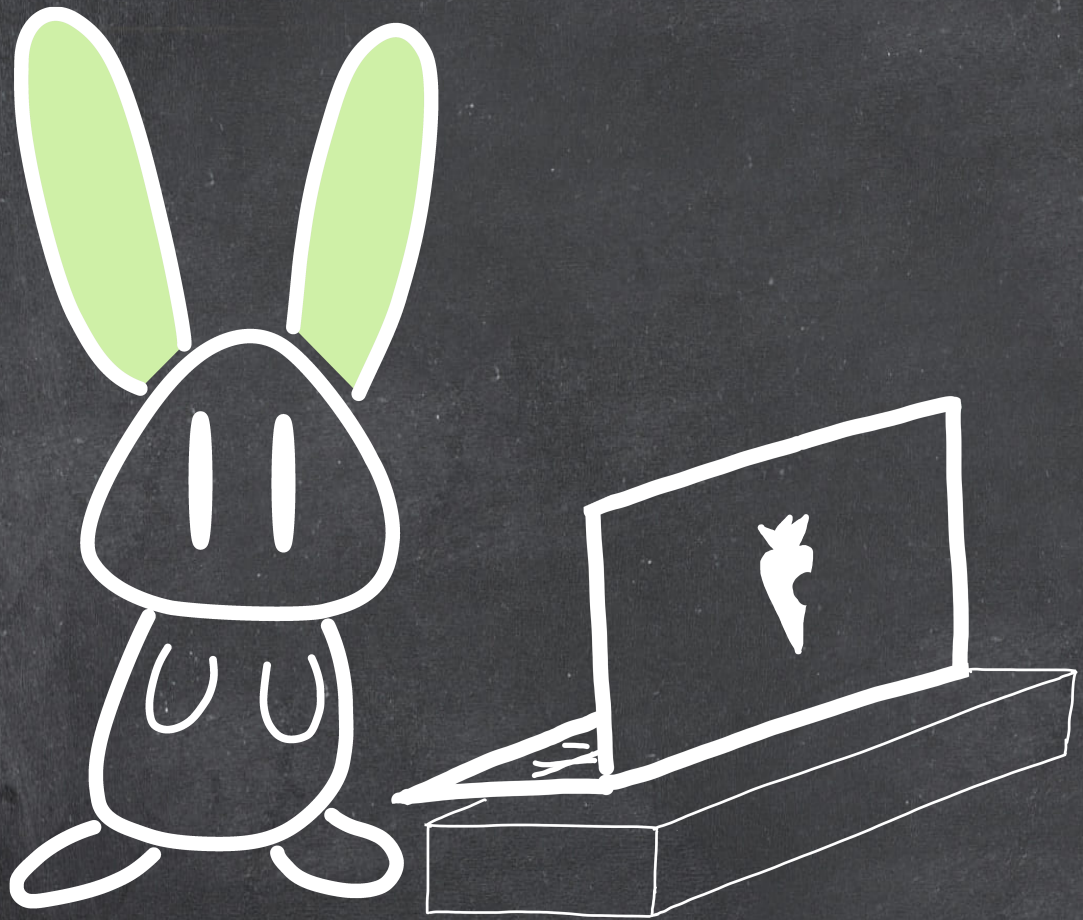
KOMBINATORIKA

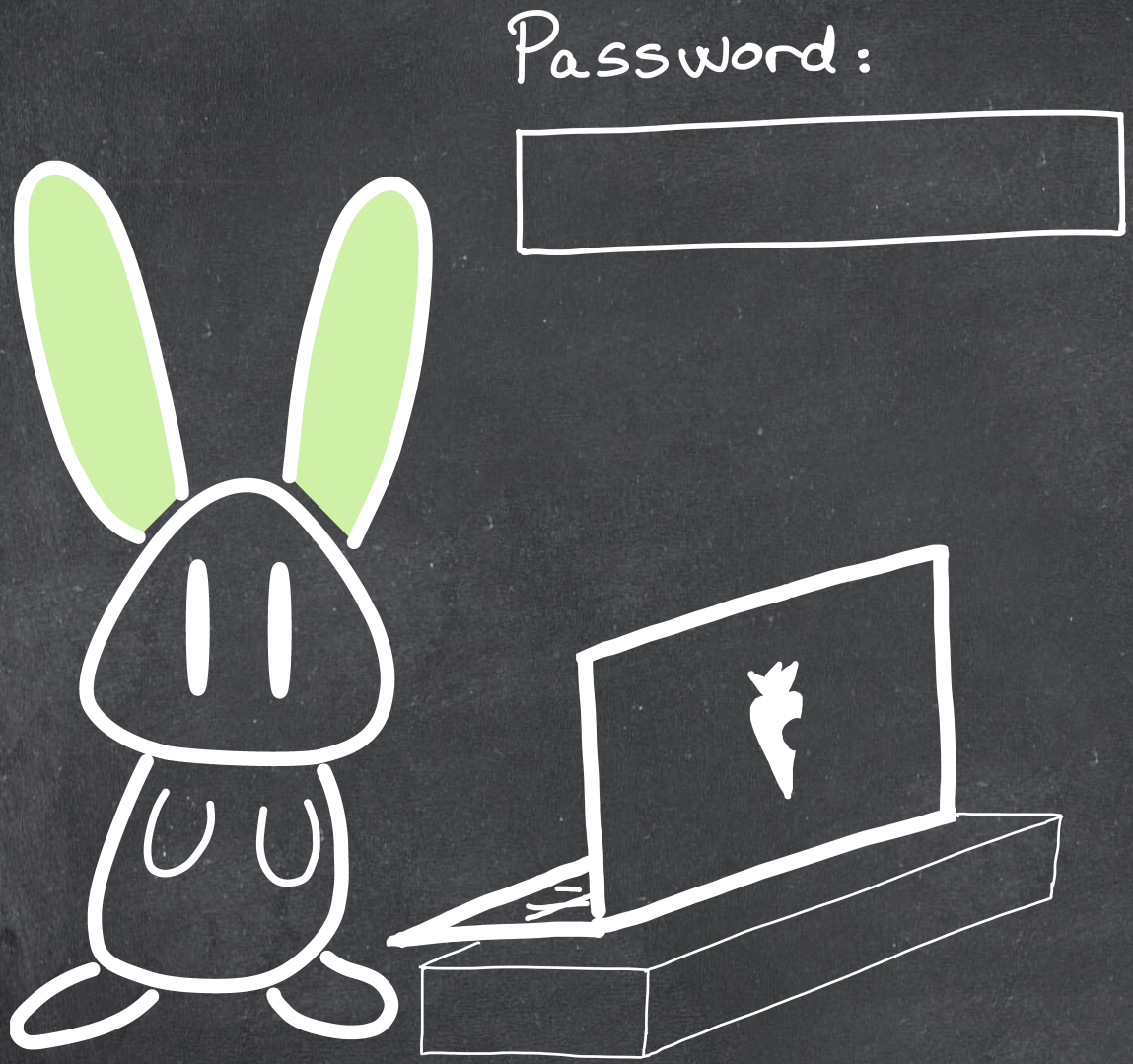
összeszámlálási feladatok

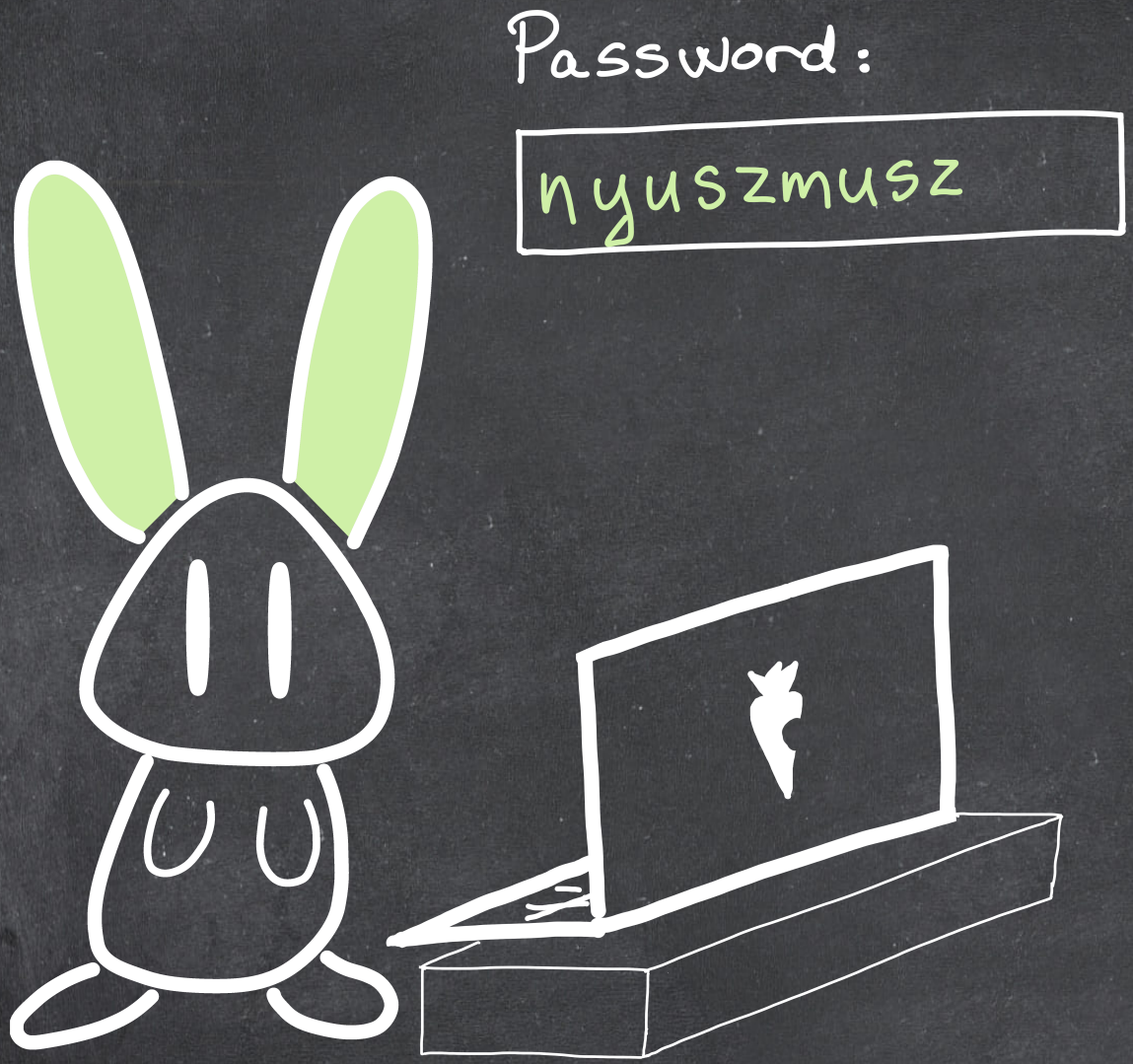
Szakács Nóra

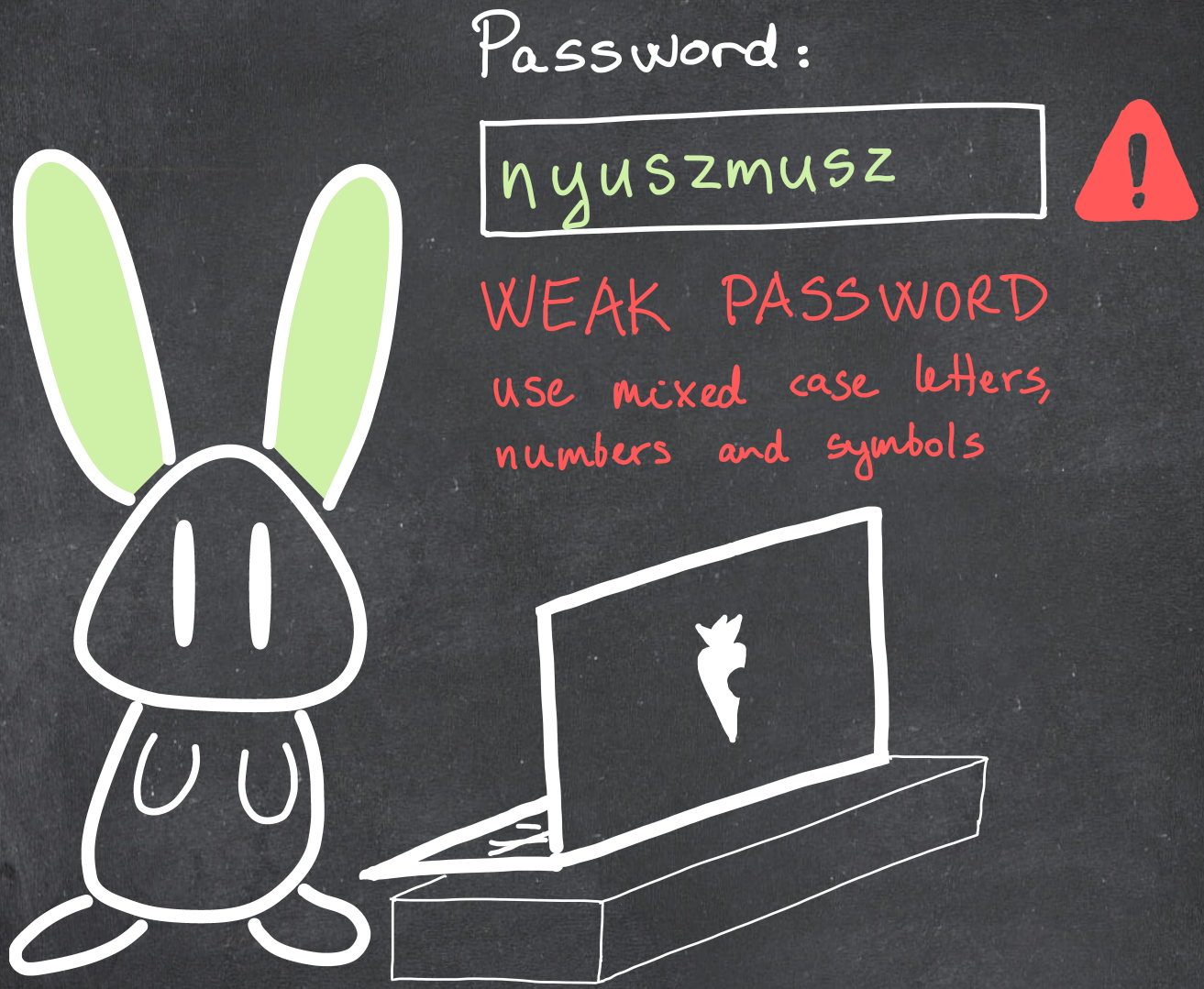
SZTE Bolyai Intézet

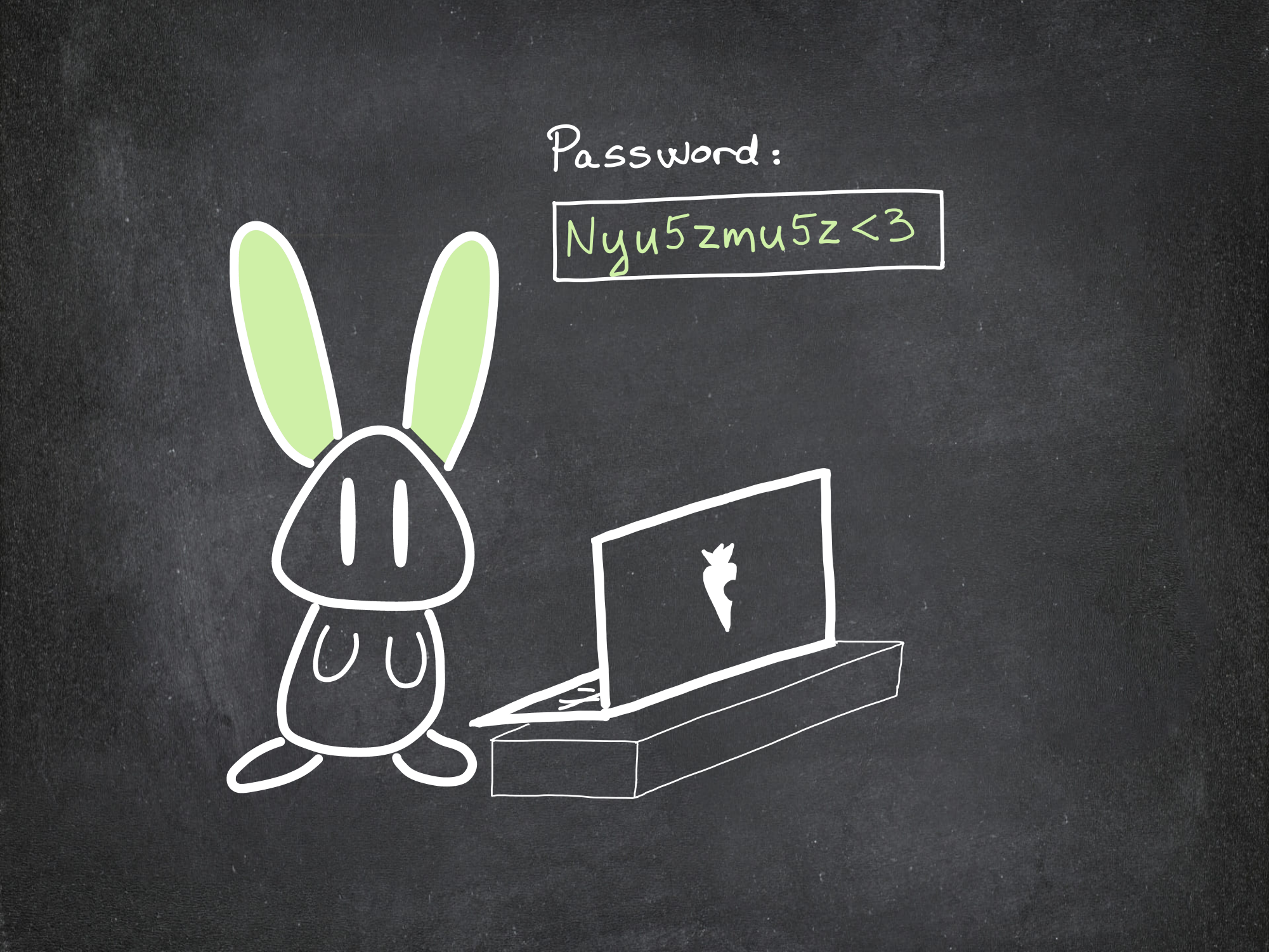
Tartalom




Password:


Password:
nyuszmusz


Password:
nyuszmusz
WEAK PASSWORD
use mixed case letters,
numbers and symbols


Password:
