# Protocolli Crittografici

- Poker Mentale
- Condivisione di segreti
- Lancio di una moneta
- Oblivious Transfer
- Blind Signature
- Moneta Elettronica
- Elezioni
- Certified email



# Mental Poker

- Poker senza carte, con giocatori "curiosi" ma "onesti"
- Tre giocatori: **A**nnarella, **B**iagio, **C**iro
- Cifratura e decifratura commutative:

$$D(E(x,k_1),k_2) = E(D(x,k_2),k_1)$$

Esempio: RSA con lo stesso modulo

[Shamir, Rivest, Adleman 1978]



# Mental Poker: B ottiene 5 carte


Cifro e permuto le 52 carte $E(x_1,k_A),\ldots,E(x_{52},k_A)$

$E(x_4,k_A),\ldots,E(x_{32},k_A)$ →

Scelgo 5 carte e le cifro

← $E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)$

Decifro i 5 valori

$E(x_5,k_B),\ldots,E(x_2,k_B)$ →

$x_5,\ldots,x_2$



# Mental Poker: C ottiene 5 carte


Invio le 47 carte cifrate da A

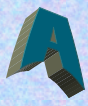
$E(x_4,k_A),\ldots,E(x_{32},k_A)$

**47 carte**



# Mental Poker: C ottiene 5 carte





Invio le 47 carte cifrate da A

Scelgo 5 carte e le cifro

$E(x_4,k_A),\ldots,E(x_{32},k_A)$ →

← $E(E(x_{31},k_A),k_C),\ldots,E(E(x_{50},k_A),k_C)$

**5 carte**



# Mental Poker: C ottiene 5 carte



Invio le 47 carte cifrate da A

Scelgo 5 carte e le cifro

$E(x_4,k_A),\ldots,E(x_{32},k_A)$ →

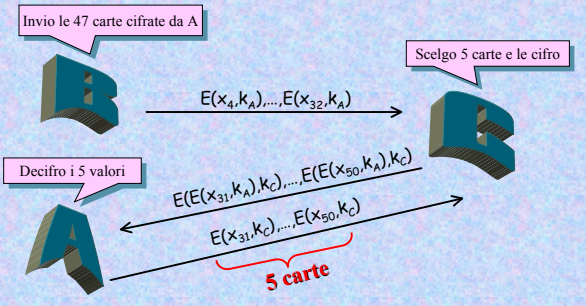
Decifro i 5 valori

← $E(E(x_{31},k_A),k_C),\ldots,E(E(x_{50},k_A),k_C)$

← $D(E(E(x_{31},k_A),k_C),k_A),\ldots,D(E(E(x_{50},k_A),k_C)k_A)$

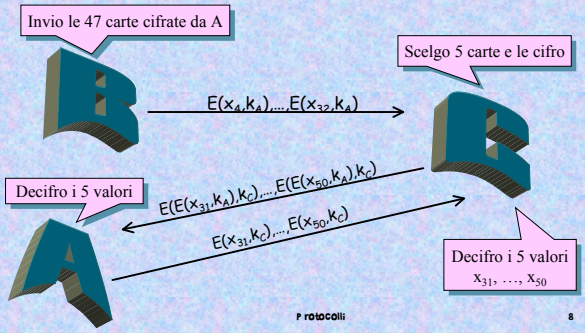
**5 carte**

# Mental Poker: C ottiene 5 carte



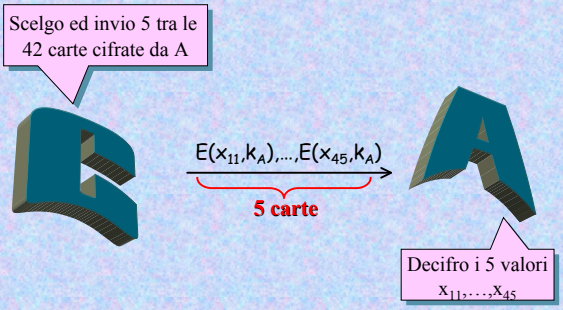



# Mental Poker: C ottiene 5 carte






# Mental Poker: A ottiene 5 carte






# Condivisione di segreti

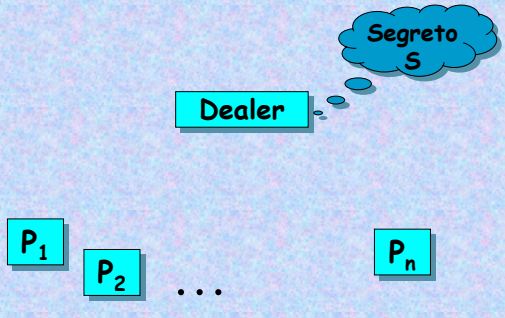
Un dealer vuole condividere un segreto S tra n partecipanti in modo che:

- k o più partecipanti possano ricostruire S
- k-1 o meno partecipanti non hanno alcuna informazione su S

[Adi Shamir, 1979]

