

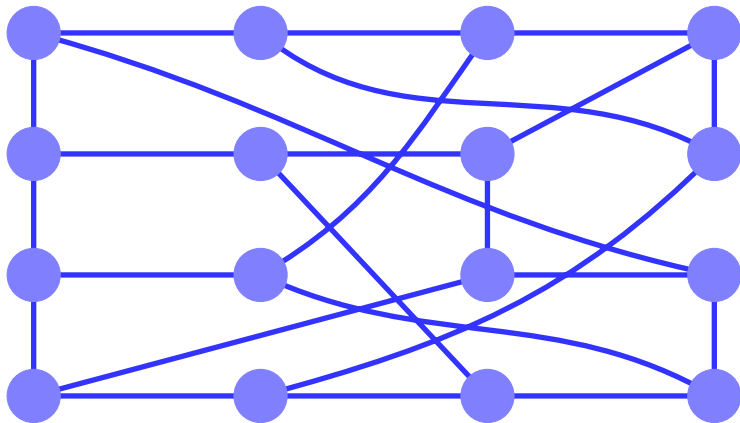
Kriptográfia házi használatra

Csirmaz László

CEU – Rényi – ELTE

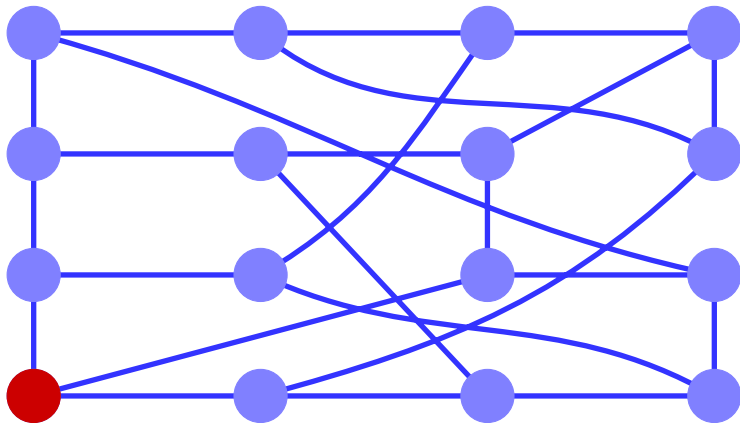
2018 Szeptember 26

A fagylaltos kocsik hová álljanak?



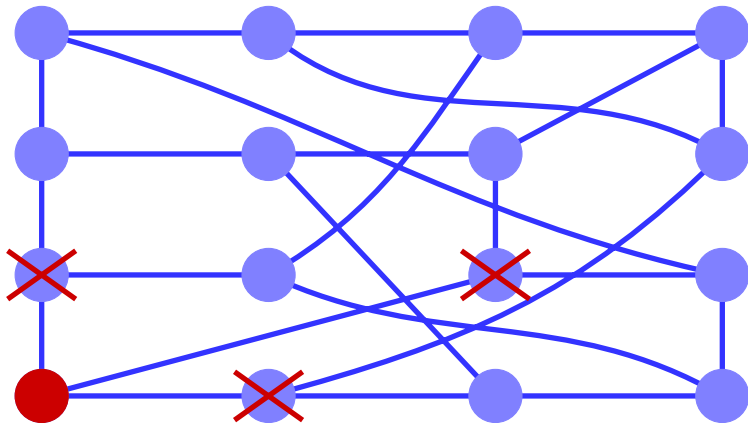
Szomszédos sarkokon nincs fagylaltoskocsi.

A fagylaltos kocsik hová álljanak?



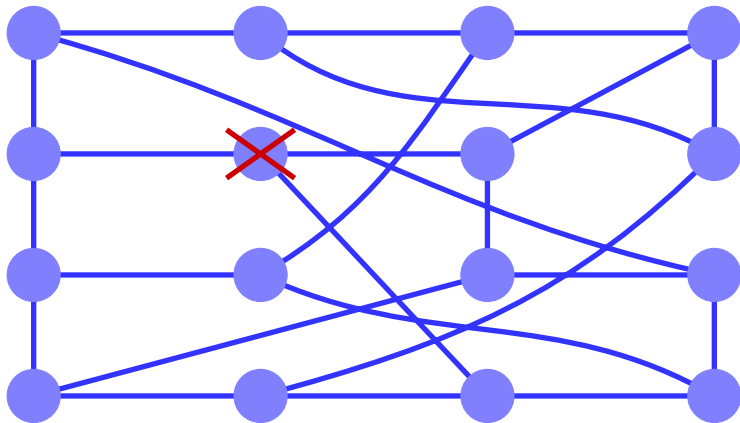
Szomszédos sarkokon nincs fagylaltoskocsi.

A fagylaltos kocsik hová álljanak?



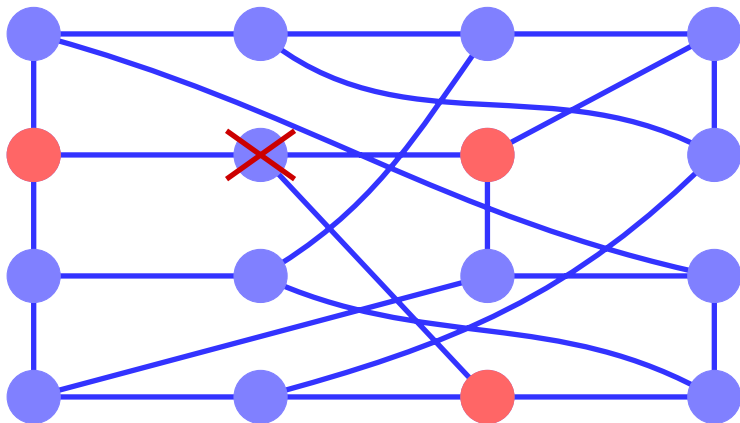
Szomszédos sarkokon nincs fagylaltoskocsi.

A fagyaltos kocsik hová álljanak?



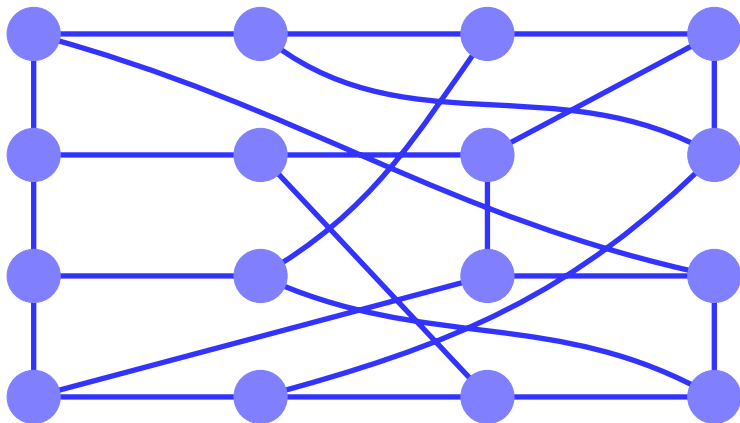
Mindenhonnan legfeljebb egy sarokra *pontosan* egy kocsi áll.

A fagyaltos kocsik hová álljanak?



