

The Basic Model of Public Key Systems

Communication model:

1. Alice generates a pair of keys: **e** (public key) and **d** (private key).
2. She keeps **d** secret, but makes **e** public.
3. If Bob wants to send a message to Alice, he uses Alice's public key **e**.
4. Based on the equation $c = E(e, m)$, only Alice can decrypt c using her private key, with $m = D(d, c)$, where m is the message.
5. If anyone else wants to send a message to Alice, they can also use her public key **e**.

The system is secure from a decryption perspective because only Alice can decrypt the message, but Alice can never be sure if Bob sent the message, as the public key **e** can be used by anyone.

From:

<https://edu.iit.uni-miskolc.hu/> - Institute of Information Science - University of Miskolc

Permanent link:

https://edu.iit.uni-miskolc.hu/tanszek:oktatas:techcomm:rsa_encryption?rev=1728306857

Last update: 2024/10/07 13:14

