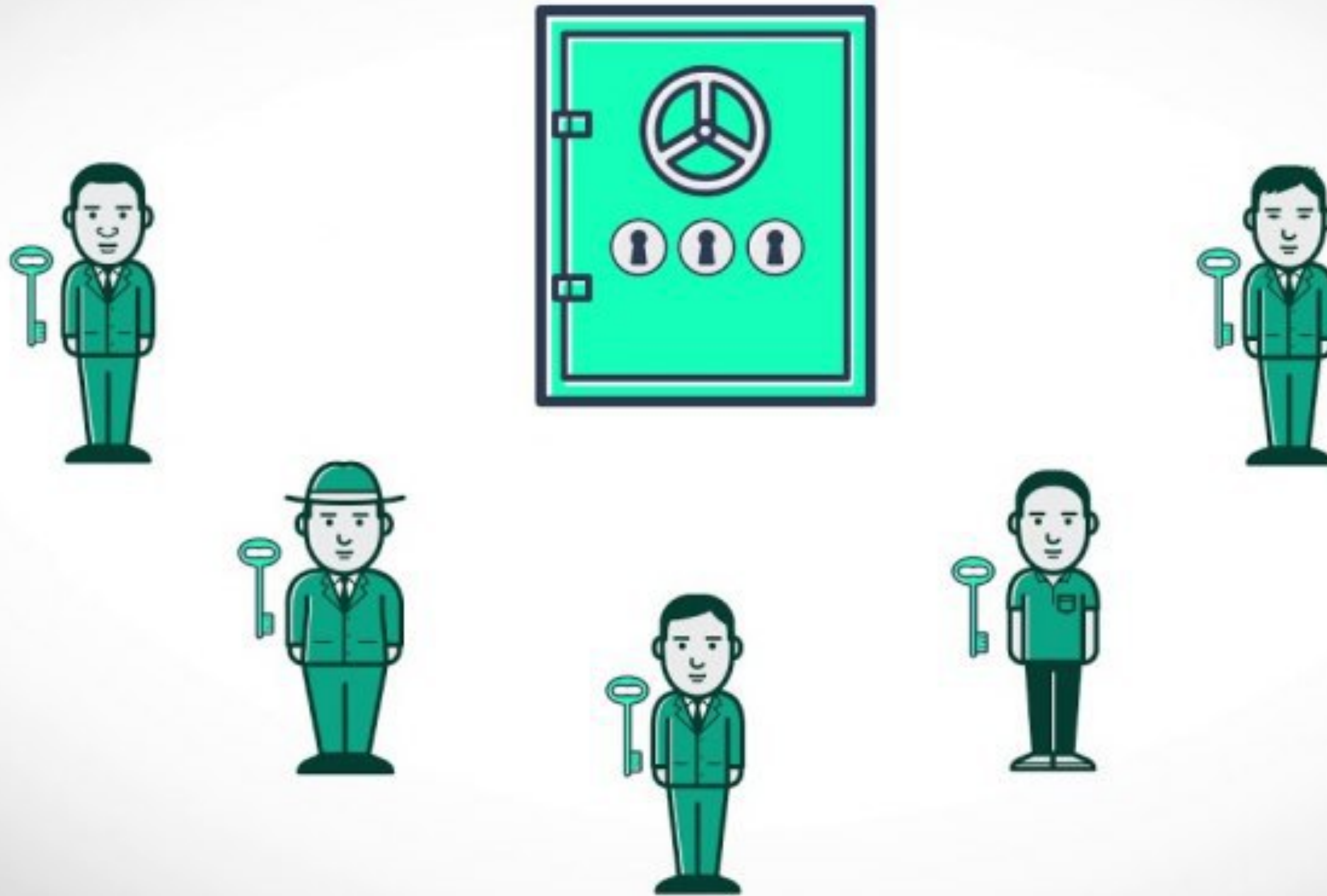


Схеми таємного поширення інформації



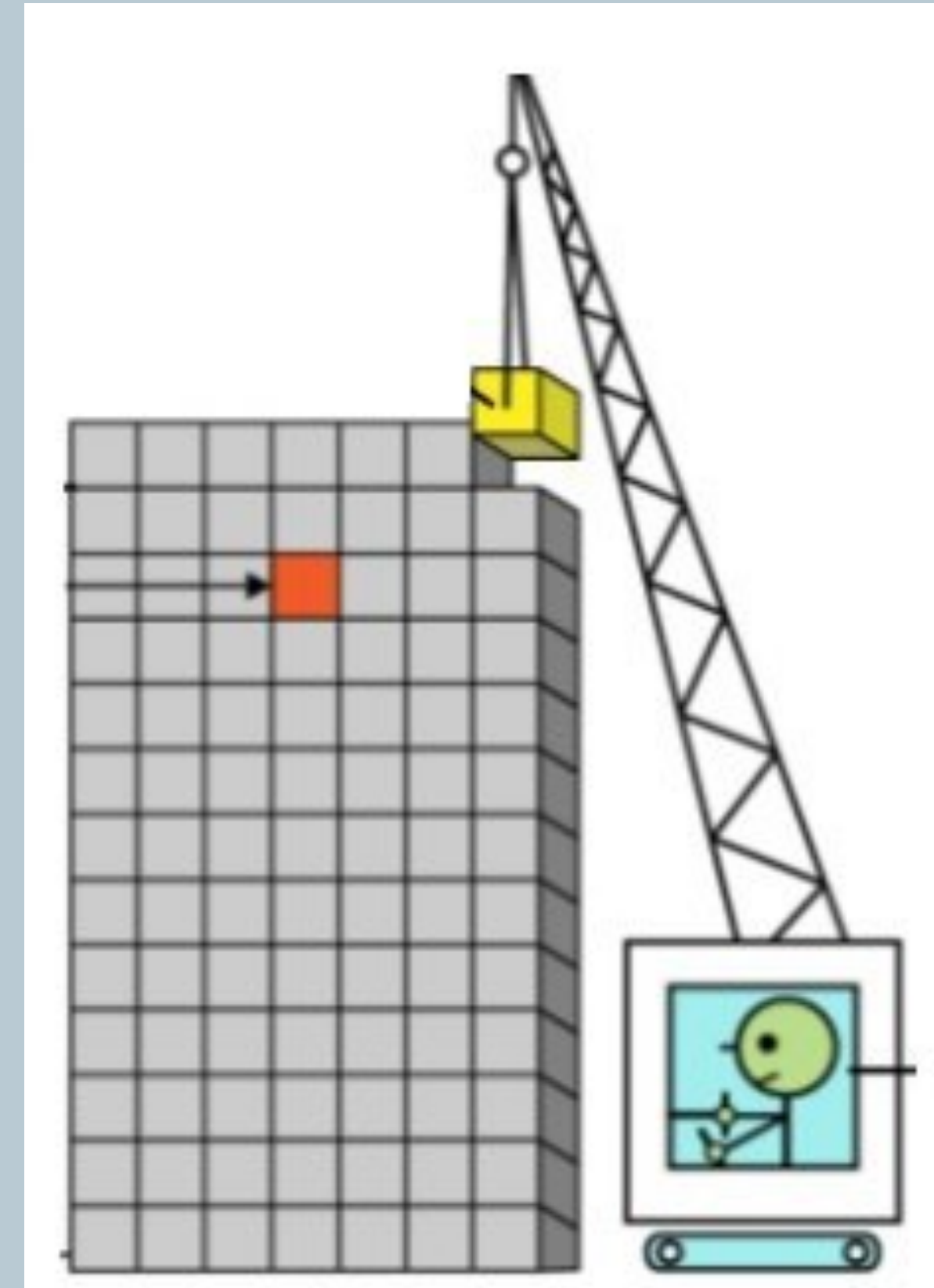
18.05.2020

by Stanislav Stepaniuk

Основні складові

Розподіл

Відновлення



Найпростіша схема

(n, n)

Порогова схема

(t, n)