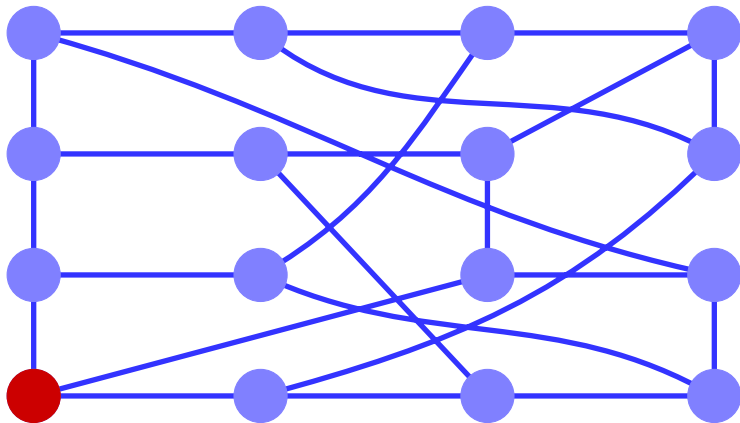
Mindenhonnan legfeljebb egy sarokra *pontosan* egy kocsi áll.

A fagylaltos kocsik hová álljanak?



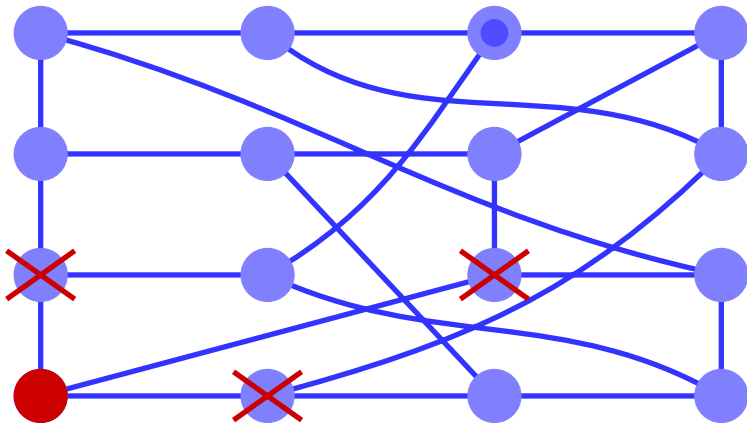
Keressünk egy jó elrendezést!

A fagyaltos kocsik hová álljanak?



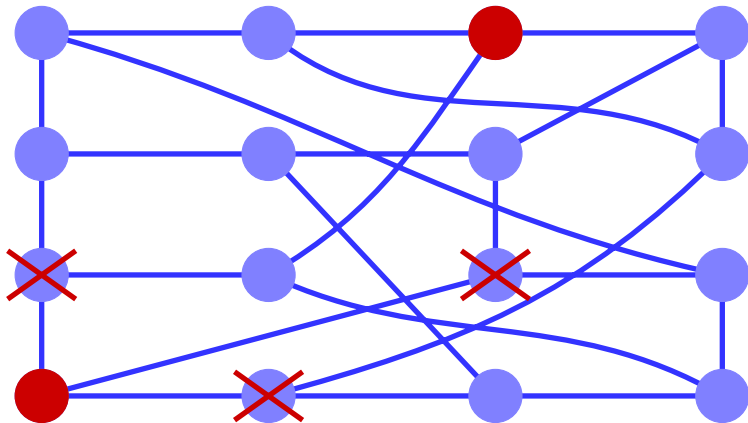
Keressünk egy jó elrendezést!

A fagyaltos kocsik hová álljanak?



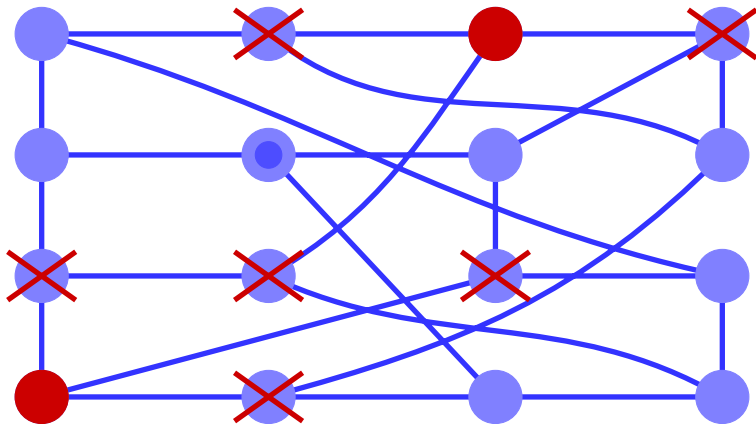
Keressünk egy jó elrendezést!

A fagylaltos kocsik hová álljanak?



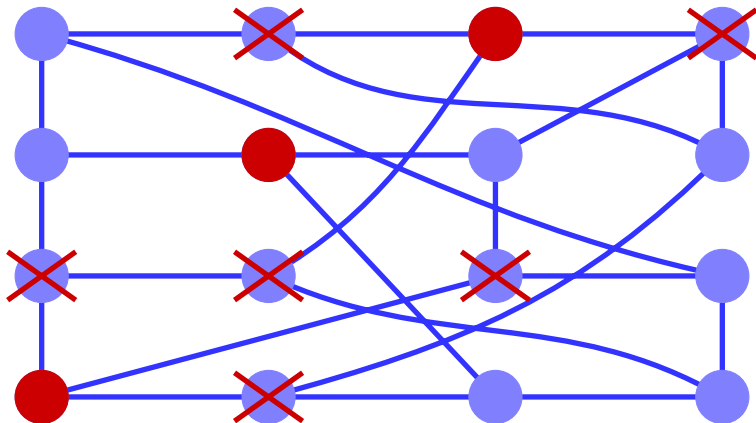
Keressünk egy jó elrendezést!

A fagyaltos kocsik hová álljanak?



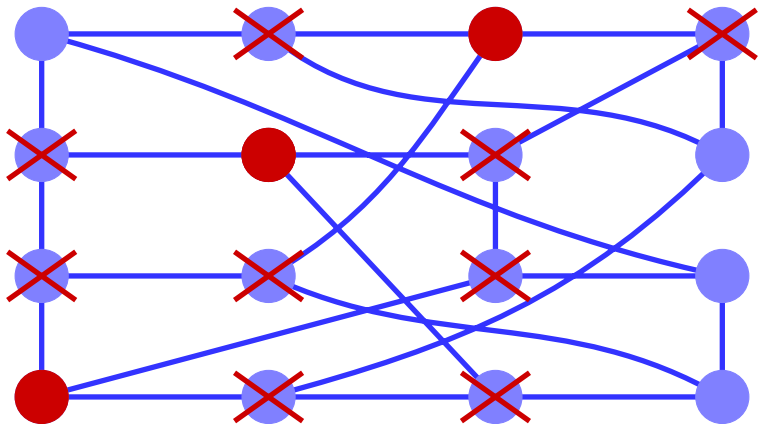
Keressünk egy jó elrendezést!

A fagyaltos kocsik hová álljanak?



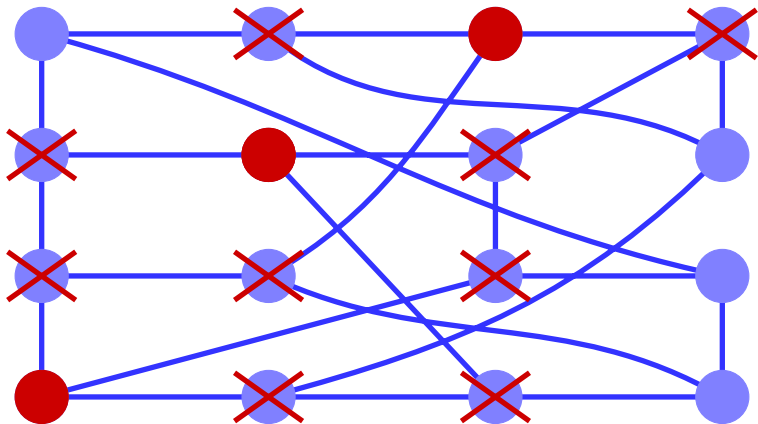
Keressünk egy jó elrendezést!