Nyu5zmu5z<3

Találgass!

Mi a biztonságosabb? Egy 8-karakteres, kis- és nagybetűkből, számokból és szimbólumokból álló véletlenszerű jelszó, vagy egy 12-karakteres, csupa kisbetűből álló véletlenszerű jelszó?
Mennyivel biztonságosabbak ezek, mint a gyenge 8-karakteres kisbetűs jelszó?

kisbetűk száma: 26
nagybetűk száma: 26
számjegyek száma: 10
szimbólumok száma: 16

8 karakter hosszú kisbetűs jelszavak száma: 26^8
8 karakter hosszú vegyes karakteres jelszavak száma: $(26+26+10+16)^8 = (3 \cdot 26)^8 = 3^8 \cdot 26^8$
12 karakter hosszú kisbetűs jelszavak száma: $26^{12} = 26^4 \cdot 26^8$

Ha	26^8	$\longleftrightarrow$	1 óra
akkor	$3^8 \cdot 26^8$	$\longleftrightarrow$	kb. 9 hónap
és	$26^4 \cdot 26^8$	$\longleftrightarrow$	kb. 52 év

Brute force attack vs dictionary attack

A legtöbb jelszó gyökere értelmes szó.

- egy átlagos értelmező kéziszótár bejegyzései: $\sim$ 200000 szó
- egy átlagember teljes szókicse: $\sim$ 20000 szó
- gyakran használt szavak: $\sim$ 5000 szó

$$
\begin{aligned}
26^8 &\longleftrightarrow \text{1 óra} \\
200000 &\longleftrightarrow \text{4 ms} \\
20000 &\longleftrightarrow \text{0,4 ms} \\
5000 &\longleftrightarrow \text{0,1 ms}
\end{aligned}
$$

Brute force attack vs dictionary attack

A legtöbb jelszó gyökere értelmes szó.