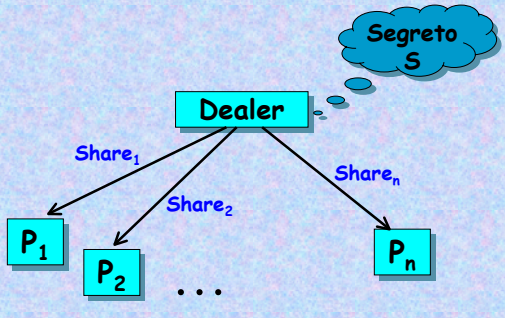


# Scenario

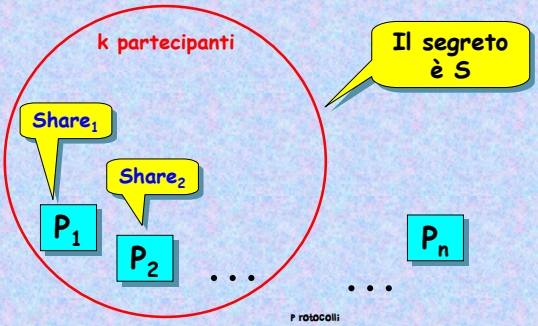





# Distribuzione del segreto

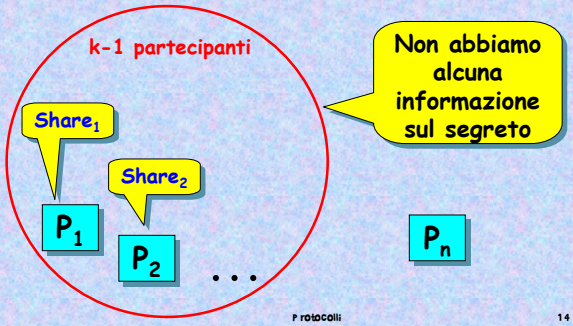


# Ricostruzione del segreto



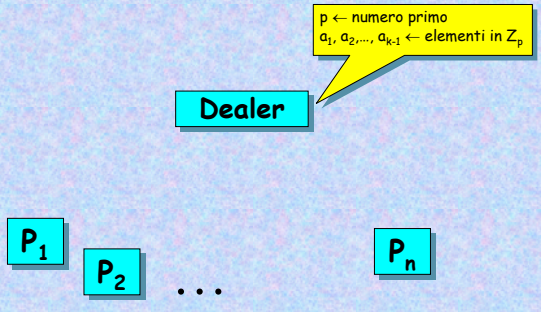



# Ricostruzione del segreto



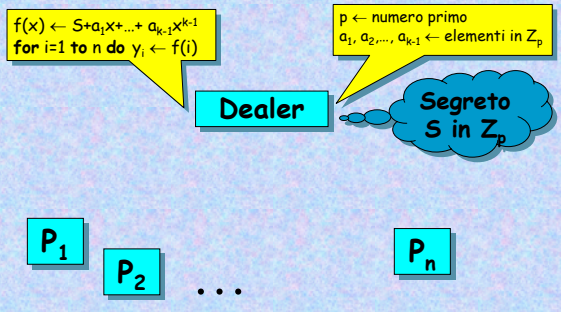



# Inizializzazione schema (k,n)



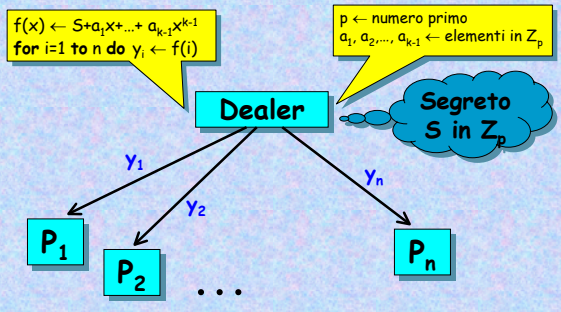



# Calcolo share schema (k,n)



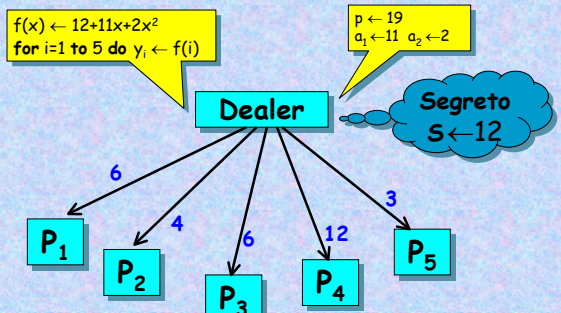



# Distribuzione share

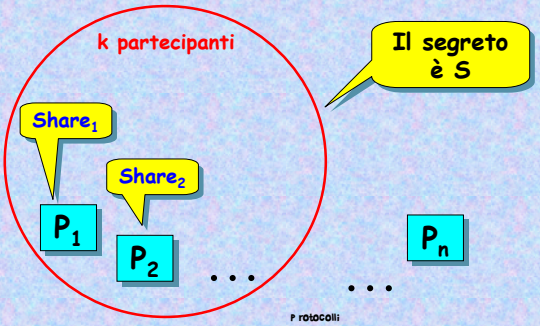





# Esempio schema (3,5)



# Ricostruzione del segreto






# Informazioni k partecipanti

- k equazioni: $y_i = S + a_1 i + \ldots + a_{k-1} i^{k-1}$ per $i = i_1, i_2, \ldots i_k$
- k incognite: $S, a_1, \ldots, a_{k-1}$
- Possono ricostruire il segreto!



# Esempio schema (3,5)

- $P_1$ sa che $6 = S + a_1 \cdot 1 + a_2 \cdot 1^2$
- $P_2$ sa che $4 = S + a_1 \cdot 2 + a_2 \cdot 2^2$
- $P_4$ sa che $12 = S + a_1 \cdot 4 + a_2 \cdot 4^2$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 12 \end{bmatrix}$$

det = (1-2)(1-4)(2-4) mod 19 = 13

Il sistema ha un'unica soluzione:

S=19 $a_1 = 11$ $a_2 = 2$



# Informazioni k partecipanti

Partecipanti $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$

$$\begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{k-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{k-1} \\ 1 & i_3 & i_3^2 & \cdots & i_3^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & i_k & i_k^2 & \cdots & i_k^{k-1} \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ y_{i_3} \\ \vdots \\ y_{i_k} \end{bmatrix}$$

Matrice di Vandermonde $\det = \prod_{1 \le r < t \le k} (i_r - i_t) \bmod p$

Il sistema ha un'unica soluzione



# Calcolo del Segreto

- Calcolo polinomio f(x)
- Formula di interpolazione di Lagrange
  - Grado k
  - $F(i_j)=y_{i_j}$