A fagylaltos kocsik hová álljanak?



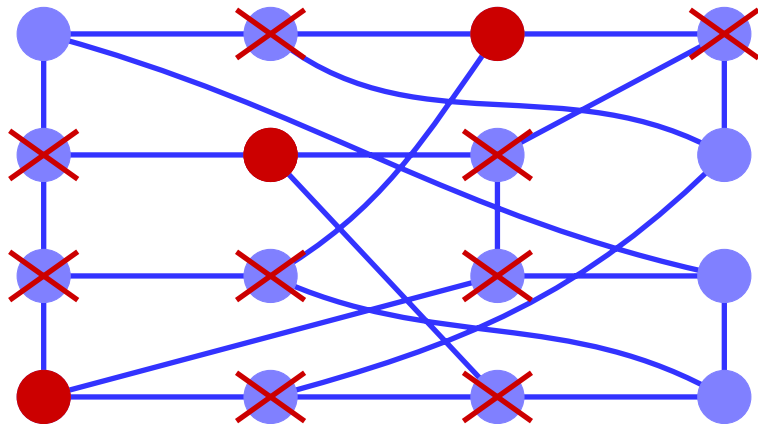
Keressünk egy jó elrendezést!

A fagylaltos kocsik hová álljanak?



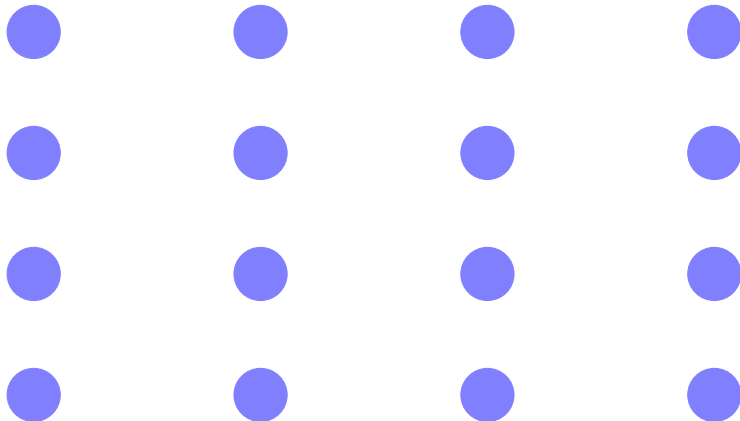
Keressünk egy jó elrendezést! És itt megakadtunk ...

A fagyaltos kocsik hová álljanak?



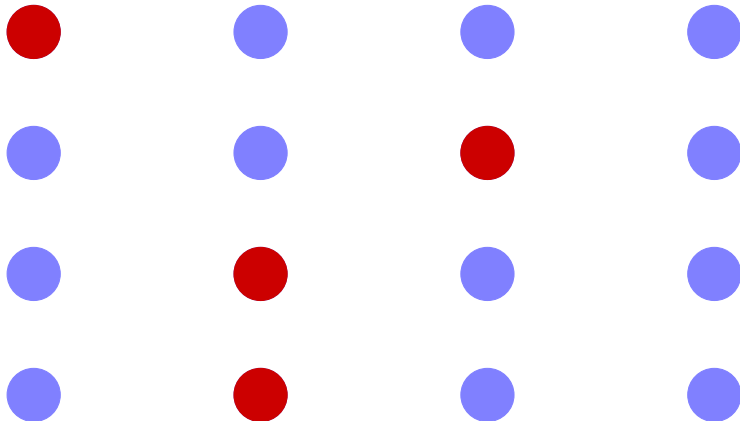
Lefogó rendszer keresése tetszőleges gráfban NP nehéz.

Hogyan készítsük a feladatot?



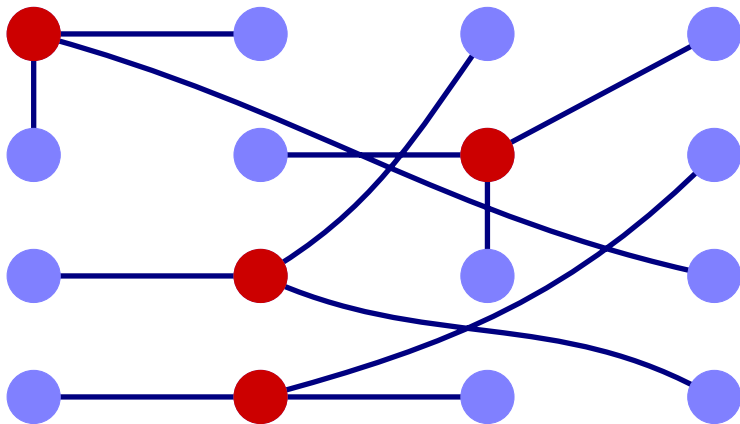
Kiindulunk a megoldásból.

Hogyan készítsük a feladatot?



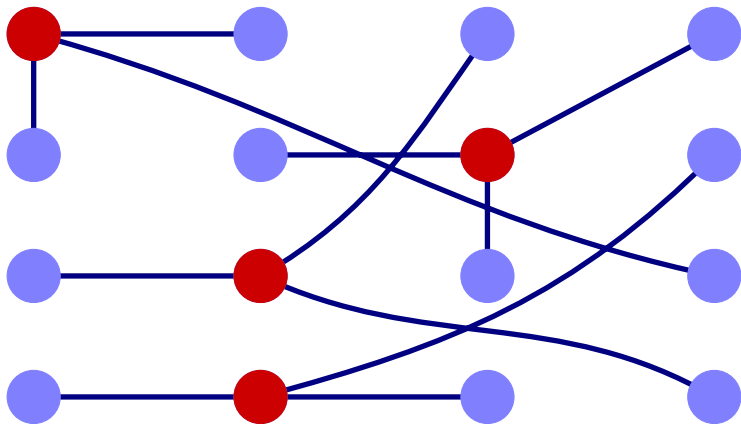
Kiindulunk a megoldásból.

Hogyan készítsük a feladatot?



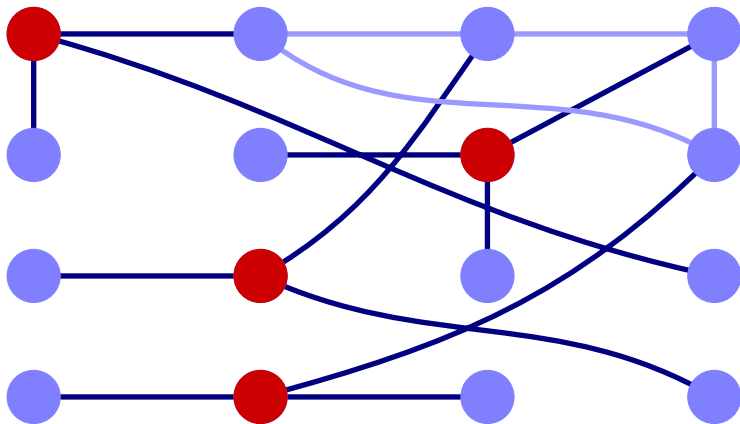
Behúzzuk az utakat amik garantálják a jó megoldást.

Hogyan készítsük a feladatot?



