Задача (basic randomization).

В даден екип на дадена компания има не по-малко от четирима служители. Да се предостави стратегия, която дава възможност на всеки от екипа да разбере каква е средната заплата, която получава член на екипа, но не и каква е персоналната на който и да е от екипа. Работи ли предоставената стратегия, ако членовете на екипа са трима?

Решение:

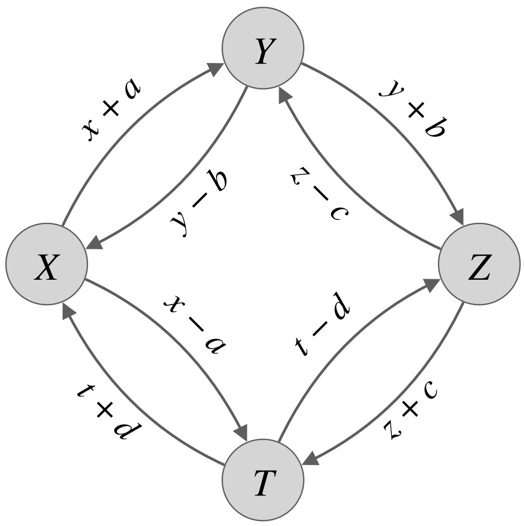
Без ограничение на общността допускаме, че членовете на екипа са точно 4. Нека ги именуваме с X, Y, Z и T и нека трудовите им възнаграждения са съответно x, y, z и t.

X избира произволно число $a \in \left[1,\, 2023x\right]$ и казва на Y че взима заплата от $x + a$, а на T, че взима заплата от $x - a$.

Y избира произволно число $b \in \left[1,\, 2023y\right]$ и казва на Z че взима заплата от $y + b$, а на X, че взима заплата от $y - b$.

Z избира произволно число $c \in \left[1,\, 2023z\right]$ и казва на T че взима заплата от $z + c$, а на Y, че взима заплата от $z - c$.

T избира произволно число $c \in \left[1,\, 2023t\right]$ и казва на X че взима заплата от $t + d$, а на Z, че взима заплата от $t - d$.



След прилагане на по-горната процедура, всеки един от екипа съобщава гласно пред всички членове на екипа полученият сбор от цялата информация, която е получил плюс оригиналната си заплата. Тоест:

X съобщава: $x + (y - b) + (t + d)$
Y съобщава: $y + (x + a) + (z - c)$
Z съобщава: $z + (y + b) + (t - d)$
T съобщава: $t + (x - a) + (z + c)$

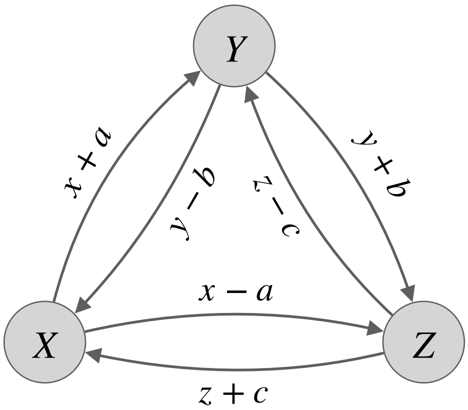
След съобщаването на тази информация, може да допуснем, че тя е меморизирана (например записана на някаква дъска) и може да и се вземе сумата ѝ, която е равна на:

$$\underbrace{x + (y - b) + (t + d)}_{X} + \underbrace{y + (x + a) + (z - c)}_{Y} + \underbrace{z + (y + b) + (t - d)}_{Z} + \underbrace{t + (x - a) + (z + c)}_{T} =$$
$$= 3(x + y + z + t)\ ,$$

което разделено на 12 дава търсеното средно възнаграждение на член от екипа. Числото 12 идва от броя на членовете на екипа умножен по 3.

Стратегията не работи за по-малко от 4-ма души в екипа. За да докажем това твърдение е необходимо да покажем как при наличито само на 3-ма членове от екипа е възможно произволен член на екипа да разбере заплатата на друг член от екипа, при предоставената по-горе стратегия. Да допуснем, че стратегията работи за екип от 3-ма души.

Използваме същото преименуване както по-горе, но с елиминиран Z.



Да разгледаме например Y. Той знае:

a) Собствената си заплата y
b) Собственото си произволно генерирано число b
c) Казаната гласна сума от $X : x + (y - b) + (z + c)$
d) Казаната гласно сума от $Z : z + (x - a) + (y + b)$
e) Средната заплата на целия екип след края на процедурата: $\dfrac{x + y + z}{3}$
f) Съобщената му информация от $X : x + a$
g) Съобщената му информация от $Z : z - c$

Възможни изчисления на Y:

1) Събирайки почленно c) и d) Y ще знае: $2x + 2y + 2z + (c - a)$ и тъй като знае e), той ще знае и $(c - a)$
2) Изваждайки почленно d) от c) Y ще знае: $c + a - 2b$ и тъй като знае b), той ще знае и $(c + a)$
3) От 1) и 2) следва, че той ще знае и произволните генерирани числа: a на X и c на Z
4) От 3) и f) следва, че Y ще може да разбере каква е истинската заплата на X, което е в конфликт с условието на задачата и следователно допускането, че стратегията работи за по-малко от 4-ма души е грешно.

$\square$