Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $\gcd(e, \varphi(n))$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1))$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6)$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6) = \gcd(e, 60)$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6) = \gcd(e, 60) = 1$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6) = \gcd(e, 60) = 1$$

     Vyhovuje například $e = 13$,

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6) = \gcd(e, 60) = 1$$

     Vyhovuje například $e = 13$, což snadno ověříme pomocí Euklidova algoritmu.

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

1. Nejprve vytvoříme veřejný klíč (e, n).
   - $n = pq = 11 \cdot 7 = 77$
   - Hodnotu e určíme tak, aby platilo $\gcd(e, \varphi(n)) = 1$, tj.:

     $$\gcd(e, \varphi(n)) = \gcd(e, (p-1)(q-1)) = \gcd(e, 10 \cdot 6) = \gcd(e, 60) = 1$$

     Vyhovuje například $e = 13$, což snadno ověříme pomocí Euklidova algoritmu.

$$\Rightarrow \quad \text{veřejný klíč } (e, n) = (13, 77).$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)
   - Hodnotu d určíme tak, aby platilo $ed \equiv 1(\mod \varphi(n))$, tj.:

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)
   - Hodnotu d určíme tak, aby platilo $ed \equiv 1 \pmod{\varphi(n)}$, tj.:

$$13d \equiv 1 \pmod{60}.$$

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)
   - Hodnotu d určíme tak, aby platilo $ed \equiv 1 \pmod{\varphi(n)}$, tj.:

$$13d \equiv 1 \pmod{60}.$$

Hledáme řešení této lineární kongruence v množině $\{1, 2, \ldots, 59\}$.

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)
   - Hodnotu d určíme tak, aby platilo $ed \equiv 1 (\mod \varphi(n))$, tj.:

$$13d \equiv 1 (\mod 60).$$

Hledáme řešení této lineární kongruence v množině $\{1, 2, \ldots, 59\}$. Je jím $d = 37$.

Příklad na generaci klíčů pro RSA algoritmus

Jsou zadány prvočísla $p = 11$ a $q = 7$. Nalezněte nějaký *veřejný* a *soukromý klíč*.

2. Nalezneme soukromý klíč (d, n).
   - $n = 77$ (to jsme určili už při hledání veřejného klíče.)
   - Hodnotu d určíme tak, aby platilo $ed \equiv 1 (\mod \varphi(n))$, tj.:

$$13d \equiv 1 (\mod 60).$$

Hledáme řešení této lineární kongruence v množině $\{1, 2, \ldots, 59\}$. Je jím $d = 37$.

$$\Rightarrow \quad \text{soukromý klíč } (d, n) = (37, 77).$$