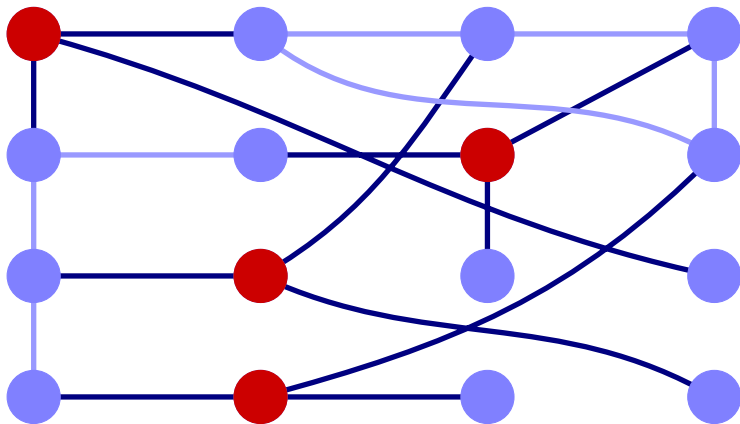
Aztán a kék csúcsok között tetszőlegesen húzunk további éleket.

Hogyan készítsük a feladatot?



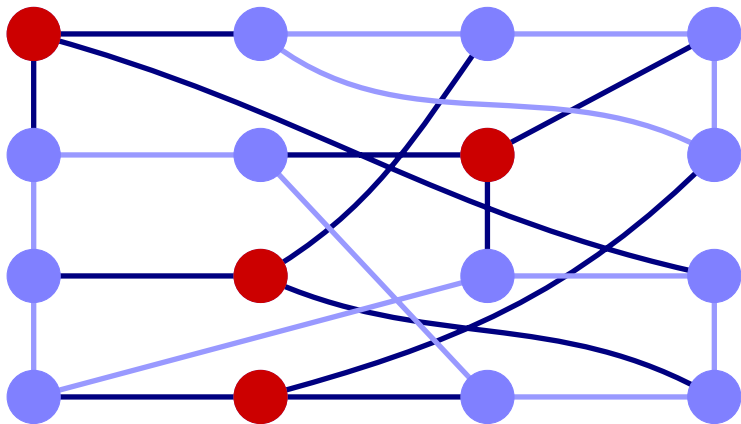
Aztán a kék csúcsok között tetszőlegesen húzunk további éleket.

Hogyan készítsük a feladatot?



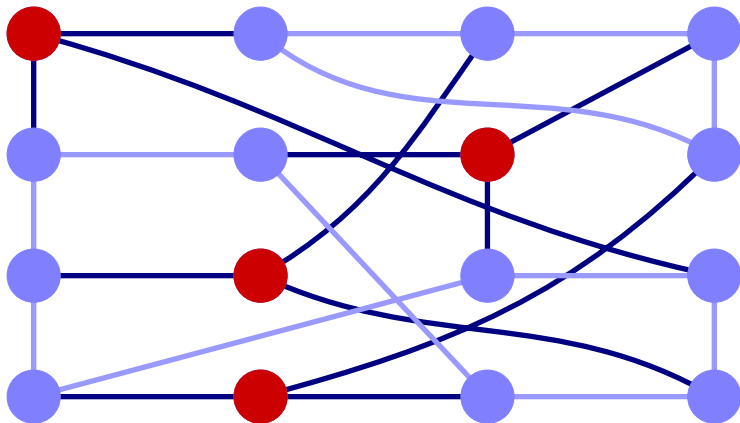
Aztán a kék csúcsok között tetszőlegesen húzunk további éleket.

Hogyan készítsük a feladatot?



Aztán a kék csúcsok között tetszőlegesen húzunk további éleket.

Hogyan készítsük a feladatot?



Kész a feladat!

Nyilvános kulcsú titkosítás

Láttuk, hogy könnyen tudunk olyan nehéz feladatot készíteni,

- aminek mi ismerjük a megoldását;
- várhatóan senki más nem tud jó megoldással előállni belátható időn belül.

Ilyen típusú feladatok állnak minden publikus kulcsú titkosítás mögött.

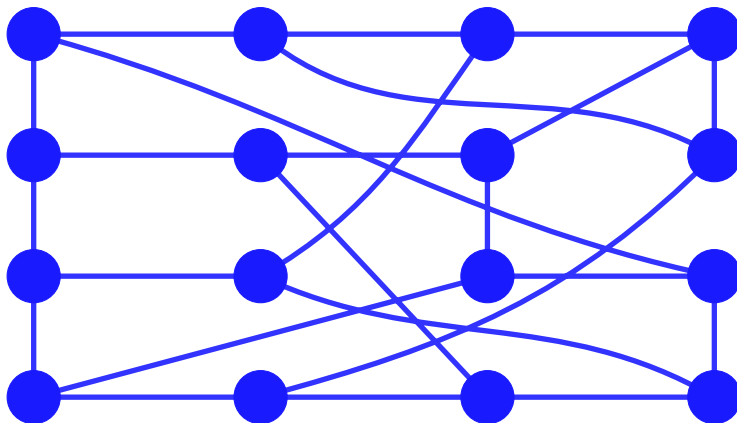
- **nyilvános kulcs:** a feladat.
- **titkos kulcs:** a feladat megoldása.

A **nyilvános kulcs** segítségével bárki tud üzenetet kódolni,
de

a kódolt üzenetet csak a **titkos kulccsal** lehet visszafejteni – még az üzenet küldője sem tud vele mit kezdeni.

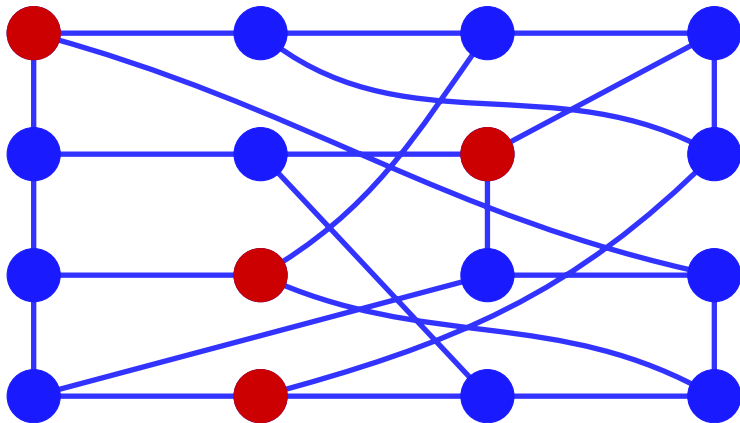
Esetünkben

a **nyilvános kulcs** a gráf (a város térképe):



Esetünkben

a **titkos kulcs** pedig a fagyaltoskocsik helye:

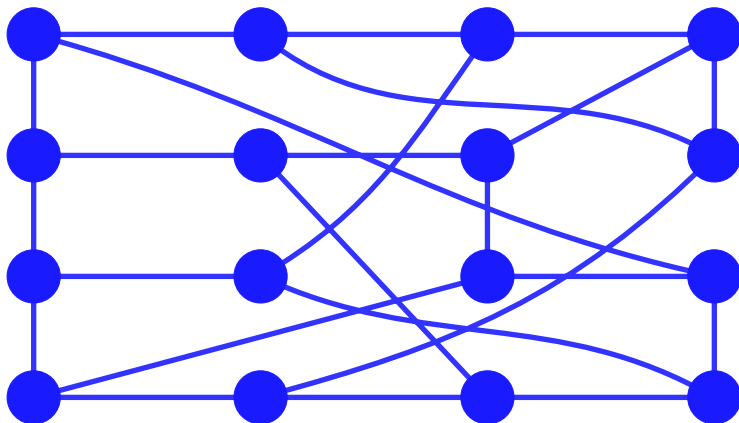


Hogyan kódoljunk?

Észrevétel: a fagylaltoskocsik és azok szomszédai minden csúcsot pontosan egyszer tartalmaznak.

