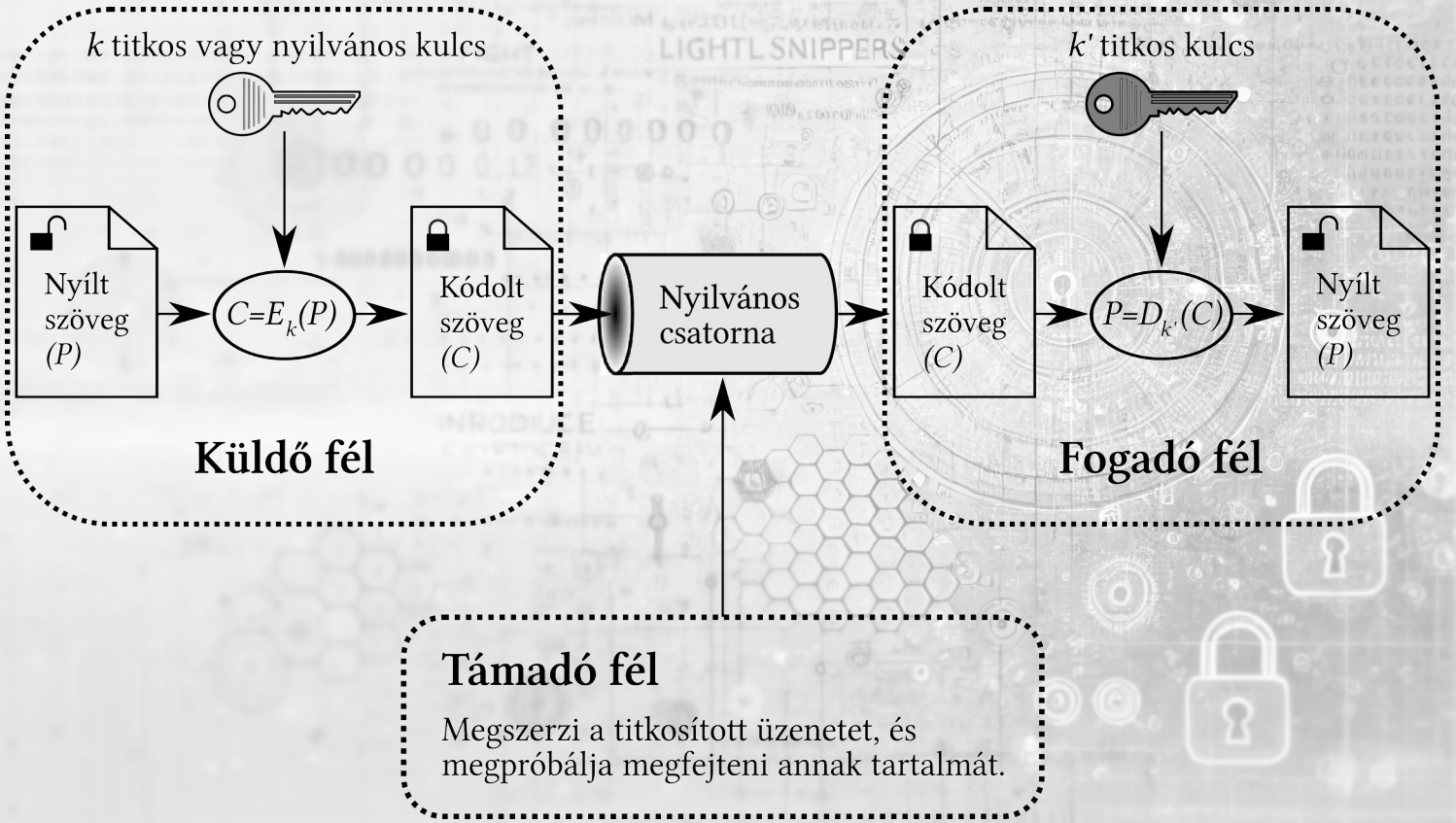

1
Kriptográfiai
alapfogalmak

- Kriptográfia – a titkosítás tudománya
  - titkosítási rendszerek felépítése
  - titkosítási rendszerek biztonsági elemzése (kriptoanalízis)
  - digitális aláírások
  - hitelesítések
  - hash függvények
  - hálózati protokollok biztonsága
  - stb.

