Quantum Time Capsules
&
Unknown Recipient Encryption

Dominique Unruh

University of Tartu

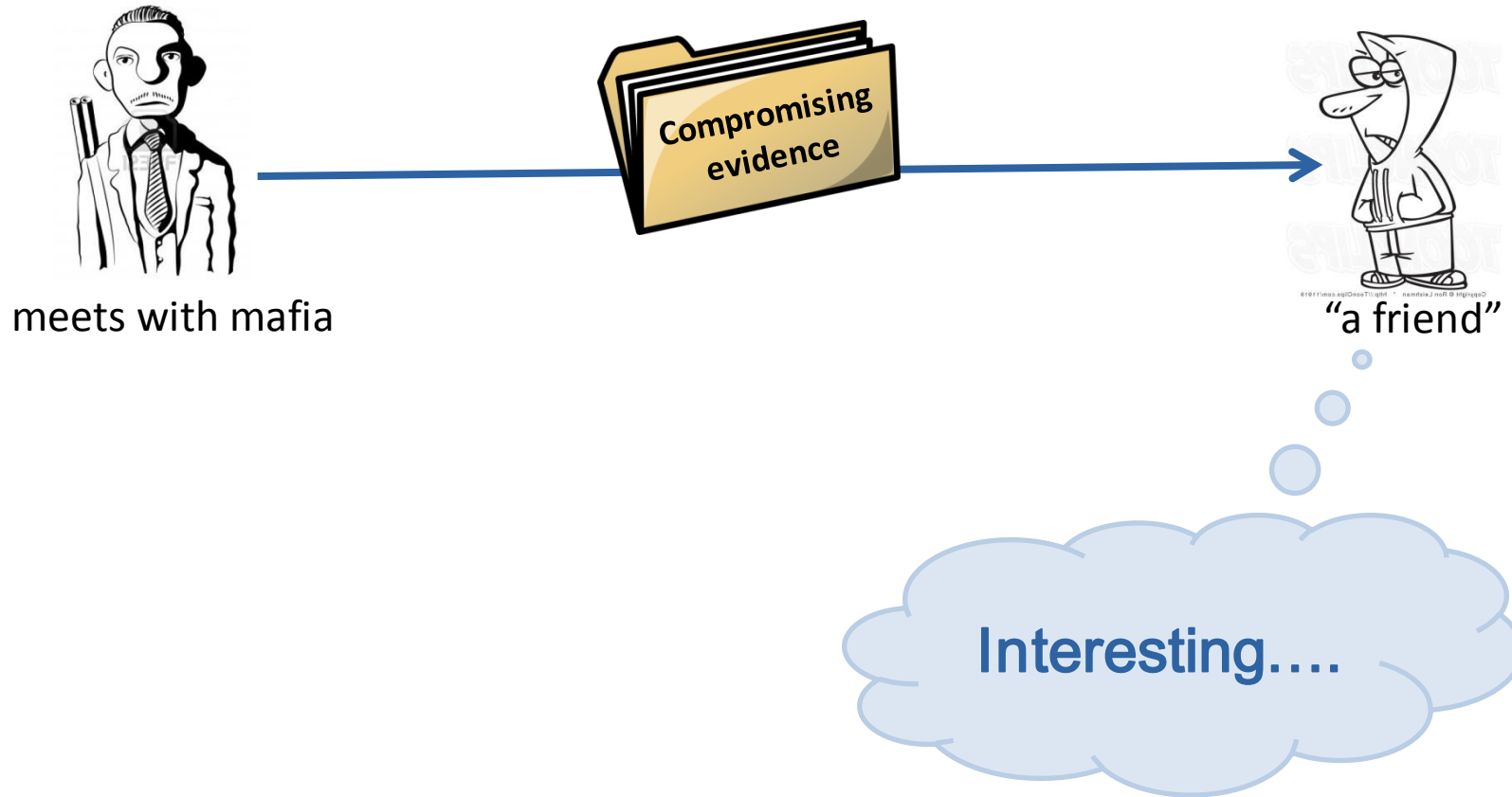# Meeting the Mafia

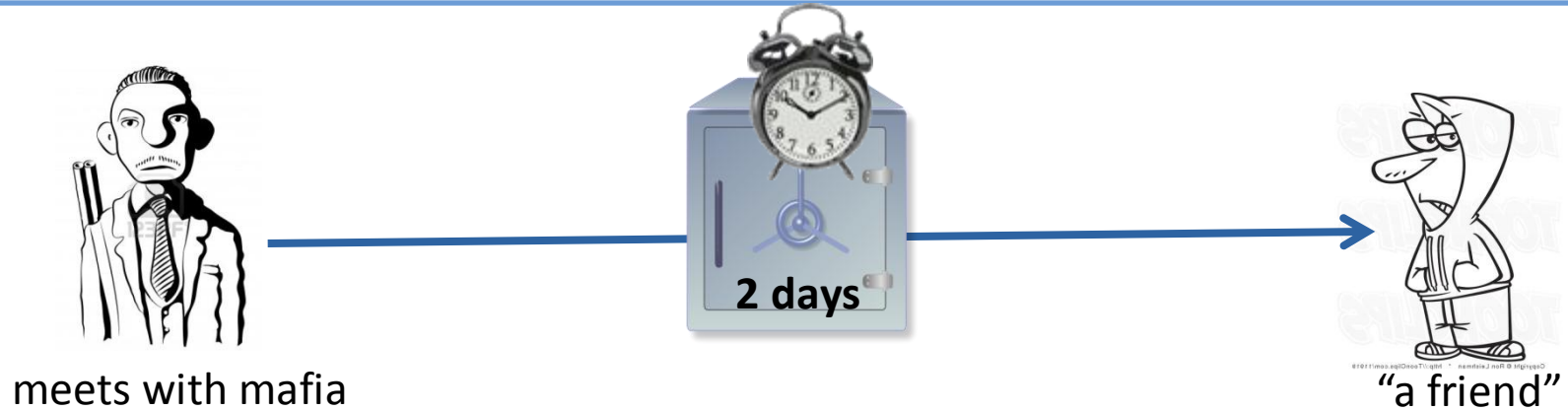meets with mafia