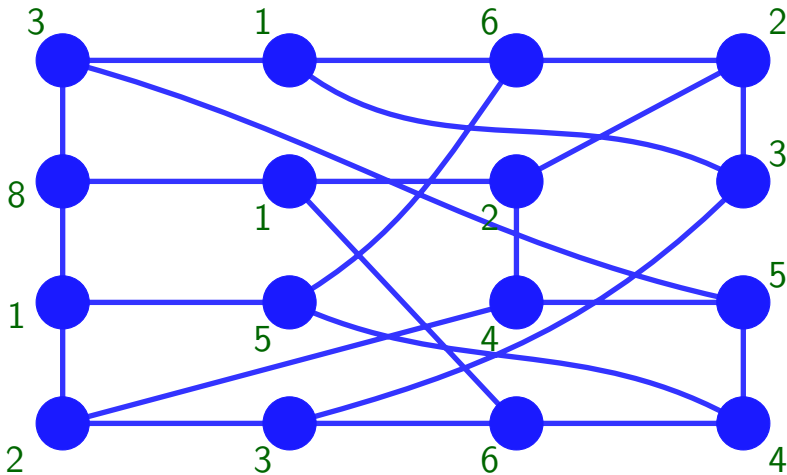
Következőképp: minden csúcshoz írunk egy **zöld** számot; majd minden csúcsba **fehérrel** beírjuk az ottani és a szomszédos zöld számok összegét. Ekkor a fagylaltoskocsiknál álló **fehér** számok összege egyenlő az összes **zöld** szám összegével.

Példa



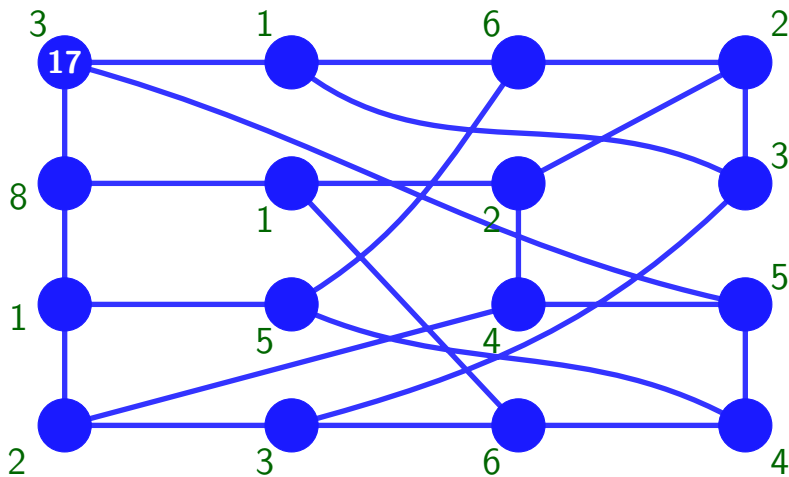
A **zöld** számok, véletlenül választva.

Példa



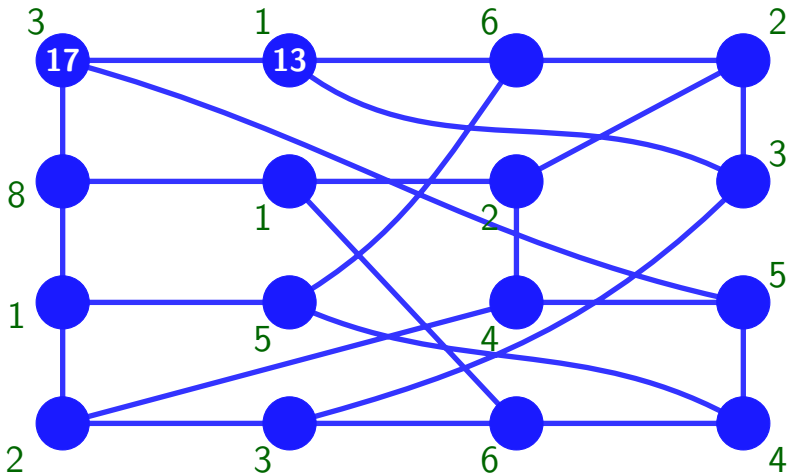
A **zöld** számok; az összegük 56.

Példa



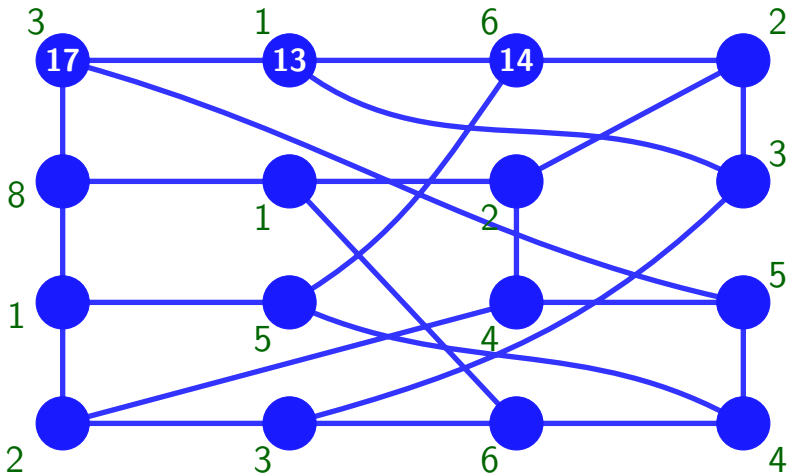
A **fehér** számok számítása ...

Példa



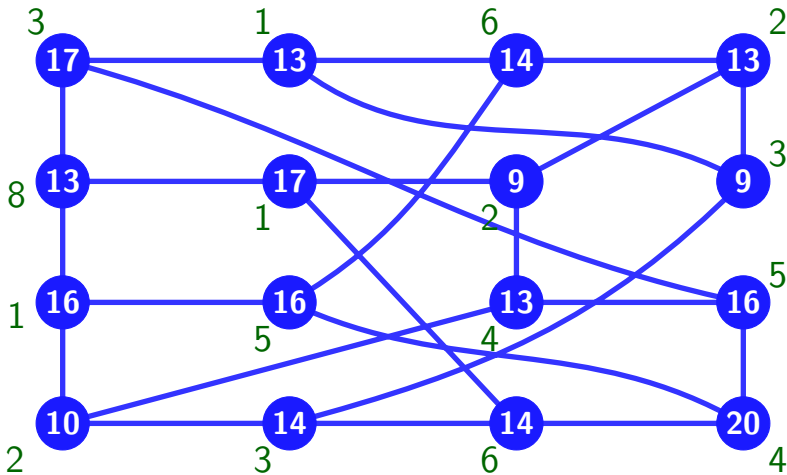
A **fehér** számok számítása ...

Példa



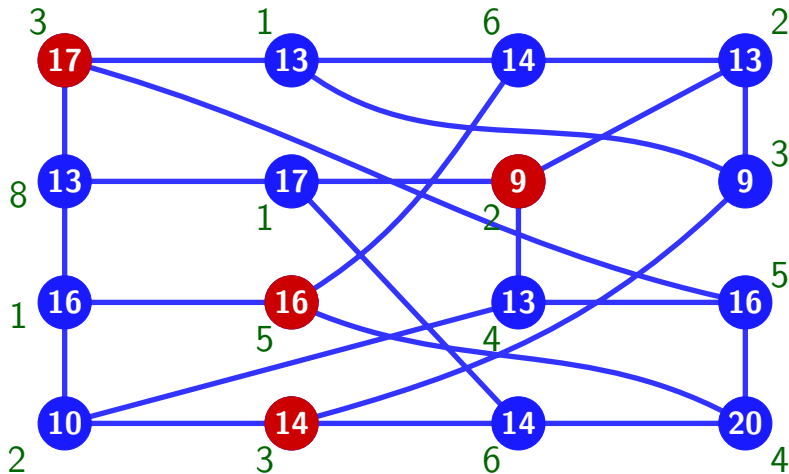
A **fehér** számok számítása ...

