Jak postupovat v příkladu s RSA?
Pan A posílá zprávu panu B, aby to ovšem mohl udělat, musel pan B něco udělat předem.

1. Pan B si vzal dvě prvočísla p, q a vynásobil je, $n = pq$.
2. Pan B dále spočítal $\varphi(n)$ a to snadno, protoze zná prvočíselný rozklad čísla n, takže
$$\varphi(n) = (p-1)(q-1).$$
3. Pan B si dále zvolí nějaké číslo e menší než $\varphi(n)$, které je s ním nesoudělné, $(e, \varphi(n)) = 1$.
4. Pan B si ještě dopočítá hodnotu d, což je inverze k e modulo $\varphi(n)$, tedy $e \cdot d \equiv 1 \ (mod\ \varphi(n))$.
5. Poslední krok je, že předá veřejnosti (a tedy i panu A) veřejný klíč, což je dvojice n, e (e se nazývá šifrovací exponent).

Nyní tedy opravdu pan A posílá zprávu panu B, přečte si, že B zveřejnil n, e. Chce poslat zprávu M, tak ji zašifruje jako C, přičemž platí $C \equiv M^e \ (mod\ n)$. Toto C pošle panu B.

Pan B se již připravil na dešifrování, když si spočítal číslo d, dešifrovací exponent. Dostal zašifrovanou zprávu ve formě čísla C. Spočítá $C^d \equiv M \ (mod\ n)$.

Nyní tedy nějaké skutečné („minipísemkové“) zadání.

Příklad 1. *Šifrou RSA s veřejným klíčem $n = 95$, $e = 55$ bylo posláno číslo $C = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, \ldots, 95\}$.*

Řešení. Abychom prolomili šifru, potřebujeme se seznámit s prvočísly p, q. V tomto případě snadno spočítáme, že
$$n = 95 = 5 \cdot 19 = p \cdot q.$$
Díky tomu dopočítáme i hodnotu Eulerovy funkce pro n, tedy
$$\varphi(n) = (5-1)(19-1) = 4 \cdot 18 = 72.$$
Podíváme se, že $e = 55$, takže počítáme $55d \equiv 1 \ (mod\ 72)$. Zde pozor na ten modul, který je $\varphi(n)$ a nikoliv n, v tom se často dělá chyba.

Inverzi spočítáme například takto: $72d \equiv 0 \ (mod\ 72)$

$55d \equiv 1 \ (mod\ 72)$
$17d \equiv -1 \ (mod\ 72)$
$4d \equiv 4 \ (mod\ 72)$
$d \equiv -17 \ (mod\ 72)$
$0d \equiv 4 + 4 \cdot 17 \equiv 72 \equiv 0 \ (mod\ 72)$ Takže $d \equiv -17 \equiv 55 \ (mod\ 72)$. Nyní dešifrujeme: $M \equiv C^d \equiv 42^{55} \ (mod\ 95)$. Zde je vhodné (opět díky znalosti prvočíselného rozkladu) řešit umocnění modulo 5 a pak modulo 19.
$42^{55} \equiv ? \ (mod\ 5)$

$2^{55} \equiv (2^4)^{13} \cdot 2^3 \equiv 1^{13} \cdot 8 \equiv 3 \ (mod\ 5)$
$M \equiv 3 \ (mod\ 5)$ Nyní modulo 19. $42^{55} \equiv ? \ (mod\ 19)$

$4^{55} \equiv 2^{110} \equiv (2^{18})^6 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \ (mod\ 19)$
$M \equiv 4 \ (mod\ 19)$

(Použili jsme Malou Fermatovu větu.) Z toho plyne, že $M = 3 + 5t$ pro nějaké celé číslo t. Takže dosadíme do druhé kongruence
$3 + 5t \equiv 4 \ (mod\ 19)$

$5t \equiv 1 \ (mod\ 19)$

$t \equiv 4 \ (mod\ 19)$
Dopočítáme $M = 3+5(4+19k)$, kde $k \in \mathbb{Z}$, tedy $M = 3+20+95k = 23+95k$. Protože jsme chtěli dostat číslo v intervalu $[1, 95]$, tak jsme hotovi, řešením je

$$M = 23.$$

□

Vyřešme ještě jeden příklad, stručněji.

Příklad 2. *Šifrou RSA s veřejným klíčem $n = 115$, $e = 15$ bylo posláno číslo $C = 47$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, \ldots, 115\}$.*

Řešení. $n = 115 = 5 \cdot 23, \varphi(n) = 4 \cdot 22 = 88$

$$\begin{aligned}
15d &\equiv 1 \ (mod\ 88)\\
15d &\equiv 1 + 2 \cdot 88 \equiv 177 \ (mod\ 88)\\
15d &\equiv 177 \equiv 3 \cdot 59 \ (mod\ 88)\\
5d &\equiv 59 \ (mod\ 88)\\
5d &\equiv 59 + 2 \cdot 88 \equiv 235 \equiv 5 \cdot 47 \ (mod\ 88)\\
d &\equiv 47 \ (mod\ 88)
\end{aligned}$$

$$\begin{aligned}
M &\equiv 47^{47} \ (mod\ 115)\\
M &\equiv 47^{47} \ (mod\ 5)\\
M &\equiv 2^{47} \ (mod\ 5)\\
M &\equiv (2^4)^{11} \cdot 2^3 \equiv 8 \equiv 3 \ (mod\ 5)\\
M &\equiv 3 \ (mod\ 5)\\
M &\equiv 47^{47} \ (mod\ 23)\\
M &\equiv 1^{47} \equiv 1 \ (mod\ 23)\\
3 + 5t &\equiv 1 \ (mod\ 23)\\
5t &\equiv 1 + 23 - 3 \equiv 21 \ (mod\ 23)\\
5t &\equiv 21 - 46 \equiv -25 \ (mod\ 23)\\
t &\equiv -5 \ (mod\ 23)\\
M &= 3 + 5(-5 + 23k) = 3 - 25 + 115k = -22 + 115k = (115 - 22) + 115k = 93\\
M &= 93.
\end{aligned}$$

Pro kontrolu si lze ještě spočítat, že $93^{15} \equiv 47 \ (mod\ 115)$.

□