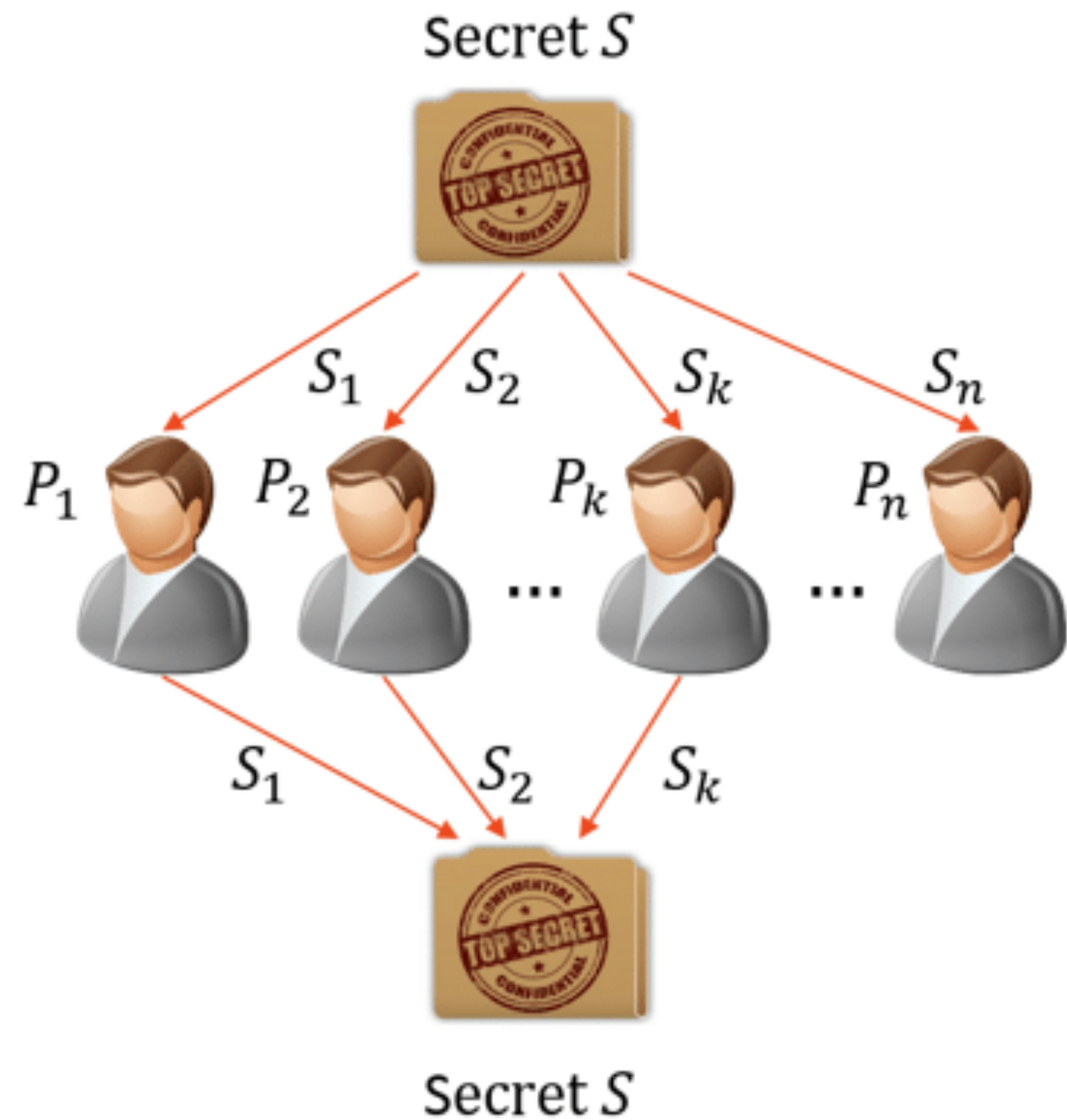
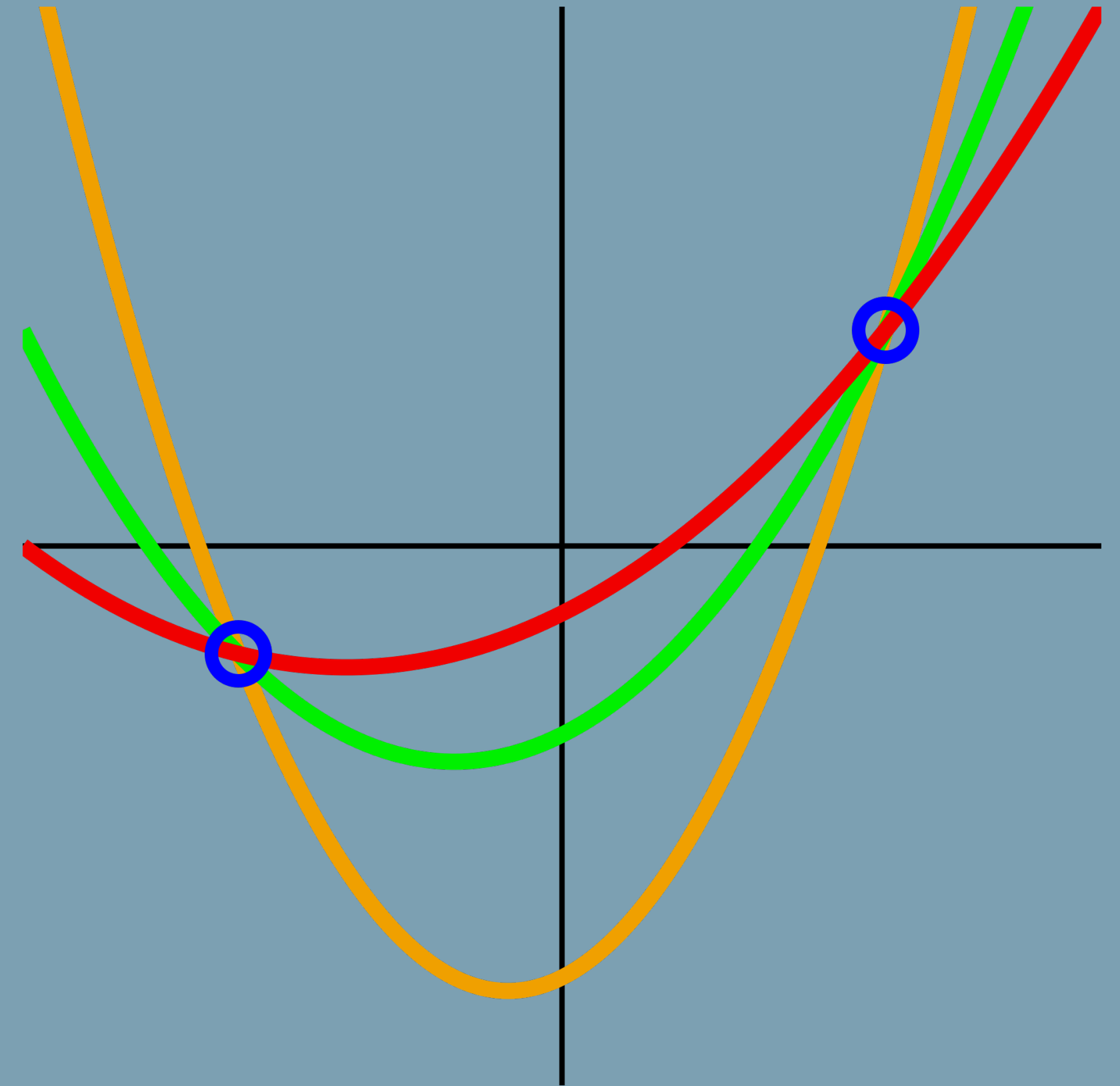