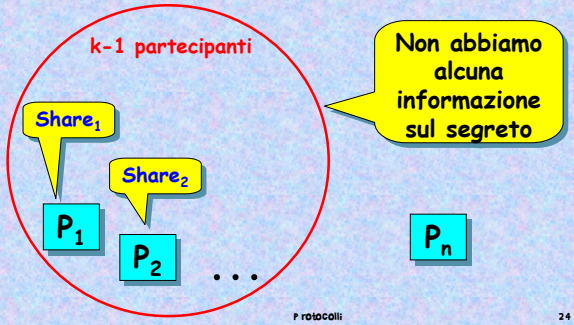
$$f(x) = \sum_{j=1}^{k} y_{i_j} \prod_{\substack{1 \le t \le k \\ t \ne j}} \frac{x - i_t}{i_j - i_t}$$

- Serve solo f(0)=S

$$f(0) = \sum_{j=1}^{k} y_{i_j} \prod_{\substack{1 \le t \le k \\ t \ne j}} \frac{i_t}{i_t - i_j}$$



# Ricostruzione del segreto



## Informazioni k-1 partecipanti

- k-1 equazioni: $y_i = S+a_1 i+\ldots+ a_{k-1} i^{k-1}$ per $i=i_1, i_2, \ldots i_{k-1}$
- k incognite: $S, a_1,\ldots, a_{k-1}$
- Non possono ricostruire il segreto
- Ogni segreto è equamente possibile



## Esempio schema (3,5)

- $P_1$ sa che $6 = S + a_1 \cdot 1 + a_2 \cdot 1^2$
- $P_2$ sa che $4 = S + a_1 \cdot 2 + a_2 \cdot 2^2$

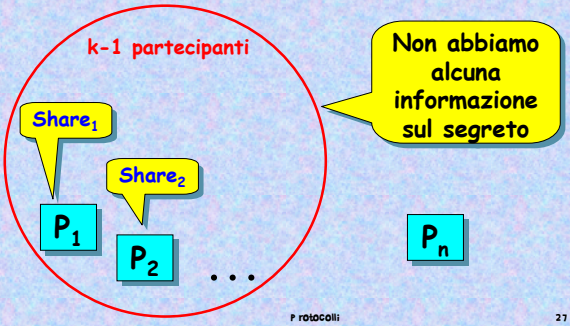
$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \end{bmatrix}$$

Il sistema ha 19 soluzioni:

| S | $a_1$ | $a_2$ |
|---|---|---|
| 0 | 10 | 15 |
| 1 | 18 | 6 |
| 2 | 7 | 16 |
| 3 | 15 | 7 |
| 4 | 4 | 17 |
| 5 | 12 | 8 |
| 6 | 1 | 18 |
| 7 | 9 | 9 |
| 8 | 17 | 0 |
| 9 | 6 | 10 |
| 10 | 14 | 20 |
| 11 | 3 | 11 |
| 12 | 11 | 2 |
| 13 | 0 | 12 |
| 14 | 8 | 3 |
| 15 | 16 | 13 |
| 16 | 5 | 4 |
| 17 | 13 | 14 |
| 18 | 2 | 5 |



## Ricostruzione del segreto






## Informazioni k-1 partecipanti

- k-1 equazioni: $y_i = S+a_1 i+\ldots+ a_{k-1} i^{k-1}$ per $i=i_1, i_2, \ldots i_{k-1}$
- k incognite: $S, a_1,\ldots, a_{k-1}$
- Ipotizzano un valore per il segreto S

  $S = S+a_1 0+\ldots+ a_{k-1} 0^{k-1}$

$$\begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{k-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{k-1} \\ 1 & i_3 & i_3^2 & \cdots & i_3^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & i_k & i_k^2 & \cdots & i_k^{k-1} \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ y_{i_3} \\ \vdots \\ y_{i_k} \end{bmatrix}$$

$i_k = 0$

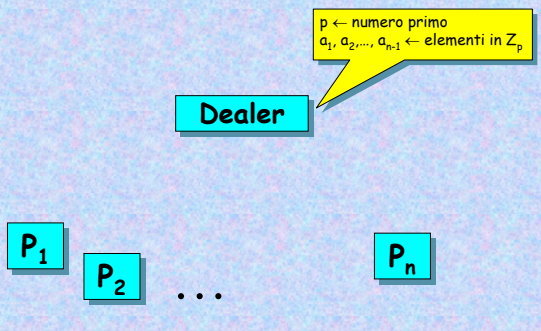
$$\det = \prod_{1 \le r < t \le k} (i_r - i_t) \bmod p$$