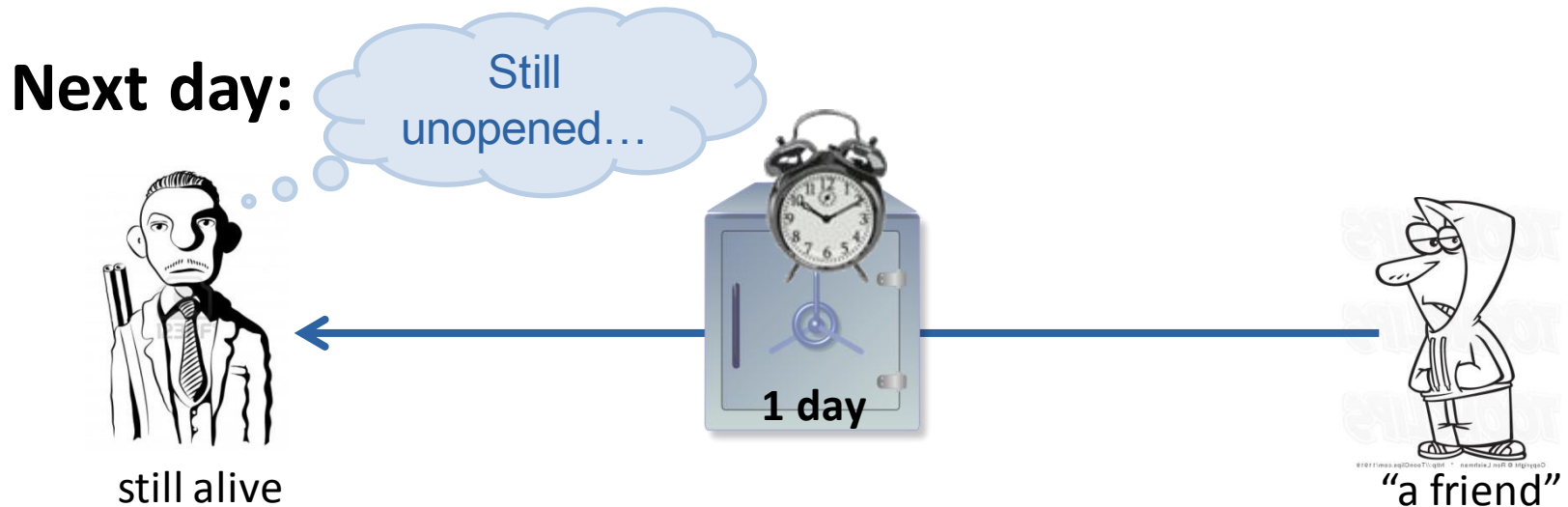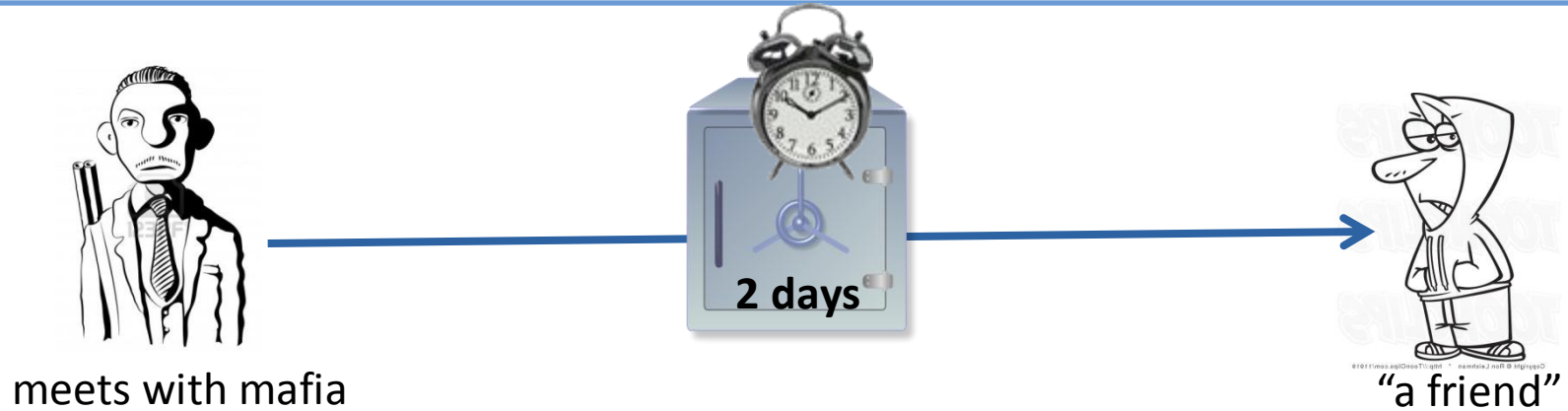
Compromising evidence