Схема Шаміра

властивості:

- 1.Безпека
- 2.Мінімалізм
- 3.Розширюваність
- 4.Динамічність
- 5.Гнучкість:



Пропозиція схеми

Шифрувати частини секрету користуючись асиметричною технікою шифрування RSA

Secret: 48468722958635381340480276230627209439649824273353758645046163201165456821345

Shares:

(1, 3669845134750661879108003894576642672856955636406923384065587858120721823143)

(2, 43219960414130498480004867615378650654235136645786398935576084159049170960619)

(3, 51326979559458695719599882384345325530514382635851621260120068096037674593839)

(4, 27990902570735253597893048201476667301694693606602590357697539669086232722803)

(5, 3110777406661826982666985757116629894411061890859588248037290882151410167478)

Шифрування акцій

перша акція до шифрування:

(1,366984513475066187910800389457664267285695563640692338406558
7858120721823143)

Та після:

bhXBGeLy+vkJdVR0D1Due+MDz4AUGIe897MWQLtjYNOL+iCdAcyvi
MCvXt/0//
aLsM2juVM8tQHLNOyvjteblSnj8WgmWd0uFyJLt7yQqb2M0qPmlvRVaAT
rKQWE1J3EnezIUwYRAumEHtgzbqZwUtqM/PXmyiWVdoDN+y2caVQ=

Відновлений секрет

```
Recovered Secret 48468722958635381340480276230627209439649824273353758645046163201165456821345
```

```
Process finished with exit code 0
```

Співпадає з початковим секретом

В прикладі була продемонстрована (t, n) – схема розподілення секрету при $t = 3, n=5$. І секрет відновлювався з 3-х акцій(мінімально достатніх для коаліції) аналогічно працюватиме і для 4-х та 5-ти.