Matrice di Vandermonde

Il sistema ha un'unica soluzione

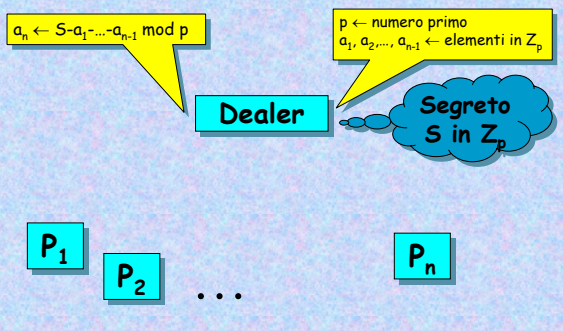


## Inizializzazione schema (n,n)

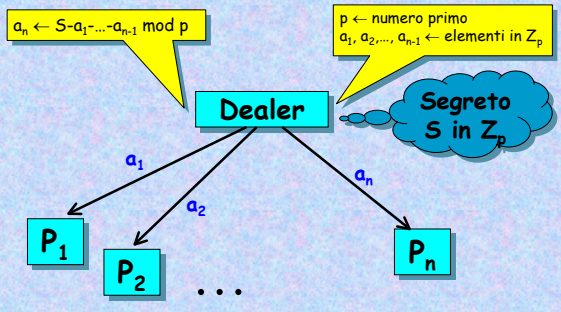





## Calcolo share schema (n,n)

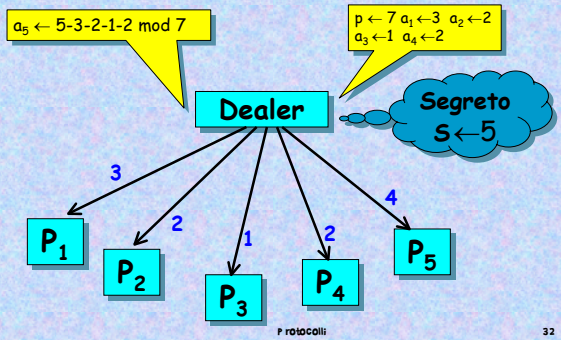


## Distribuzione share



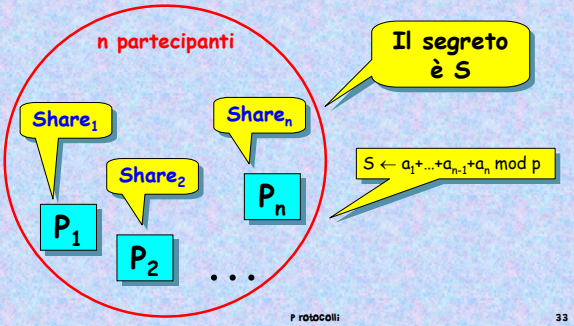



## Esempio schema (5,5)



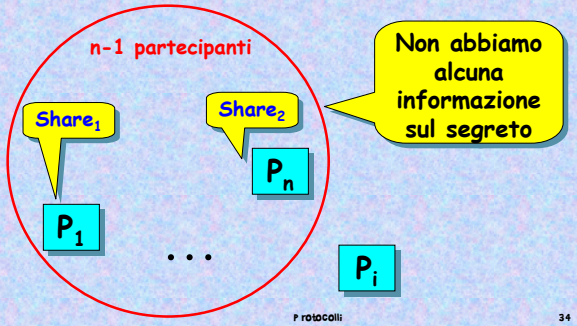



## Ricostruzione del segreto






## Ricostruzione del segreto






## Esempio schema (5,5)

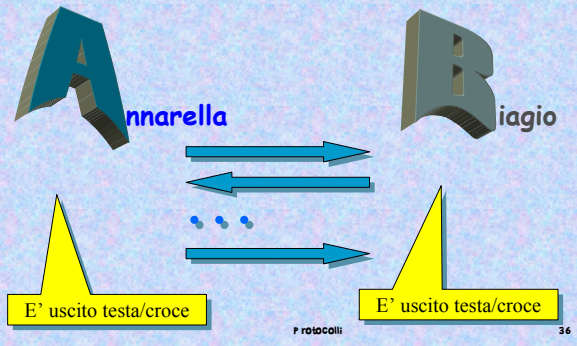
- $P_1$ sa che $3 = a_1$
- $P_2$ sa che $2 = a_2$
- $P_3$ sa che $1 = a_3$
- $P_5$ sa che $4 = S-a_1-a_2-a_3-a_4 \bmod 7$

Il sistema ha 7 soluzioni:

| S | $a_4$ |
|---|---|
| 0 | 4 |
| 1 | 5 |
| 2 | 6 |
| 3 | 0 |
| 4 | 1 |
| 5 | 2 |
| 6 | 3 |



## Lancio di una moneta



## Lancio di una moneta protocollo *naive*



Lancio moneta

testa

E' uscito testa

E' uscito testa



## Lancio di una moneta



Scegli bit b

x←commitment(b)

x

b´

Scegli bit b´

rivela b

E' uscito b⊕b´

E' uscito b⊕b´



## 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** $(C_i)$



## Blind Signature

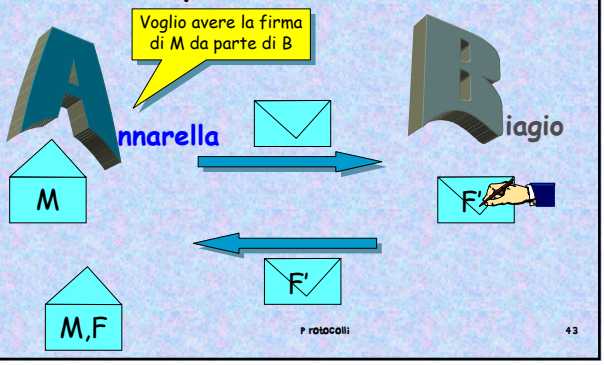
Voglio avere la firma di M da parte di B



