Textbook RSA encryption:

- public key: **(N,e)** Encrypt: $\mathbf{c} \leftarrow \mathbf{m}^{\mathbf{e}}$ (in Z_N)
- secret key: **(N,d)** Decrypt: $\mathbf{c}^{\mathbf{d}} \longrightarrow \mathbf{m}$

Insecure cryptosystem !!

- Is not semantically secure and many attacks exist

⇒ The RSA trapdoor permutation is not an encryption scheme !