Példa



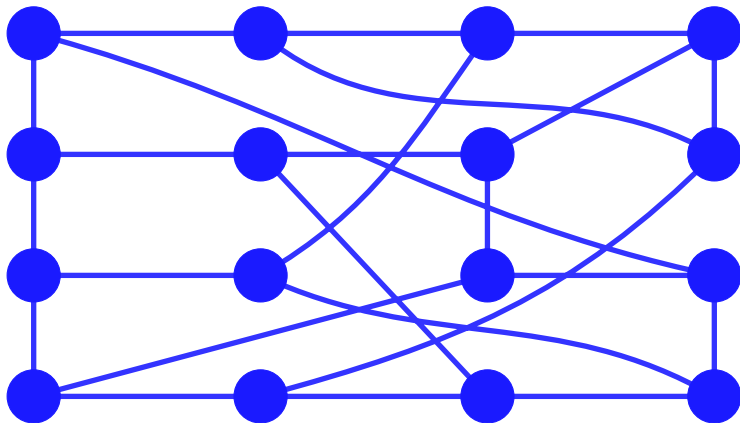
A **fehér** számok, és a többi ...

Példa



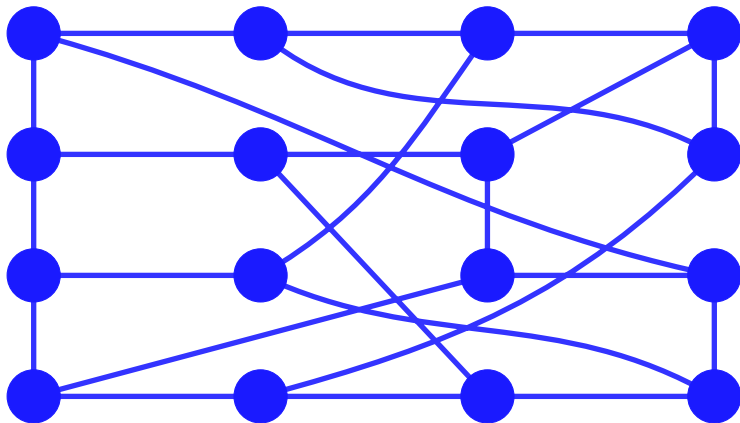
A fagyaltoskocsinál a számok összege $17 + 9 + 16 + 14 = 56$.

Üzenet kódolása a nyilvános kulccsal



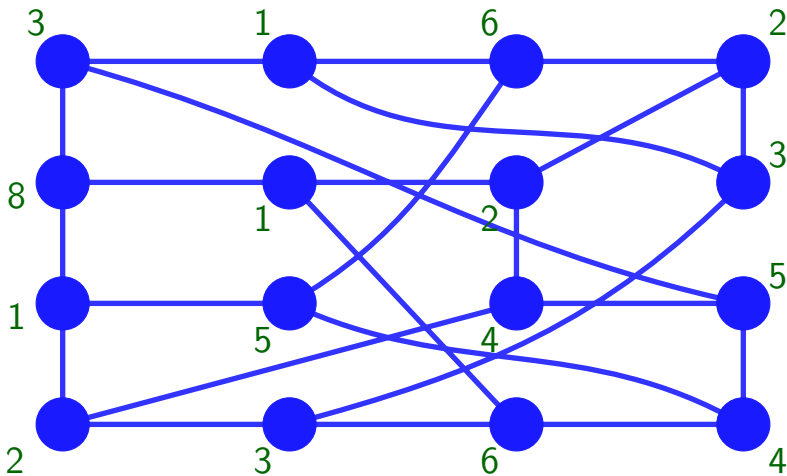
Az **üzenet** egy 0 és 9 közötti számjegy, mondjuk 6.

Üzenet kódolása a nyilvános kulccsal



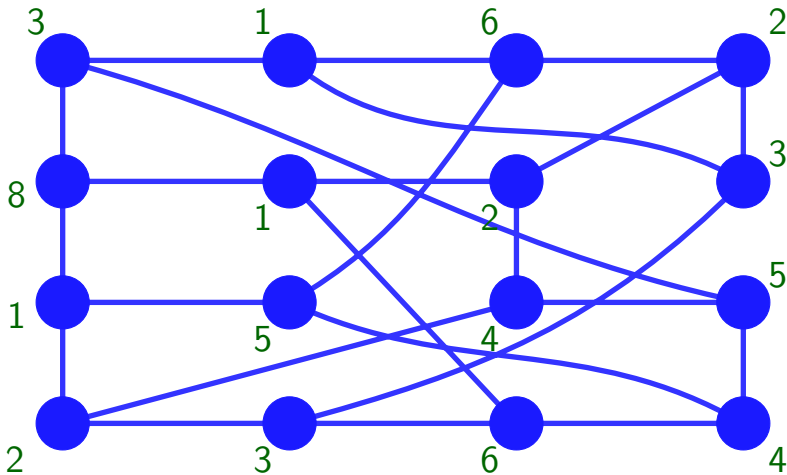
Válasszunk **zöld** számjegyeket hogy a teljes összeg 6-ra végződjön.

Üzenet kódolása a nyilvános kulccsal



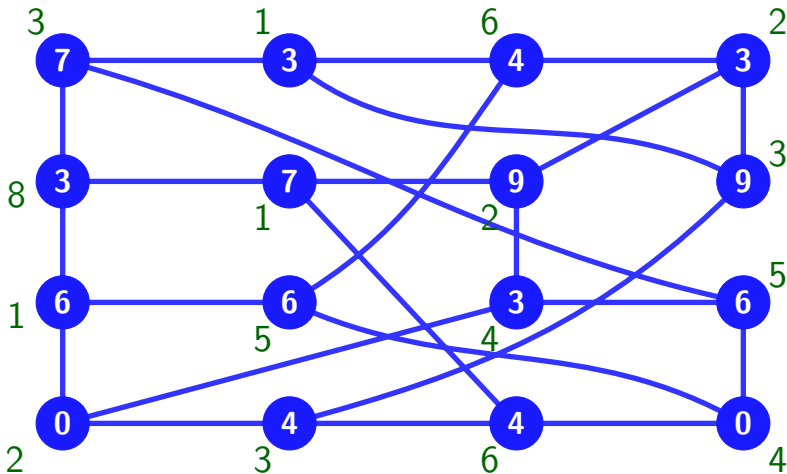
Válasszunk **zöld** számjegyeket hogy a teljes összeg 6-ra végződjön.

Üzenet kódolása a nyilvános kulccsal



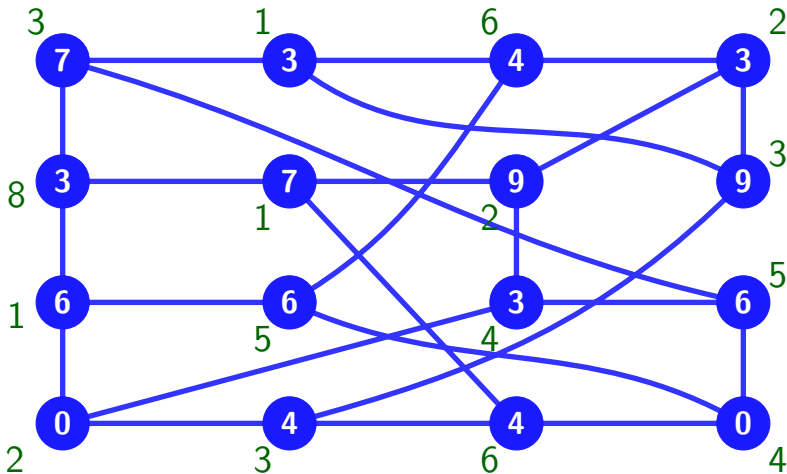
Írjuk minden csúcsba a megfelelő összeg **utolsó** jegyét.