F è la firma di M da parte di B

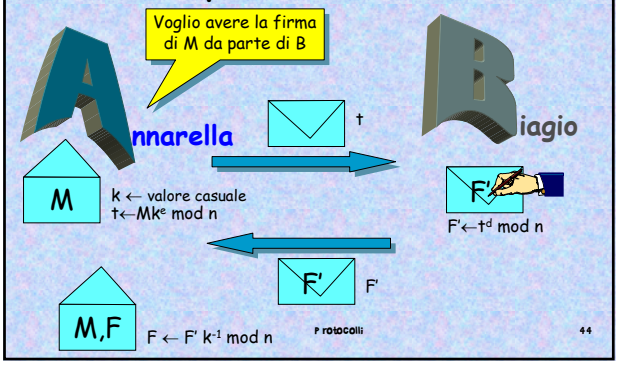
Non so che cosa ho firmato

# Blind Signature
## protocollo con busta



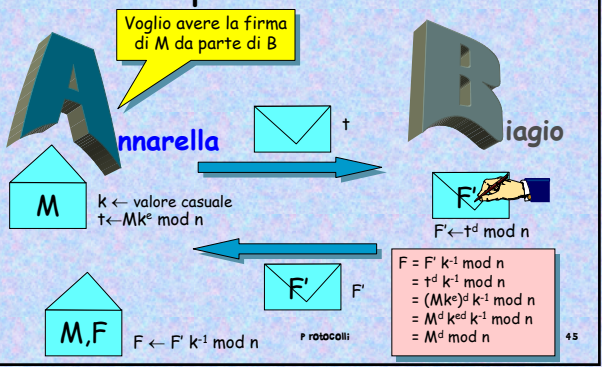



# Blind Signature
## protocollo con RSA





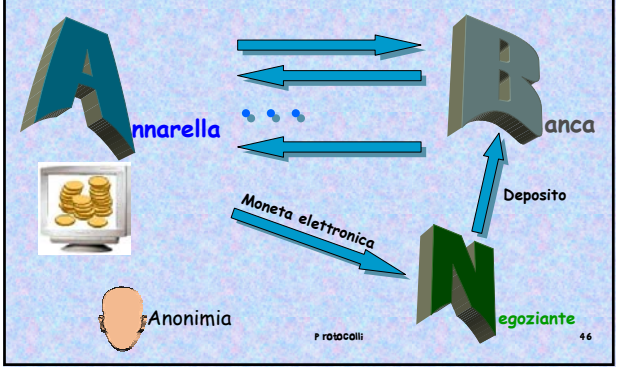

# Blind Signature
## protocollo con RSA




F = F' k^-1 mod n
= t^d k^-1 mod n
= (Mk^e)^d k^-1 mod n
= M^d k^ed k^-1 mod n
