Megoldás. Megmutatjuk, hogy $n \geq 1$ esetén $p(n) = \binom{n}{2}$. Az alábbi eljárás legfeljebb $\binom{n}{2}$ próbálkozásból oldja meg a feladatot, azaz $p(n) \leq \binom{n}{2}$. Legyenek a kulcsok $k_1, k_2, \ldots, k_n$, és jelölje b_i azt a bőröndöt, amit k_i nyit. Célunk a b_i megtalálása minden i-re. A k_1 kulcsot próbáljuk bele az első néhány bőröndbe, amíg ki nem derül, melyik a b_1. Ehhez legfeljebb $n-1$ próbálkozás kell, mert amint már $(n-1)$-szer sikertelenül próbálkoztunk, azonnal tudjuk, hogy k_1 bizonyosan az utolsó, ki nem próbált bőröndöt nyitja. A k_2 kulccsal is tegyük ugyanezt, azzal a megszorítással, hogy a b_1 bőrönddel semmiképp se próbálkozzunk. Hasonló okból legfeljebb $n-2$ próbálkozást végzünk addig, amíg meg nem találjuk b_2-t. Általában, a $b_1, b_2, \ldots, b_{i-1}$ bőröndök megtalálása után a b_i-t keressük meg úgy, hogy a k_i kulcsot sorra belepróbáljuk a lehetséges $n-(i-1) = n-i+1$ bőröndbe. Világos, hogy legfeljebb $n-i$ próbálkozás után megtaláljuk b_i-t. Összességében tehát nem több, mint $\sum_{i=1}^{n}(n-i) = \binom{n}{2}$ próbálkozást végzünk.

Megmutatjuk másrészt, hogy $p(n) \geq \binom{n}{2}$, azaz $\binom{n}{2}$-nél kevesebb próbálkozást megengedve nem lehetünk bizonyosak afelől, hogy mindig megtaláljuk az összetartozó bőrönd-kulcs párokat. Tegyük fel, hogy egy olyan módszer szerint próbáljuk a kulcsokat a bőröndökhöz, amely beazonosítja az összetartozó bőrönd-kulcs párokat, másrészt az ehhez felhasznált próbálkozásszámok lehetséges legnagyobbika is a lehető legkisebb. Világos, hogy ezen stratégia szerint eljárva sosem fogunk belepróbálni egy kulcsot egy bőröndbe akkor, ha már a próba előtt bizonyosak lehetünk afelől, hogy az adott kulcs nyitja a szóban forgó bőröndöt. Ez azt jelenti, hogy fel kell arra készülnünk, hogy csupa sikertelen próbálkozás alapján kell megbizonyosodnunk az összes összetartozó (b_i, k_i) bőrönd-kulcs párról.

Ha ez megtörtént, és valamely $1 \leq i < j \leq n$ esetén nem próbáltuk bele sem a k_i kulcsot a b_j bőröndbe, sem a k_j kulcsot a b_i bőröndbe, akkor az elvégzett próbálkozásaink alapján nem zárhatjuk ki azt a lehetőséget, hogy a k_i kulcs a b_j bőröndöt, a k_j kulcs pedig a b_i bőröndöt nyitja, míg a többi kulcs ahhoz a bőröndhöz tartozik, amelyikhez eddig gondoltuk. Ez pedig azt jelentené, hogy mégsem tudjuk bizonyosan összepárosítani a kulcsokat és bőröndöket. Tehát tetszőleges $1 \leq i < j \leq n$ esetén a $k_i - b_j$ és a $k_j - b_i$ próbák valamelyikét el kell végeznünk. Mivel különböző (i, j) párokhoz ezen próbák különböznek, legalább annyi próbálkozásra van szükség, ahányféleképpen különböző i-t és j-t tudunk választani, vagyis legalább $\binom{n}{2}$-re. Ezzel megmutattuk, hogy $p(n) \geq \binom{n}{2}$, és ezt összevetve a korábban igazolt $p(n) \leq \binom{n}{2}$ egyenlőtlenséggel éppen a bizonyítani kívánt $p(n) = \binom{n}{2}$ állítás adódik. $\square$

Megjegyzések. 1. A fenti bizonyítás kulcslépése az alsó becslés bizonyítása, azon belül is az „ellenség módszer" alkalmazása, amikor is azt indokoljuk, hogy csupa negatív próba után is össze kell tudnunk párosítani a kulcsokat a bőröndökkel.

2. Ez az alsó becslés gráfelméleti nyelven is elmondható. Tekintsük azt a G gráfot, amelynek csúcsai a bőröndök és a kulcsok, él pedig az összetartozó párok között fut. Világos, hogy minden egyes próbálkozás egy-egy lehetséges bőrönd-kulcs él G-beliségének „lekérdezését" jelenti, célunk pedig a G gráf meghatározása. Az ellenség-módszert (adversary method) használó érv azt indokolja, hogy akkor is meg kell tudnunk határozni G-t, ha minden értelmes lekérdezéskor az derül ki, hogy az adott él nincs G-ben. A fent közölt bizonyítás úgy is elmondható, hogy ha G-t sikerült így meghatároznunk, akkor tetszőleges $i \neq j$-re le kellett kérdeznünk a $k_i b_j$ és $k_j b_i$ élek közül legalább az egyiket.

Máshogyan is igazolhatjuk az alsó becslést. Ha a lekérdezések negatív eredményei egyértelműen meghatározzák G-t, akkor a le nem kérdezett $k-b$ élek nem alkothatnak alternáló kört a G gráf éleivel. Ekkor ugyanis nem lenne az kizárható, hogy e körnek a G-n kívüli élei mentén tartoznak össze a kulcsok és bőröndök. (A fenti bizonyításban 4 hosszú alternáló körrel dolgoztunk.) Innen könnyen igazolható, hogy valamelyik bőrönd vagy kulcs legalább $n-1$ próbálkozásban szerepelt. Feltehető, hogy ez a k_n vagy b_n valamelyike. Ugyanilyen megfontolással látható, hogy a $b_1, b_2, \ldots b_{n-1}$ bőröndök, illetve a $k_1, k_2, \ldots, k_{n-1}$ kulcsok valamelyike (mondjuk az $n-1$ indexű) legalább $n-2$ olyan próbálkozásban szerepelt, amelyben nem szerepelt sem b_n, sem k_n. A gondolatmenetet folytatva meg lehet mutatni, hogy az összetartozó $b_i k_i$ bőrönd–kulcs párokat el tudjuk látni indexszel úgy, hogy minden $1 \leq i \leq n$ esetén a b_i vagy a k_i legalább $i-1$ olyan próbálkozásban vett részt, amelyben $b_{i+1}, \ldots, b_n$ és $k_{i+1}, \ldots, k_n$ egyikét sem használtuk.

3. Többen próbálkoztak a fentihez hasonló érveléssel. Volt, aki elkövette azt a hibát, hogy a le nem kérdezett élek gráfjának körmentességét próbálta igazolni. Sajnos ez általában nem igaz. Valójában ez a gráf a G éleivel alternáló kört nem tartalmazhat. Szerencsére, ahogy azt az előző megjegyzésbeli bizonyítás vázlat mutatja, már ez is elég az alsó becsléshez.