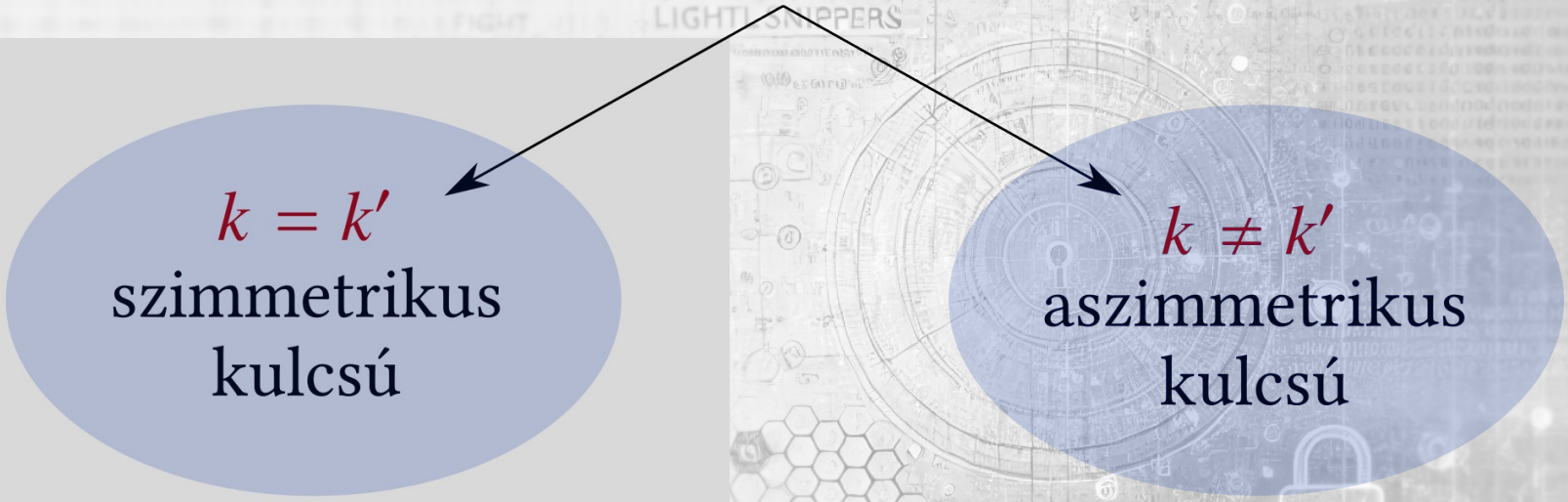
Egy titkosítási rendszer sémája



Egy titkosítási rendszer sémája

- E_k – titkosító eljárás, ami *kódolja* (*titkosítja* vagy *rejtjelezi*) a P üzenetet
- $D_{k'}$ – dekódoló eljárás, ami *dekódolja* (*megfejti*) a C kódolt üzenetet (figyelem: dekódol $\neq$ feltör)
- k – kódoláshoz használt kulcs
- k' – dekódoláshoz használt kulcs

Kriptorendszer



- helyettesítő kódok
- átrendezéses (keveréses) kódok
- helyettesítő-átrendező (hibrid) kódok

Kerckhoffs-elv

1. Ha elméletileg nem is, a rendszernek gyakorlatilag feltörhetetlennek kell lennie.
2. A módszerrel titkosított üzenetek biztonsága ne függjön magának a módszernek a titkosságától: a módszer leírását ugyanis az ellenség is megszerezheti.
3. A kulcs könnyen megjegyezhető, továbbítható és változtatható kell, hogy legyen (anélkül, hogy azt papírra kellene írni).

Kerckhoffs-elv

4. A kódolt üzenetnek olyan formája legyen, hogy azt táviraton továbbítani lehessen.
5. A rendszer által használt segédeszközök hordozhatóak kell, hogy legyenek, és a kódolás/dekódolás műveletét egyetlen személynek is el kell tudnia végezni.
6. A módszer használata legyen egyszerű (ne kelljen túl sok szabályt, lépést megjegyezni), szellemileg ne terhelje túl használóját.

Támadások fajtái (kriptoanalízis)

1. Csak a kódolt üzenet ismeretén alapuló támadás: a támadónak csak a kódolt üzenetekhez van hozzáférése, semmit sem tud az eredeti üzenetek tartalmáról vagy a titkosításhoz használt kulcsról.
2. Nyílt szöveg ismeretén alapuló támadás: a támadó ismer bizonyos nyílt üzeneteket a megfelelő kódolt üzenetekkel együtt, ezek az információk adottak (például egy kém vagy egy titkos ügynök szerzi be neki).

Támadások fajtái (kriptoanalízis)

3. Választható nyílt szövegen alapuló támadás: a támadó akármilyen általa választott nyílt üzenetet tud titkosítani (vagy titkosíttatni) a módszerrel (tehát gyakorlatilag ismeri és használja E_k-t, így ő maga tudja előállítani a (P, C) párokat).
4. Választható titkosított üzeneten alapuló támadás: a támadó akármilyen általa választott titkosított üzenetnek megkaphatja a dekódolt változatát (tehát gyakorlatilag ismeri és használja $D_{k'}$-t) anélkül, hogy a k' kulcsot ismerné.

Kimerítő kulcskeresés

- Bármely kriptorendszer titkos kulcsait próbálgatással meg lehet találni (elvileg).
- Szisztematikusan az összes lehetséges kulcsot végig kell próbálni (legrosszabb esetben).
- „Brute force” módszer