$c \equiv 26^{13} (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13}(\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$26^1 \equiv 26 (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$26^1 \equiv 26 (\mod 77)$$

$$26^2 \equiv 676 \equiv -17 (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$26^1 \equiv 26 (\mod 77)$$

$$26^2 \equiv 676 \equiv -17 (\mod 77)$$

$$26^4 \equiv (-17)^2 \equiv -19 (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$
\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}
$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$
\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}
$$

$c \equiv 26^{13}$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$
\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}
$$

$$c \equiv 26^{13} \equiv 26^{8+4+1}$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$
\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}
$$

$$c \equiv 26^{13} \equiv 26^{8+4+1} \equiv -24 \cdot (-19) \cdot 26$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}$$

$$c \equiv 26^{13} \equiv 26^{8+4+1} \equiv -24 \cdot (-19) \cdot 26 \equiv 75 (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $c \equiv 26^{13} (\mod 77)$

Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně:

$$\begin{aligned}
26^1 &\equiv 26 (\mod 77) \\
26^2 &\equiv 676 \equiv -17 (\mod 77) \\
26^4 &\equiv (-17)^2 \equiv -19 (\mod 77) \\
26^8 &\equiv (-19)^2 \equiv -24 (\mod 77)
\end{aligned}$$

$$c \equiv 26^{13} \equiv 26^{8+4+1} \equiv -24 \cdot (-19) \cdot 26 \equiv 75 (\mod 77)$$

$\Rightarrow$ Zašifrovaný text je $c = 75$.

Příklad na RSA algoritmus

Dešifrujte vzkaz pro Karla, jímž je číslo $c = 75$ pomocí jeho *soukromého klíče* $(d, n) = (37, 77)$ (d je dešifrovací exponent).

Příklad na RSA algoritmus

Dešifrujte vzkaz pro Karla, jímž je číslo $c = 75$ pomocí jeho *soukromého klíče* $(d, n) = (37, 77)$ (d je dešifrovací exponent). Označme dešifrovaný text jako m. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

Příklad na RSA algoritmus

Dešifrujte vzkaz pro Karla, jímž je číslo $c = 75$ pomocí jeho *soukromého klíče* $(d, n) = (37, 77)$ (d je dešifrovací exponent). Označme dešifrovaný text jako m. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

$$m \equiv c^d (\mod n)$$

Příklad na RSA algoritmus

Dešifrujte vzkaz pro Karla, jímž je číslo $c = 75$ pomocí jeho *soukromého klíče* $(d, n) = (37, 77)$ (d je dešifrovací exponent). Označme dešifrovaný text jako m. Je to číslo z množiny $\{0, \ldots, 76\}$ splňující vztah :

$$m \equiv c^d (\mod n)$$

$$m \equiv 75^{37} (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37} (\mod 77)$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$75^1 \equiv 75\,(\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned} 75^1 &\equiv 75 (\mod 77) \\ 75^2 &\equiv 5625 \equiv 4 (\mod 77) \end{aligned}$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned} 75^1 &\equiv & & 75\,(\mod 77) \\ 75^2 &\equiv 5625 \equiv & & 4\,(\mod 77) \\ 75^4 &\equiv (4)^2 \equiv & & 16\,(\mod 77) \end{aligned}$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned}
75^1 &\equiv & & 75\,(\mod 77)\\
75^2 &\equiv 5625 \equiv & & 4\,(\mod 77)\\
75^4 &\equiv (4)^2 \equiv & & 16\,(\mod 77)\\
75^8 &\equiv (16)^2 \equiv & & 25\,(\mod 77)
\end{aligned}$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$
\begin{aligned}
75^{1} &\equiv & &\equiv 75\,(\mod 77)\\
75^{2} &\equiv 5625 &&\equiv 4\,(\mod 77)\\
75^{4} &\equiv (4)^{2} &&\equiv 16\,(\mod 77)\\
75^{8} &\equiv (16)^{2} &&\equiv 25\,(\mod 77)\\
75^{16} &\equiv (25)^{2} &&\equiv 9\,(\mod 77)
\end{aligned}
$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$
\begin{aligned}
75^{1} &\equiv & &\equiv 75\,(\mod 77)\\
75^{2} &\equiv 5625 &\equiv 4\,(\mod 77)\\
75^{4} &\equiv (4)^{2} &\equiv 16\,(\mod 77)\\
75^{8} &\equiv (16)^{2} &\equiv 25\,(\mod 77)\\
75^{16} &\equiv (25)^{2} &\equiv 9\,(\mod 77)\\
75^{32} &\equiv (9)^{2} &\equiv 4\,(\mod 77)
\end{aligned}
$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$
\begin{aligned}
75^1 &\equiv & & 75\,(\mod 77)\\
75^2 &\equiv 5625 \equiv & & 4\,(\mod 77)\\
75^4 &\equiv (4)^2 \equiv & & 16\,(\mod 77)\\
75^8 &\equiv (16)^2 \equiv & & 25\,(\mod 77)\\
75^{16} &\equiv (25)^2 \equiv & & 9\,(\mod 77)\\
75^{32} &\equiv (9)^2 \equiv & & 4\,(\mod 77)
\end{aligned}
$$