Üzenet kódolása a nyilvános kulccsal



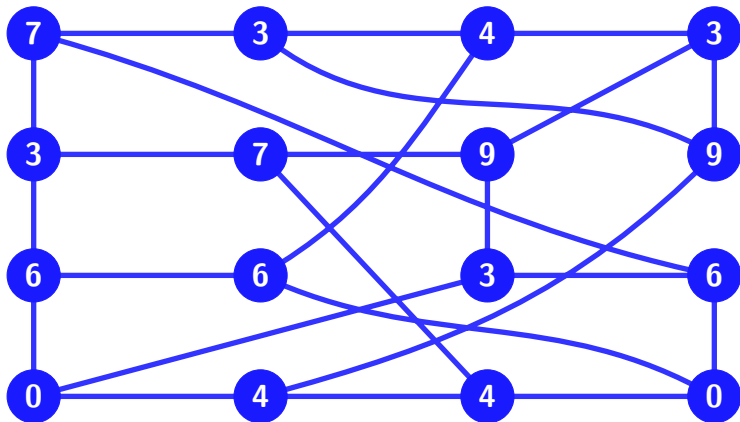
Írjuk minden csúcsba a megfelelő összeg **utolsó** jegyét.

Üzenet kódolása a nyilvános kulccsal



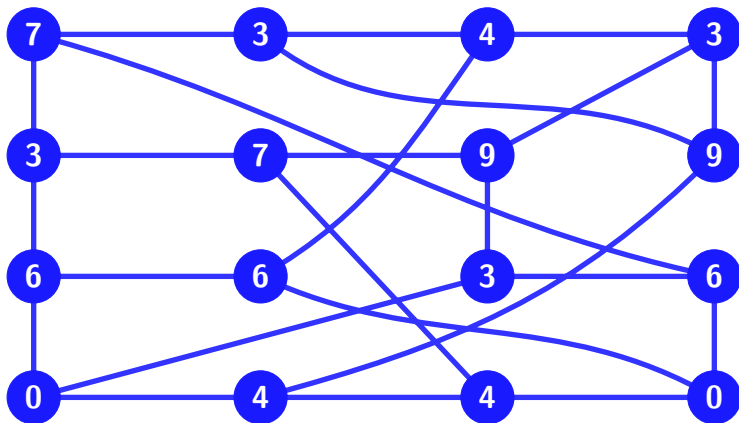
Töröljük ki a **zöld** számokat.

Üzenet kódolása a nyilvános kulccsal



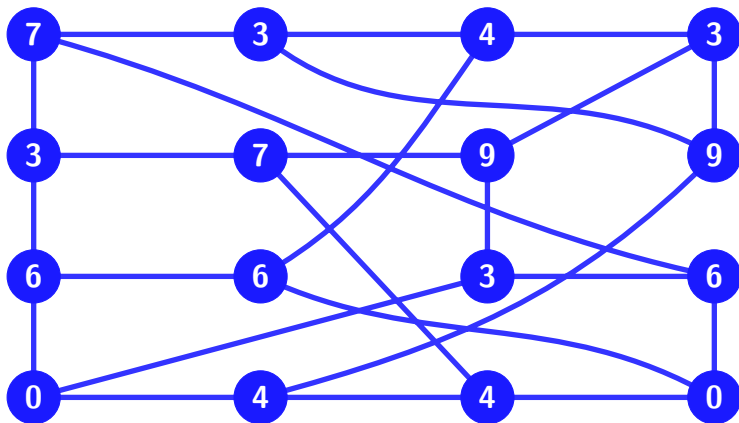
Töröljük ki a **zöld** számokat.

Üzenet kódolása a nyilvános kulccsal



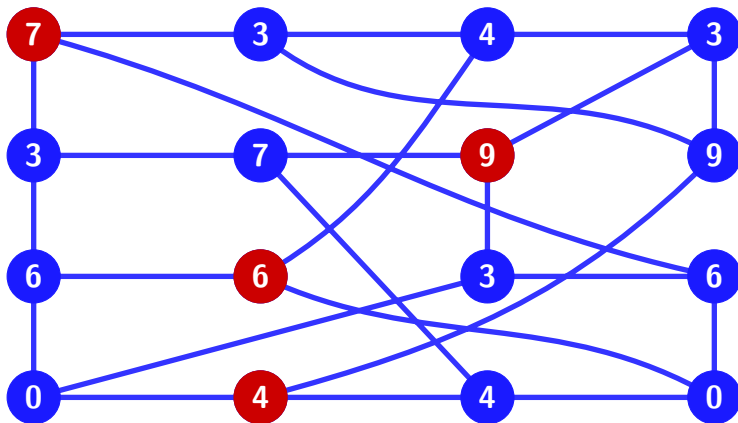
Töröljük ki a **zöld** számokat. A kód elkészült!

Kód megfejtése a titkos kulccsal



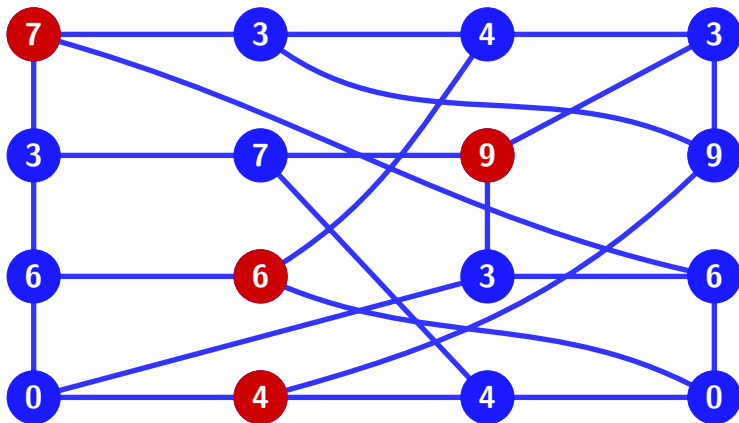
Megkaptuk az üzenetet, elővesszük a titkos kulcsunkat ...

Kód megfejtése a titkos kulccsal



Megkaptuk az üzenetet, elővesszük a titkos kulcsunkat ...

Kód megfejtése a titkos kulccsal



Összeadjuk: $7 + 9 + 6 + 4 = 26$, tehát az üzenet: **6** – egyszerű.

Végső válasz az életre, a világmindenségre meg mindenre

Megindult a projekt hogy megtudjuk:

Mi a végső válasz az életre, a világmindenségre, meg mindenre?

Zöldmezős beruházásban elkészült a *Mélyenszántó Gondolat* gép, mely teljes idejét a probléma megoldásának fogja szentelni.