"a friend"

Meeting the Mafia

meets with mafia

Compromising evidence

"a friend"

Interesting....

Using "time capsules"

meets with mafia

2 days

"a friend"

Using "time capsules"

meets with mafia

2 days

"a friend"

Next day:

Still unopened…

still alive

1 day

"a friend"

Using digital time capsules…

meets with mafia

**Enc(msg)
(2 days)**

"a friend"

Next day: ???

still alive

**Enc(msg)
(1 day)**

Enc(msg)

"a friend"

Quantum Time Capsules

$$\mathbf{Enc}(B) \qquad |msg\rangle_B$$

Classical
time vault

Quantum
encoded msg

Revocation:

$$|msg\rangle_B$$

Unknown Recipient Encryption

Enc(msg)

Only one can decrypt

(before timeout)
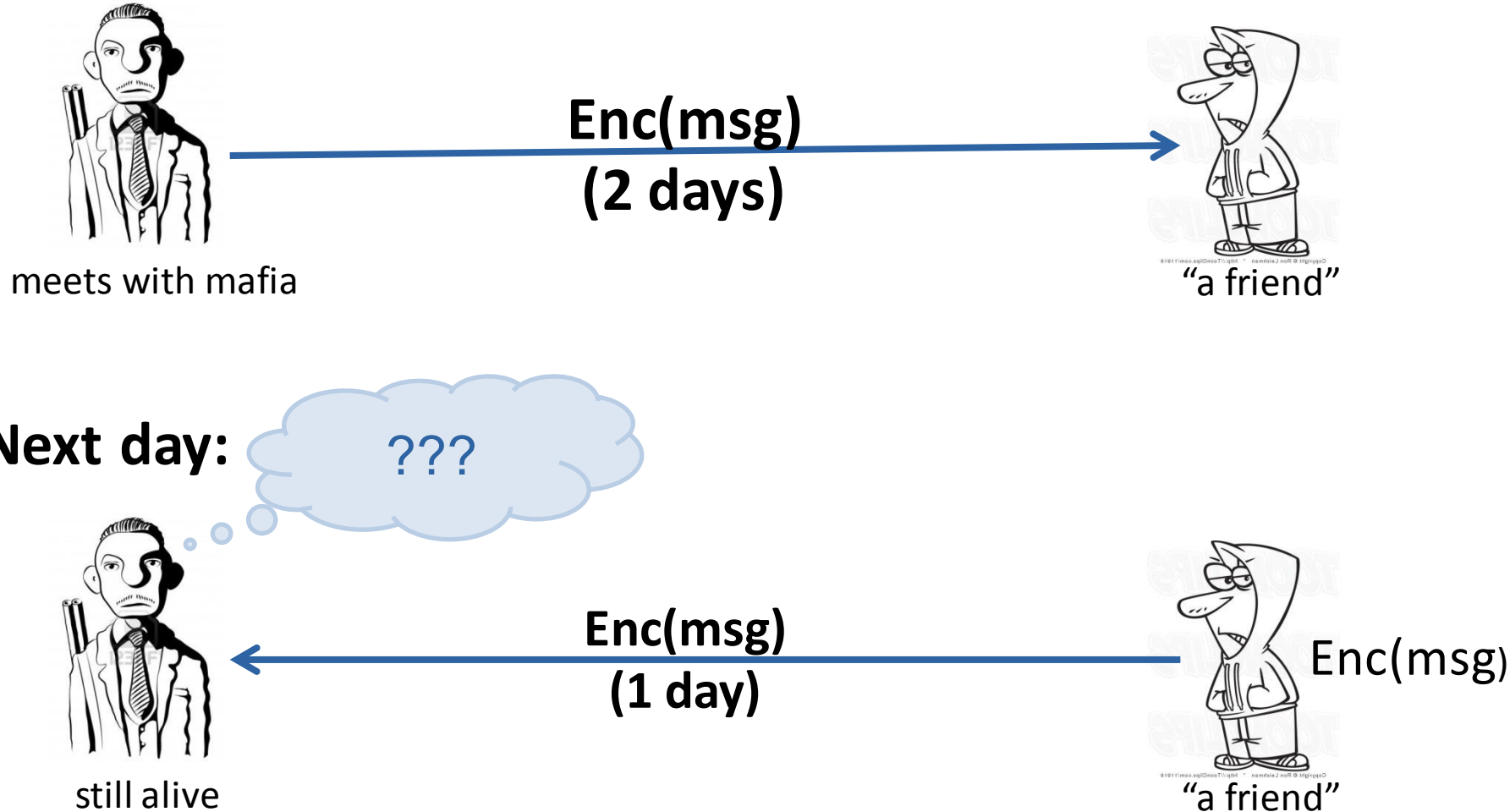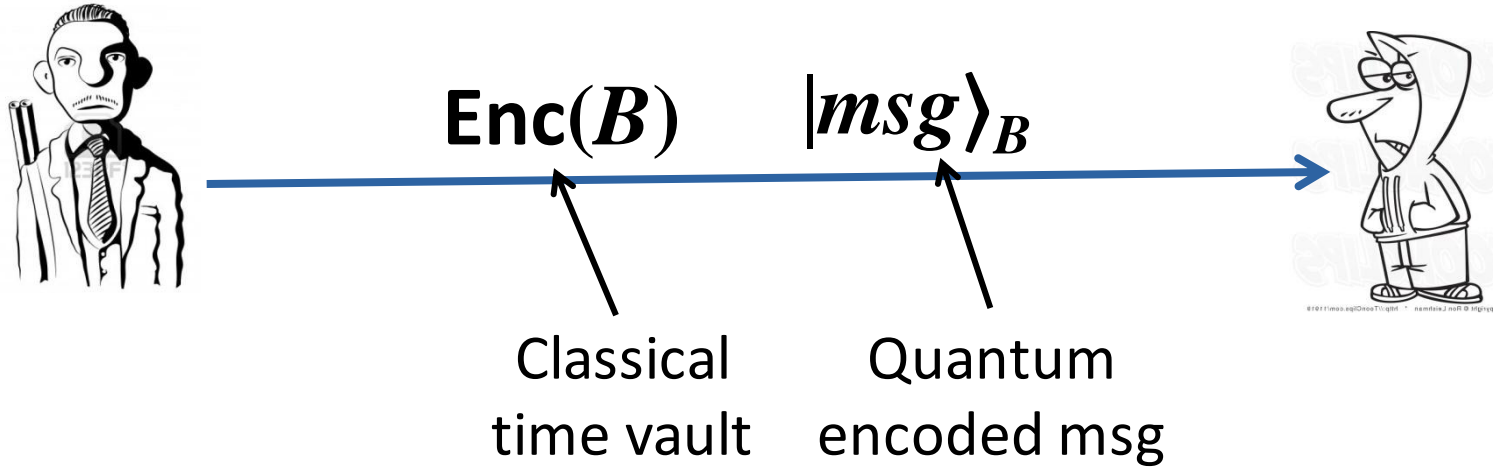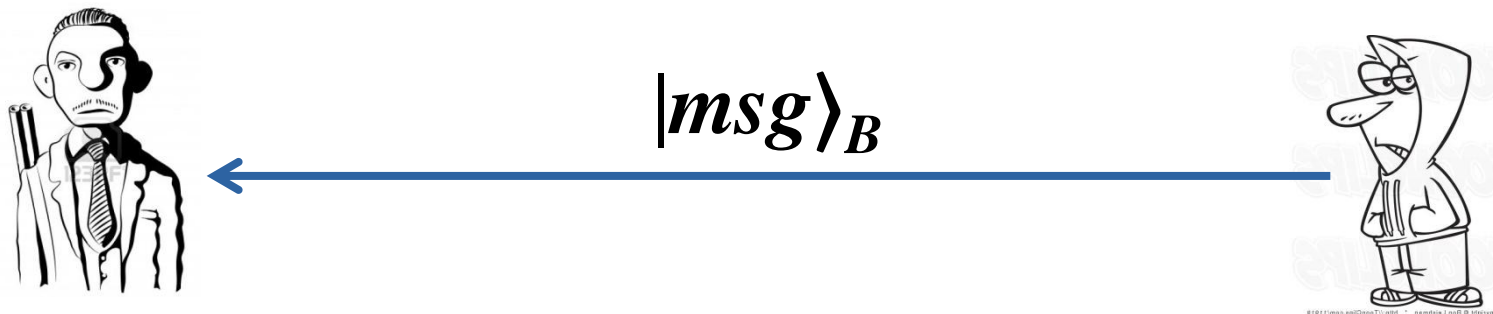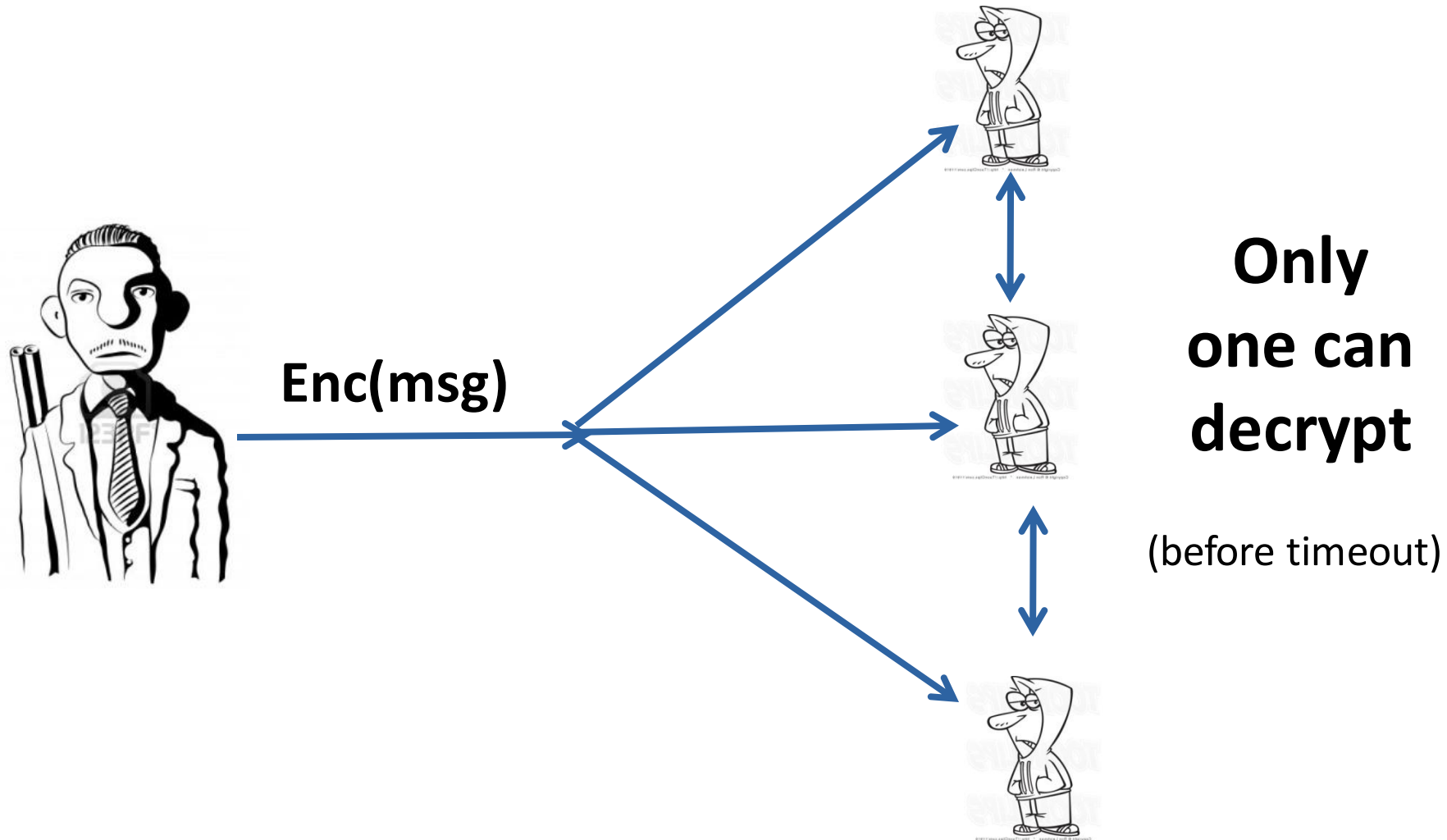
I thank for your attention