Якщо спробувати відновити секрет маючи лише 2 акції

```
79     print('Recovered Secret ',
80           recoverSecret(shares[:2]))
81
```

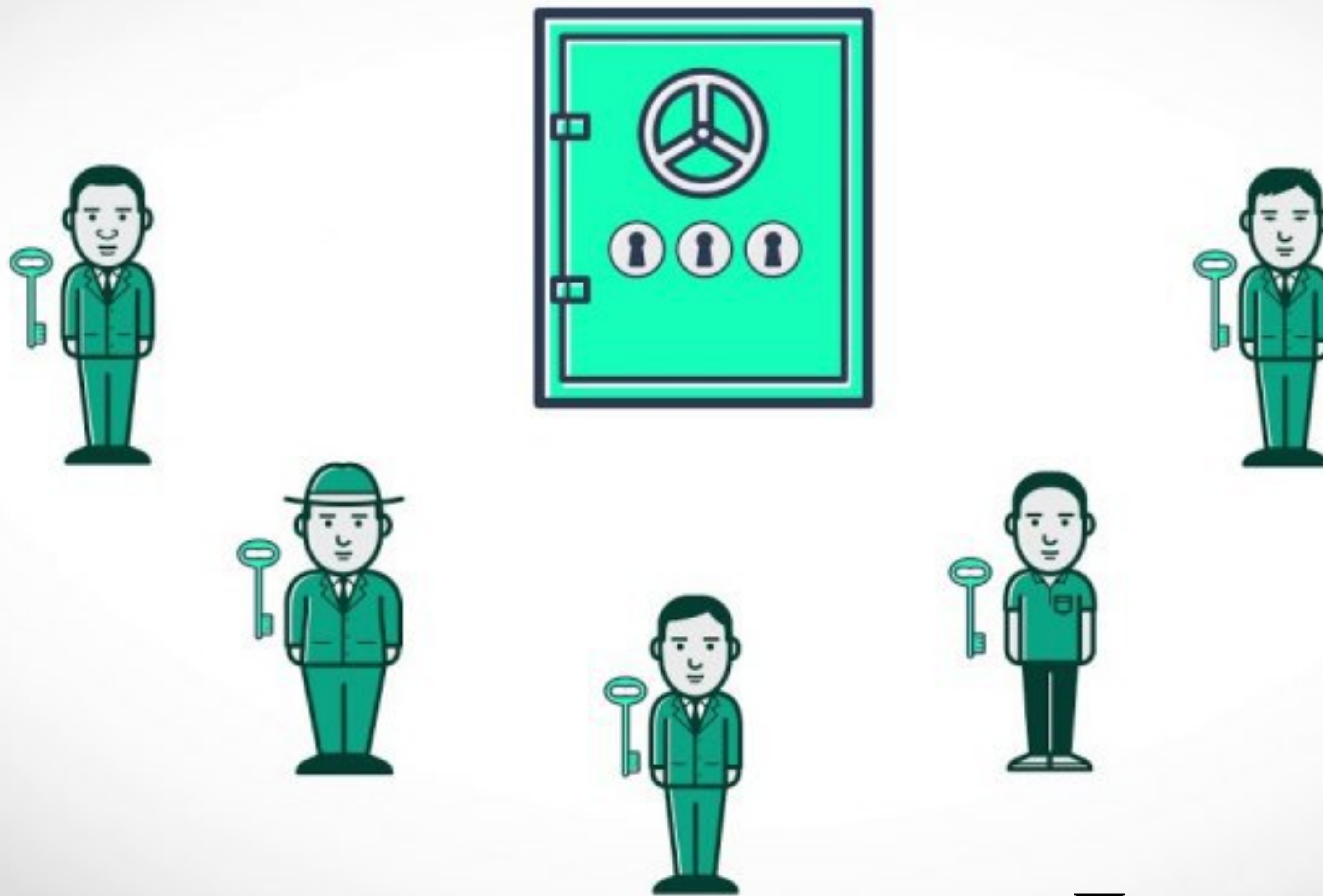
Shamir x

```
/Users/stasstepaniuk/venv/bin/python /Users/stasstepaniuk/Documents/Shamir.py
Secret: 20167156123036918554975902761094332159201257859537494301005833412214631021288
Shares:
(1, 31565749963126225570571223897784813152130291111137836237066402510499321741586)
(2, 18832755854384147582532748073497795227674705525162208958165641332914038083746)
(3, 39864218415468782302645967792577232312469493434430894484032341883415344867735)
(4, 36764093027722032019125390550679170479879662506123610794937712158046677273586)
(5, 9532379691143896731971016347803609729905212740240357890881752156808035301299)
Recovered Secret 44298744071868303558609699722071831076585876697113463515967163688084605399426

Process finished with exit code 0
```

Процес відновлення буде безуспішним

Розподіляймо секрет безпечно!



Дякую за увагу!