

# WHAT'S CRYPTOGRAPHY

Além da comunicação segura...

\* **assinatura digital**: No mundo físico quando assinamos um documento, nós escrevemos a assinatura no documento e essa assinatura é sempre a mesma.

→ e no mundo digital? Basta recortar e colar a assinatura? não...

\* **comunicação anônima**.

→ mix net  
→ bidirecional

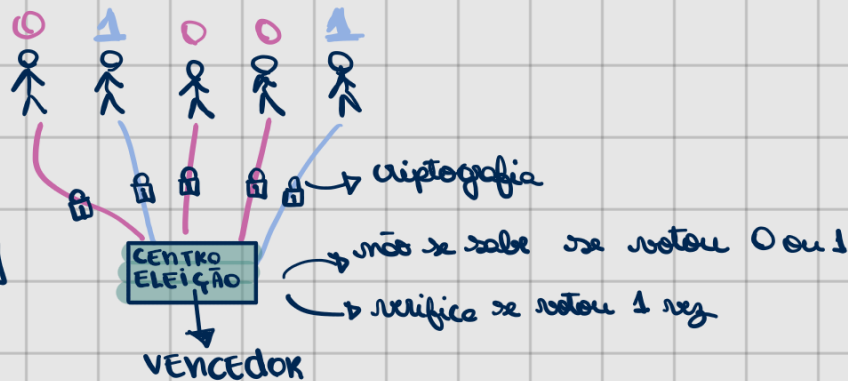
\* **dinheiro digital anônimo**: Imagine ir em uma loja, comprar um produto e a loja não sabe quem comprou.

→ PROBLEMA: Como prevenir que essa pessoa anônima duplique esse dinheiro / gaste 2x?

\* **protocolos**:

exemplo: eleição  
como computar votos sem expor alguém?

$VENCEDOR = [+ VOTOS]$

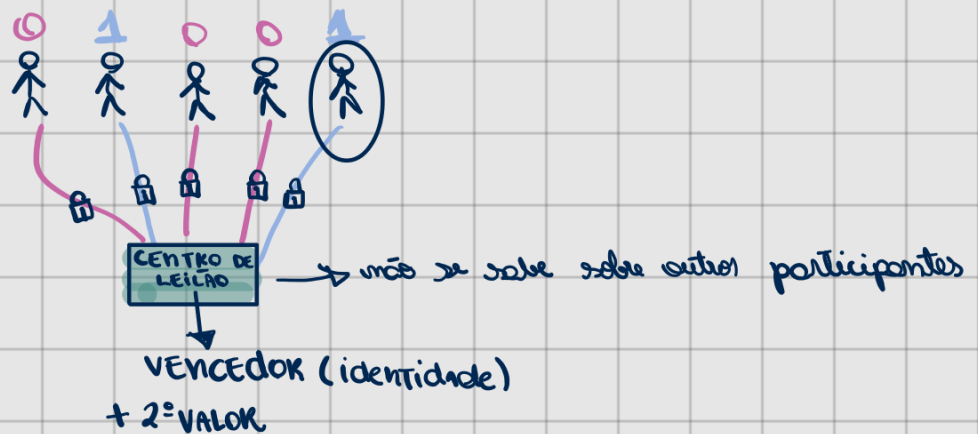


exemplo: leilão privado

mecanismo:

$VENCEDOR = [2^o VALOR + ALTO]$

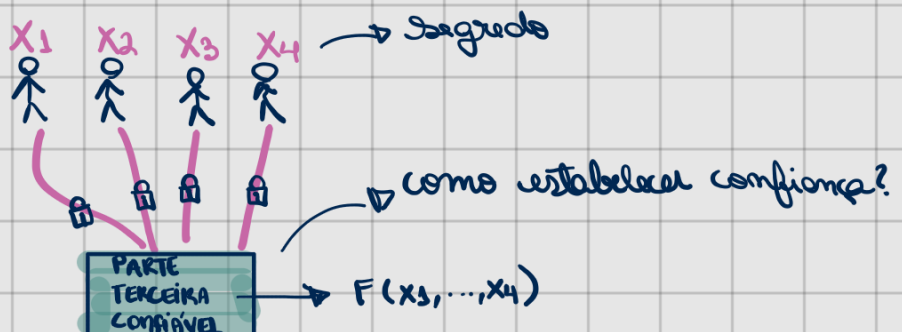
"VICKREY AUCTION"



exemplo: computação multipartidária segura

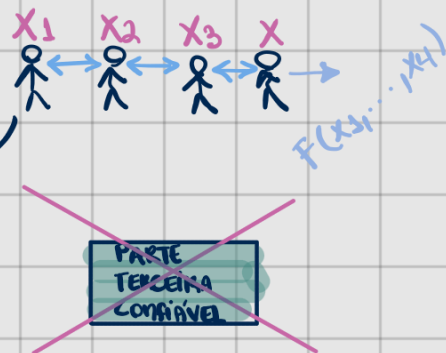
computar  $f(x_1, x_2, x_3, x_4)$   
uma função

sem que os outros participantes saibam os valores além dos próprios.

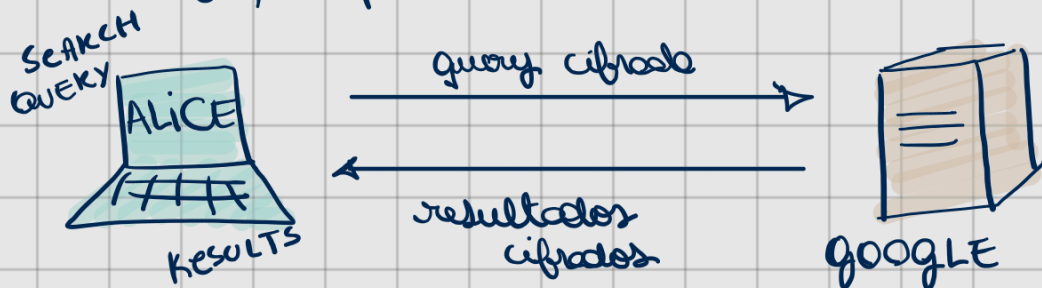


e se não quiser usar uma terceira parte:

não conversar entre si  
utilizando um protocolo



### \* terceirização privada:



### \* conhecimento zero (prova de conhecimento):