- egy átlagos értelmező kéziszótár bejegyzései: ~ 200000 szó
- egy átlagember teljes szókicse: ~ 20000 szó
- gyakran használt szavak: ~ 5000 szó

$$
\begin{aligned}
26^8 &\longleftrightarrow \text{10000 óra} \\
200000 &\longleftrightarrow \text{40 s} \\
20000 &\longleftrightarrow \text{4 s} \\
5000 &\longleftrightarrow \text{1 s}
\end{aligned}
$$

nyuszmusz vs Nyu5zmu5z<3

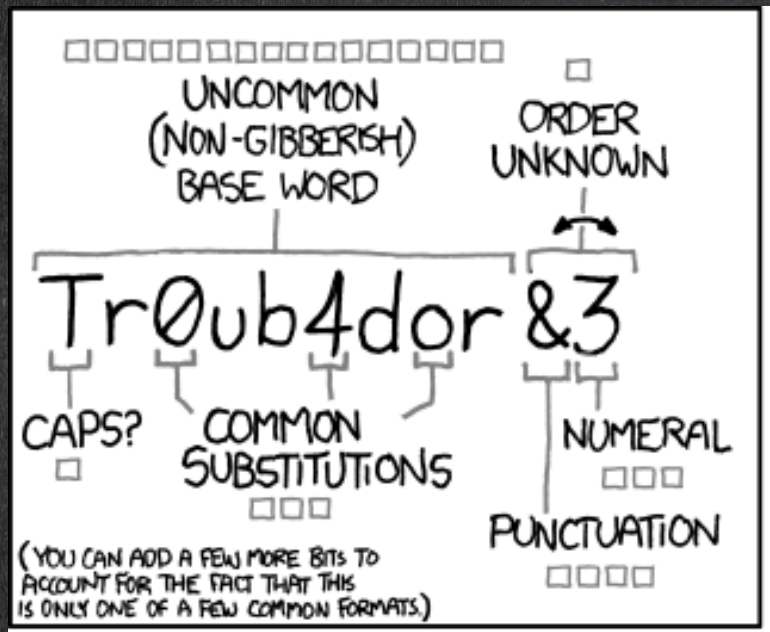
A tipikus ‘biztonságos’ jelszó:

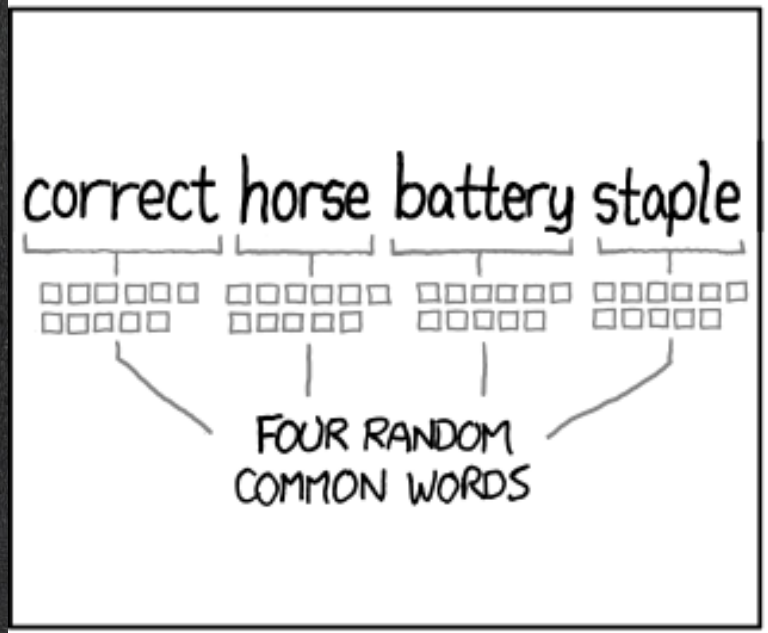
1. értelmes kisbetűs szó
2. néhány szótag kezdőbetűjét átírjuk nagyra
3. néhány betűt átírunk számra, pl. $o \to 0, i \to 1, s \to 5, e \to 3$
4. $1 - 2$ szimbólum vagy szám a végére

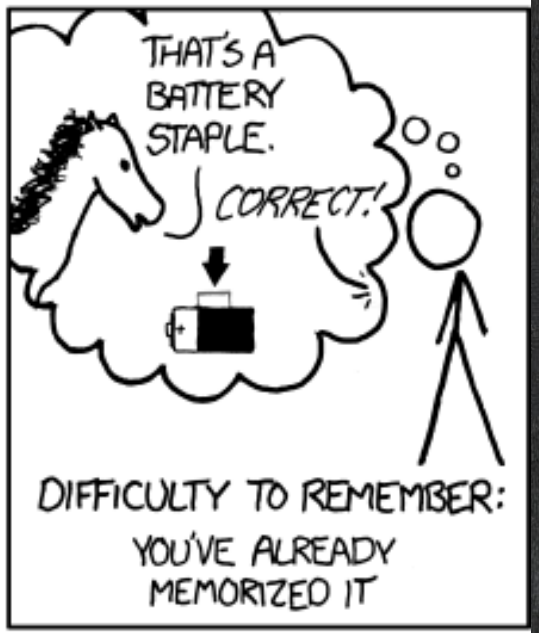
A nyuszmusz tipikus módosításainak száma:

$$2^2 \cdot 2^4 \cdot (26 + 26^2) = 44928$$

$$\begin{aligned} 26^8 &\longleftrightarrow \text{10000 óra} \\ 200000 &\longleftrightarrow \text{40 s} \\ 20000 &\longleftrightarrow \text{4 s} \\ 5000 &\longleftrightarrow \text{1 s} \\ 44928 &\longleftrightarrow \text{10 s} \\ 20000 \cdot 44928 &\longleftrightarrow \text{50 óra} \end{aligned}$$







THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Tartalom

Összegzési szabály

Ha az összes lehetséges esetet esetszétválasztással számláljuk, akkor

$$\text{összes lehetőség} = \sum \text{lehetőségek esetenként}$$

Szorzási szabály

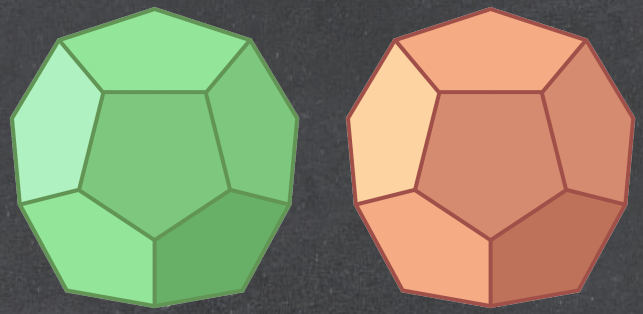
Ha minden lehetséges esetet lebontunk lehetőségek (ugyanannyi!) egymásutánjára, akkor

$$\text{összes lehetőség} = \prod \text{független lehetőségek}$$

Feladat

Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka?

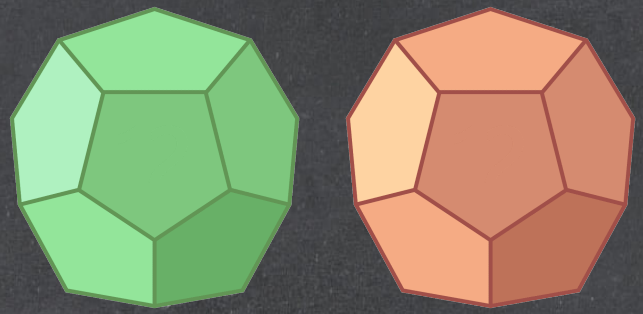
Megoldás:



Feladat

Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka, ha tudjuk, hogy a két dobás eredménye különböző?

Megoldás:



Feladat

Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka, ha tudjuk, hogy az egyik dobás biztosan páros?

Feladat

Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka, ha tudjuk, hogy az egyik dobás biztosan páros?

Megoldás: esetszétválasztás

1. eset: a zöld dobás páros

2. eset: a zöld dobás páratlan

Feladat

Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka, ha tudjuk, hogy az egyik dobás biztosan páros?

Megoldás: esetszétválasztás

1. eset: a zöld dobás páros

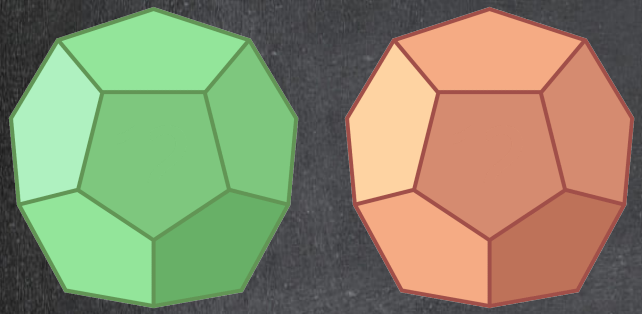
2. eset: a zöld dobás páratlan

Feladat

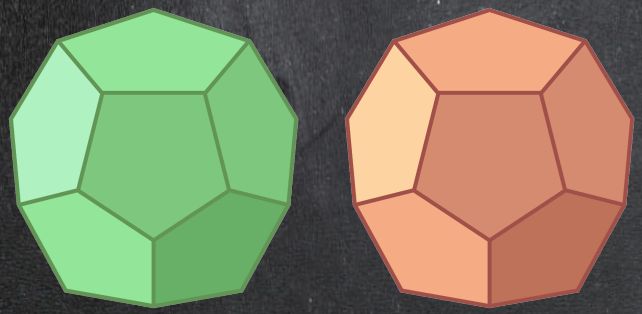
Két 12-oldalú dobókockával dobunk. Hányféle pozícióban landolhat a két kocka, ha tudjuk, hogy az egyik dobás biztosan páros?

Megoldás: esetszétválasztás

1. eset: a zöld dobás páros



2. eset: a zöld dobás páratlan



Kivonási és osztási szabály

Az összegzési és szorzási szabályt visszafele is lehet alkalmazni:

1. ha olyan eseteket is számolunk, amit nem kellene, ezeknek a számát kivonjuk
2. ha az összes esetet többször (ugyanannyiszor!) számoljuk, akkor a megfelelő számmal leosztunk

Feladat

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

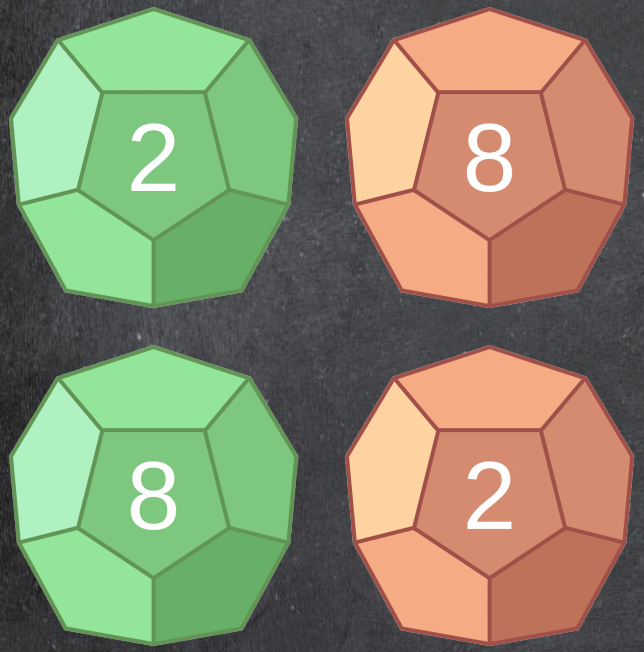
Feladat

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

Megoldás:

Ha számon tartjuk, melyik kockával dobtuk melyik számot: 12^2 lehetőség.

Így minden számkombinációt kétszer számolunk:



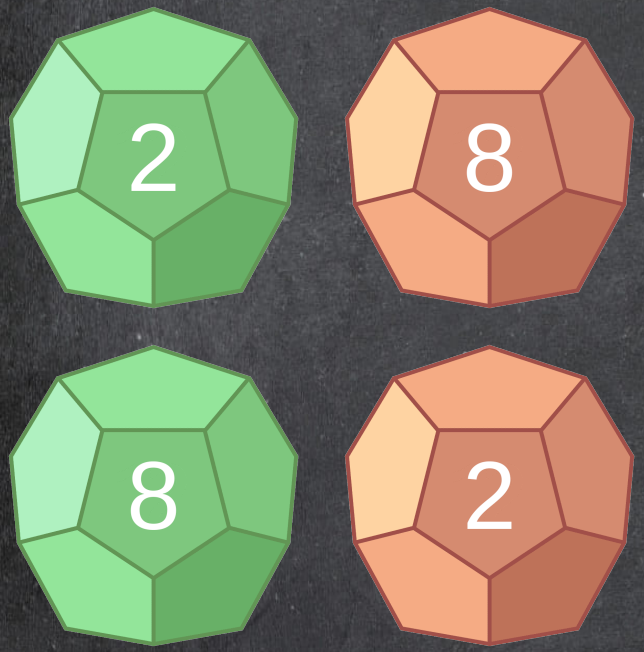
Feladat

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

Megoldás:

Ha számon tartjuk, melyik kockával dobtuk melyik számot: 12^2 lehetőség.

Így minden számkombinációt kétszer számolunk:



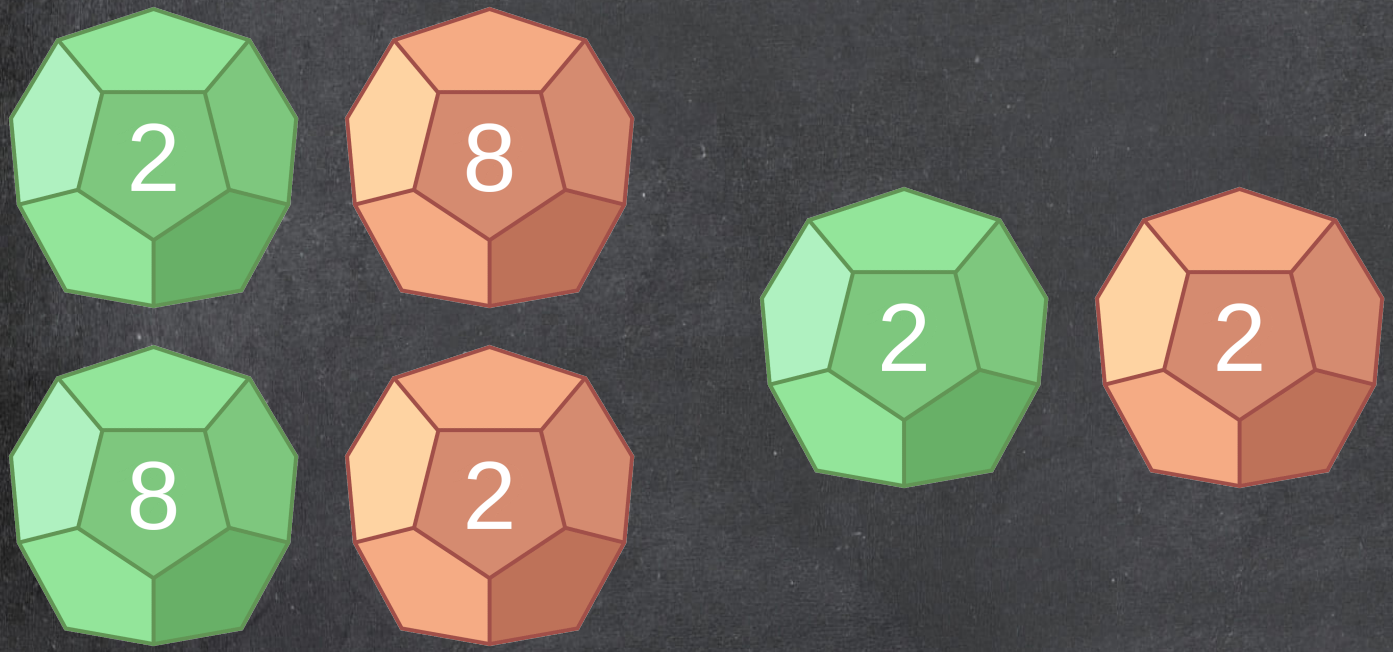
Feladat

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

Megoldás:

Ha számon tartjuk, melyik kockával dobtuk melyik számot: 12^2 lehetőség.

