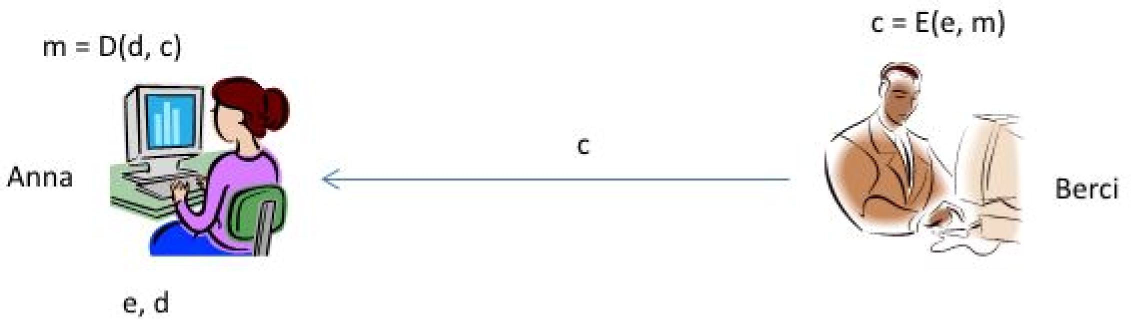
Nyilvános kulcsú rendszerek



A kommunikáció alapmodellje:

1. Anna készít egy **e,d** kulcspárt.
2. **d**-t titokban tartja, **e**-t nyilvánosságra hozza.
3. Ha Berci üzenni 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 üzenni kíván Annának, akkor használhatja az ő nyilvános (**e**) kulcsát.