$m \equiv 75^{37}$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$
\begin{aligned}
75^1 &\equiv & &\equiv 75 \,(\mod 77)\\
75^2 &\equiv 5625 &&\equiv 4 \,(\mod 77)\\
75^4 &\equiv (4)^2 &&\equiv 16 \,(\mod 77)\\
75^8 &\equiv (16)^2 &&\equiv 25 \,(\mod 77)\\
75^{16} &\equiv (25)^2 &&\equiv 9 \,(\mod 77)\\
75^{32} &\equiv (9)^2 &&\equiv 4 \,(\mod 77)
\end{aligned}
$$

$$m \equiv 75^{37} \equiv 75^{32+4+1}$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned}
75^1 &\equiv && 75 (\mod 77)\\
75^2 &\equiv 5625 \equiv && 4 (\mod 77)\\
75^4 &\equiv (4)^2 \equiv && 16 (\mod 77)\\
75^8 &\equiv (16)^2 \equiv && 25 (\mod 77)\\
75^{16} &\equiv (25)^2 \equiv && 9 (\mod 77)\\
75^{32} &\equiv (9)^2 \equiv && 4 (\mod 77)
\end{aligned}$$

$$m \equiv 75^{37} \equiv 75^{32+4+1} \equiv 4 \cdot 16 \cdot 75$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned}
75^1 &\equiv & & 75 (\mod 77)\\
75^2 &\equiv 5625 \equiv & & 4 (\mod 77)\\
75^4 &\equiv (4)^2 \equiv & & 16 (\mod 77)\\
75^8 &\equiv (16)^2 \equiv & & 25 (\mod 77)\\
75^{16} &\equiv (25)^2 \equiv & & 9 (\mod 77)\\
75^{32} &\equiv (9)^2 \equiv & & 4 (\mod 77)
\end{aligned}$$

$$m \equiv 75^{37} \equiv 75^{32+4+1} \equiv 4 \cdot 16 \cdot 75 \equiv 26 (\mod 77)$$

Příklad na RSA algoritmus

Řešíme kongruenci $m \equiv 75^{37}(\mod 77)$ Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně:

$$\begin{aligned}
75^1 &\equiv & &\equiv 75\,(\mod 77)\\
75^2 &\equiv 5625 &&\equiv 4\,(\mod 77)\\
75^4 &\equiv (4)^2 &&\equiv 16\,(\mod 77)\\
75^8 &\equiv (16)^2 &&\equiv 25\,(\mod 77)\\
75^{16} &\equiv (25)^2 &&\equiv 9\,(\mod 77)\\
75^{32} &\equiv (9)^2 &&\equiv 4\,(\mod 77)
\end{aligned}$$

$$m \equiv 75^{37} \equiv 75^{32+4+1} \equiv 4 \cdot 16 \cdot 75 \equiv 26\,(\mod 77)$$

$\Rightarrow$ Dešifrovaný text je $m = 26$.