= M^d mod n

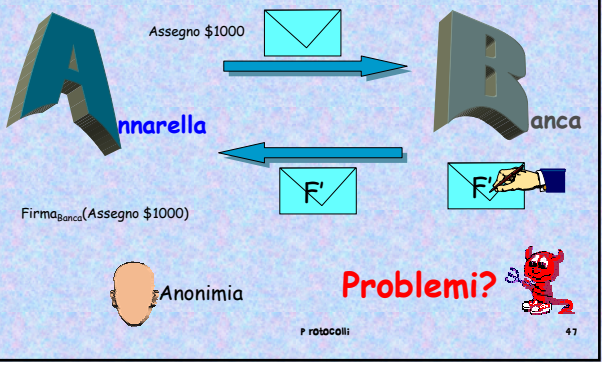


# Moneta Elettronica



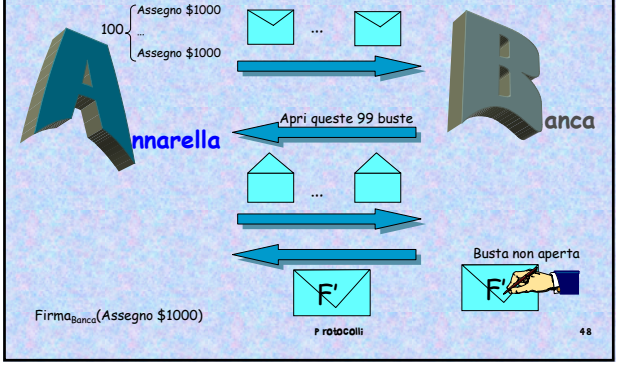



# Moneta Elettronica I

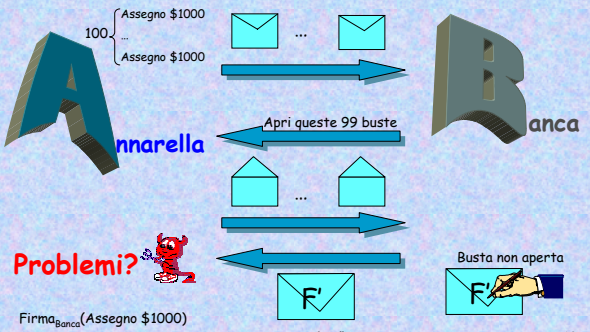





# Moneta Elettronica II



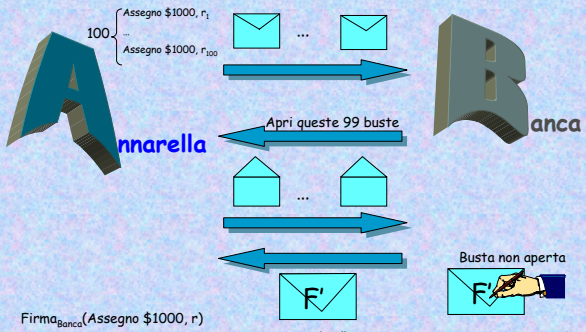
# Moneta Elettronica II




$Firma_{Banca}$(Assegno $1000)



# Moneta Elettronica III




$Firma_{Banca}$(Assegno $1000, r)