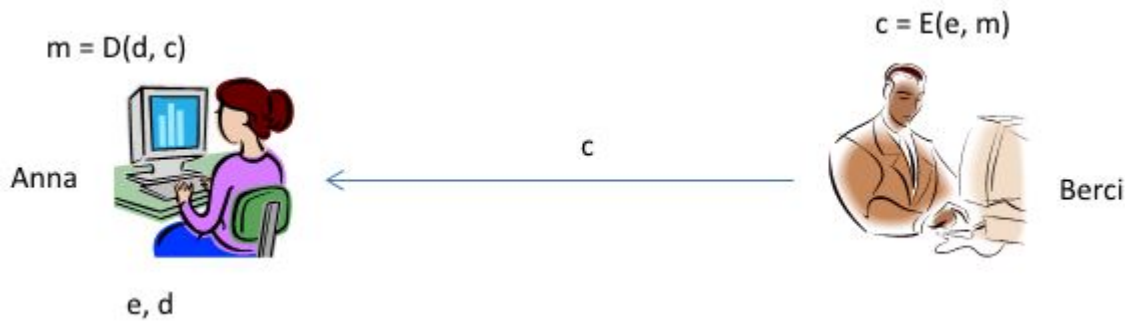


Nyilvános kulcsú rendszerek



A kommunikáció alapmodellje:

1. Anna készít egy **e,d** kulcspárt.
2. **d**-t titokban tartja, **e**-t nyilvánosságra hozza.
3. Ha Berci üzeni akar Annának, akkor Anna (**e**) nyilvános kulcsát használja.
4. **c=E(e , m)** alapján **c**-t csak Anna tudja visszafejteni, **m = D(d,c)** alkalmazásával.
5. Ha más is üzeni kíván Annának, akkor használhatja az ő nyilvános (**e**) kulcsát.

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

Permanent link: https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:nyilvanos_kulcsu_rendszerek?rev=1731519454

Last update: 2024/11/13 17:37