Így minden számkombinációt kétszer számolunk:



Feladat

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

Jó megoldás: esetszétválasztás

1. eset: a két dobás különböző

2. eset: a két dobás egyforma

Tartalom

Permutációk

Hányféleképp lehet n különböző elemet (számot, betűt, üveggolyót, kiskutyát, bármi egyebet) sorbarendezni?

Válasz: $n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Precíz megfogalmazás:
Legyen A egy n-elemű halmaz (pl. $A = \{1, 2, \ldots, n\}$).

A elemeinek egy sorbarendezése, azaz permutációja: $A \to A$ bijekció

Tétel
Egy n-elemű halmaz permutációinak száma $n!$.

Megjegyzés: $0! = 1$

Feladat

Hányféleképp lehet a MATEMATIKA szó betűit sorbarendezni?

Megoldás:

A,A,A,E,I,K,M,M,T,T

Vigyázat, a betűk nem különbözők!
Az

A,A,A,E,I,K,M,M,T,T

betűket 10!-féleképp lehet sorbaállítani. Hányszor számoltunk egy esetet?

- a 3 db A sorrendje: 3!
- a 2 db M sorrendje: 2!
- a 2 db T sorrendje: 2!

Ismétléses permutációk

Tétel

Ha adott n elem, amelyek között pontosan r különböző jelenik meg, és ezekből rendre $k_1, k_2, \ldots, k_r$ darab van (tehát $n = k_1 + \ldots + k_r$), akkor az n elemet

$$\frac{n!}{k_1!k_2!\cdots k_r!}$$

-féleképp lehet sorbanrendezni.

Példa

MATEMATIKA:

$n = 10$,

$k_1 = 3$ (A), $k_2 = 2$ (M), $k_3 = 2$ (T),

$k_4 = k_5 = k_6 = 1$ (E,I,K)

Tartalom

Az alapkérdés

Hányféleképp lehet
n különböző elem közül k-t kiválasztani?

1. Számít a kiválasztás sorrendje?
   - IGEN: variáció
   - NEM: kombináció
2. Választhatjuk-e az elemeket többször?
   - IGEN: ismétléses
   - NEM: ismétlés nélküli

Variációk

Feladat

Hányféleképp választható ki k (nem feltétlenül különböző) elem n elem közül, ha a kiválasztás sorrendje számít?

Válasz: n^k

Tétel

Egy n-elemű halmaz elemeiből n^k számú k hosszú sorozat képezhető.

Feladat

Hányféleképp választható ki k különböző elemet n elem közül, ha a kiválasztás sorrendje számít?

Válasz: $n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$

Tétel

Egy n-elemű halmaz különböző elemeiből $\frac{n!}{(n-k)!}$ számú k hosszú sorozat képezhető.

Ismétlés nélküli kombináció

Feladat

Hányféleképp választható ki k különböző elem n elem közül, ha a kiválasztás sorrendje nem számít?

Ha a sorrend számítana: $n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$

k különböző elem lehetséges sorrendje: $k!$

Válasz:

$$\frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Tétel

Egy n-elemű halmaznak $\binom{n}{k}$ számú k-elemű részhalmaza van.

Megjegyzés: $\binom{n}{k} = \binom{n}{n-k}$

Feladat

Azon év márcusában, melyet Nem Nevezünk Nevén, Adorján elmegy a boltba vécépapírért, lisztért és babkonzervért, mert már csak fél évre elegendő a család készlete. Összesen 10 árucikket szeretne venni (több hely nincs a szekrényben), a pontos mennyiségekről a készletet látva dönt majd. Hányféleképp választhat? (Nem biztos, hogy vesz mindhárom termékből.)

Nem akarja, hogy a kasszás ferde szemmel nézzen rá, úgyhogy magával viszi a három fiát, hogy ők fizessék ki külön-külön a háromféle árut.
A boltban hatalmas a tömeg. A fiúk előre beállnak a kasszasorba, amíg Adorján összeszedi a cuccokat. A szalaghoz érve lefoglalnak maguknak egy akkora részt, amin elfér a 10 árucikk és a 2 áruelválasztó, ide fogják felpakolni a vécépapír tekercseket, a kilós liszteket és a konzerveket sorban.

A megoldás

Ismétléses kombináció

Feladat

Hányféleképp választható ki k (nem feltétlenül különböző) elem n elem közül, ha a kiválasztás sorrendje nem számít?

k árucikk és $n-1$ áruelválasztó: $n+k-1$ hely a szalagon

az áruelválasztók lehetséges helyei: $\binom{n+k-1}{n-1}$

Válasz:

$$\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$$

Tétel

Egy n-elemű halmaz k (nem feltétlenül különböző) eleméből $\binom{n+k-1}{k}$-féle rendszer képezhető.

Feladat (újra)

Két 12-oldalú dobókockával dobunk. Hányféle számkombinációt kaphatunk?

Megoldás: 12-féle szám közül választunk kettőt, ismétléssel, nem számít a sorrend (ismétléses kombináció).
$n = 12, k = 2$, a képlet szerint

$$\binom{12+2-1}{2} = 78.$$