Végső válasz az életre, a világmindenségre meg mindenre



Végső válasz az életre, a világmindenségre meg mindenre

Megindult a projekt hogy megtudjuk:

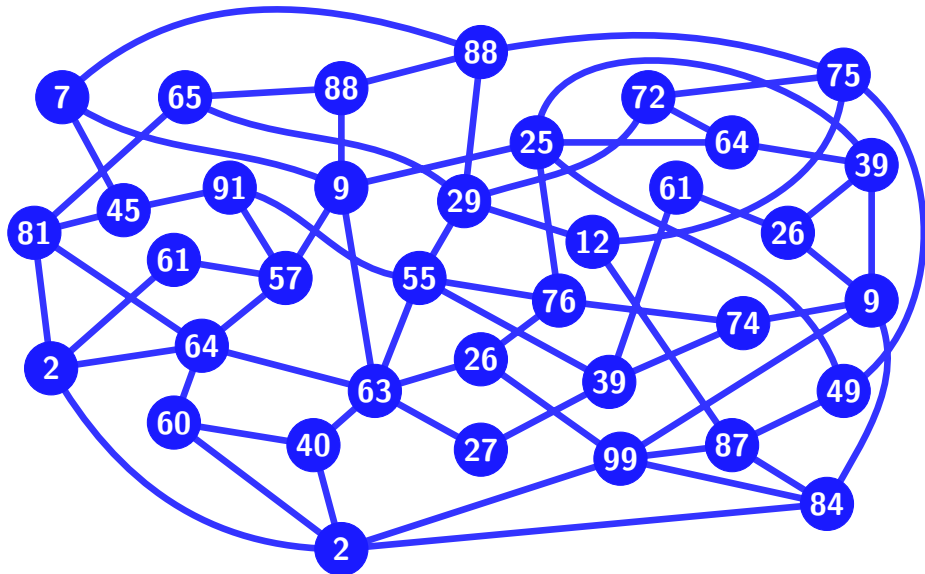
Mi a végső válasz az életre, a világmindenségre, meg mindenre?

Zöldmezős beruházásban elkészült a *Mélyenszántó Gondolat* gép, mely teljes idejét a probléma megoldásának fogja szentelni.

De én már tudom a választ,

csak nem akarom elárulni. Ehelyett elkódolom, és megmutatom a kódolt üzenetet:

Végső válasz az életre, a világmindenségre meg mindenre



Egymilliárd ével később . . .



Egymilliárd évvel később ...

a gép bejelenti az eredményt:

... a végső válasz az életre, a világmindenségre, meg mindenre ...

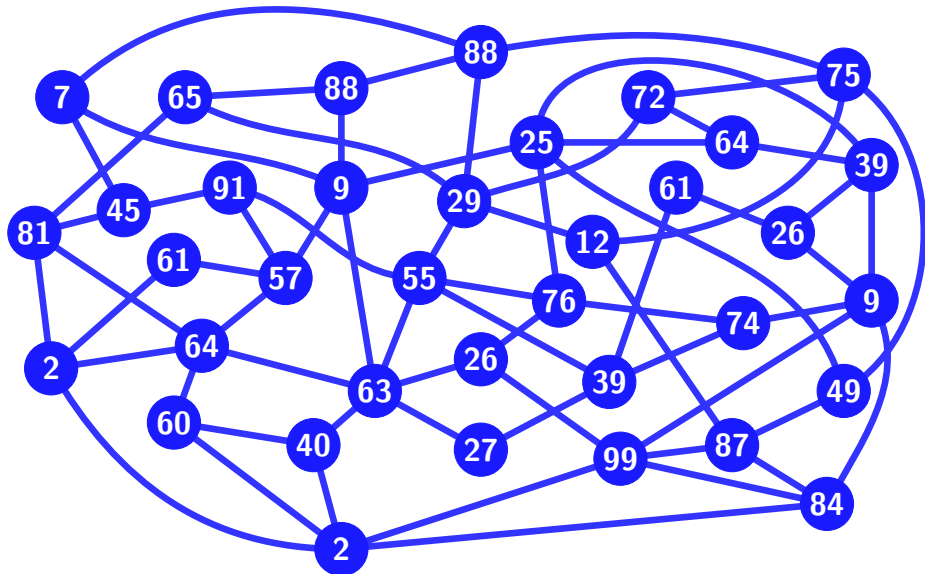
Egymilliárd évvel később ...

a gép bejelenti az eredményt:

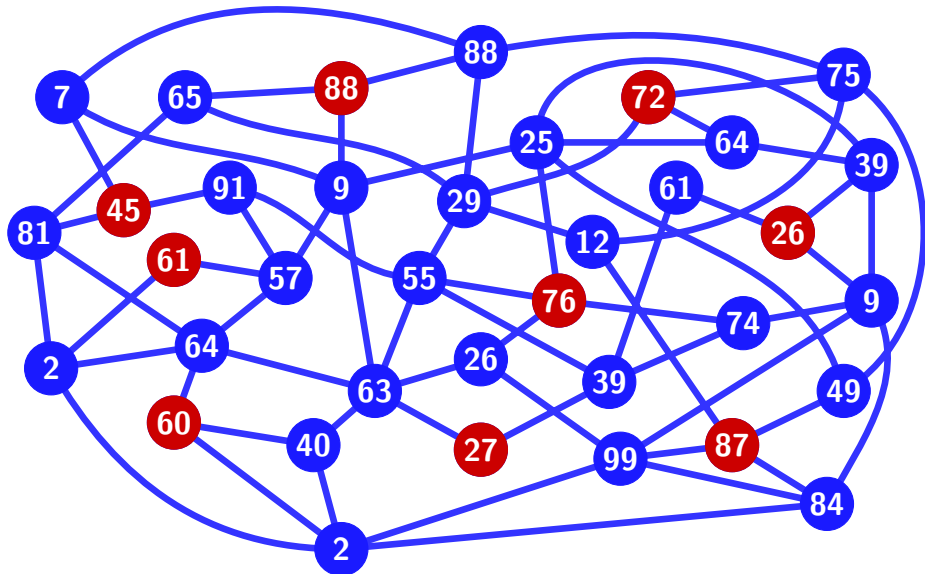
... a végső válasz az életre, a világmindenségre, meg mindenre ...

42

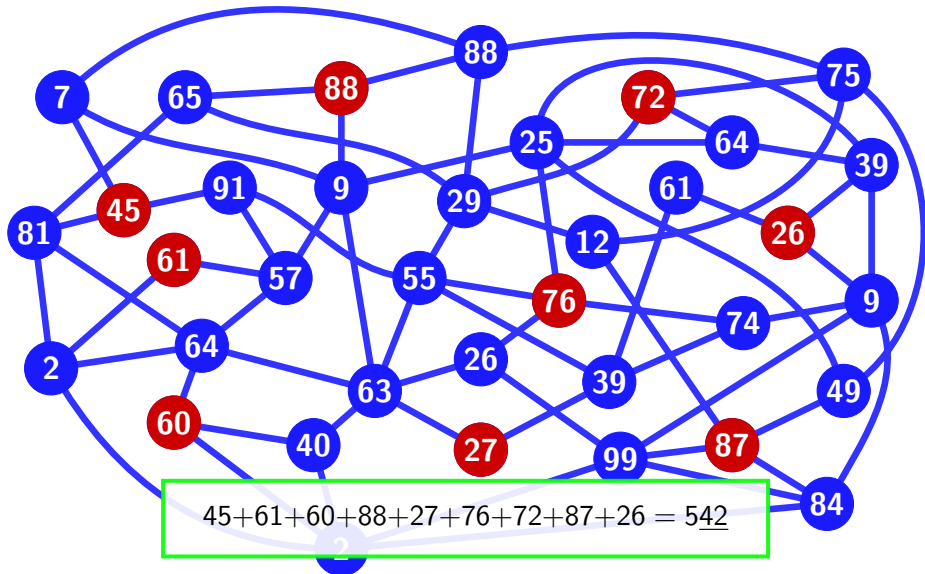
Egyilliárd évvel később ... és íme



Egyilliárd évvel később ... és íme



Egyilliárd ével később ... és íme



Köszönöm a figyelmet!

Irodalom



Tim Bell, Harold Thimbleby, Mike Fellows , Ian Witten, Neil Koblitz:

Explaining cryptographic systems to the general public



Csirmaz László:

Kriptográfia a középiskolában *A matematika tanítása*, 2005,
3–13