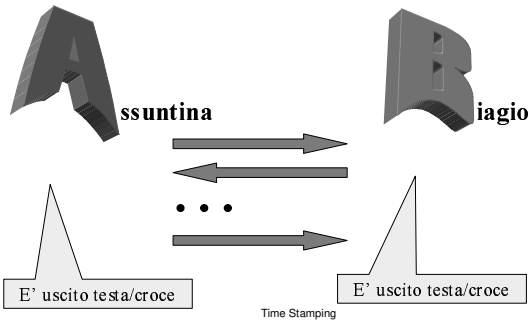
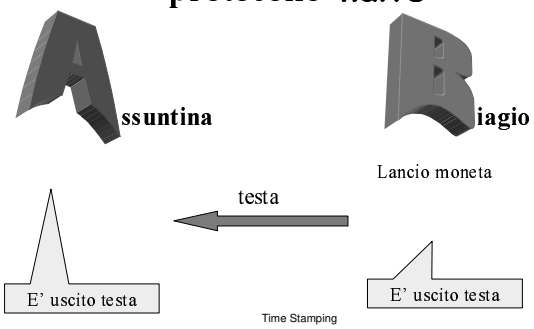
Protocolli Crittografici

- Lancio di una moneta
- Oblivious Transfer
- Blind Signature
- Moneta Elettronica
- Elezioni

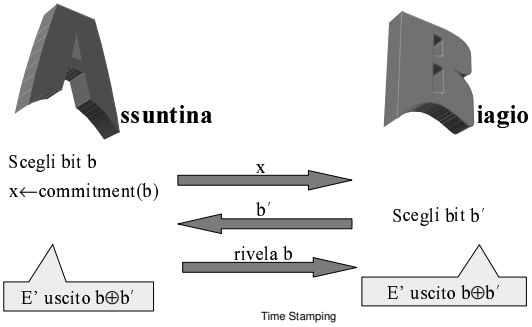
Lancio di una moneta



Lancio di una moneta protocollo naive



Lancio di una moneta



Commitment

x←commitment(b)

Equivalente digitale di una busta

- "Facile" da calcolare
- Dato x è "difficile" calcolare b
- "Facile" mostrare che x = commitment(b)
- "Difficile" mostrare che x = commitment(1-b)

Commitment

x←commitment(b)

b = predicato_difficile (x)

Esempio **$C = M^e \bmod n$**

$parità_{n,e}(C)$ = bit meno significativo di M

$$half_{n,e}(C) = \begin{cases} 0 & \text{se } M < n/2 \\ 1 & \text{se } M > n/2 \end{cases}$$

Crittografia probabilistica

Testo in chiaro $M = M_1 M_2 M_3 \ldots$

Testo cifrato $C = C_1 \ C_2 \ C_3 \ldots$

M_i = predicato_difficile (C_i)