Mental Poker

- Poker senza carte, con giocatori "curiosi" ma "onesti"

- Tre giocatori: **A**ssuntina, **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]

Poker Mentale 0

Mental Poker: B ottiene 5 carte

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

$\xrightarrow{E(x_4,k_A),\ldots,E(x_{32},k_A)}$ **52 carte**

Poker Mentale 1

Mental Poker: B ottiene 5 carte

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

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

Scelgo 5 carte e le cifro

$\xleftarrow{E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)}$ **5 carte**

Poker Mentale 2

Mental Poker: B ottiene 5 carte

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

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

Scelgo 5 carte e le cifro

$\xleftarrow{E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)}$

Decifro i 5 valori

$D(E(E(x_5,k_A),k_B),k_A),\ldots,D(E(E(x_2,k_A),k_B)k_A)$ **5 carte**

Poker Mentale 3

Mental Poker: B ottiene 5 carte

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

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

Scelgo 5 carte e le cifro

$\xleftarrow{E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)}$

Decifro i 5 valori

$\xrightarrow{E(x_5,k_B),\ldots,E(x_2,k_B)}$ **5 carte**

Poker Mentale 4

Mental Poker: B ottiene 5 carte

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

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

Scelgo 5 carte e le cifro

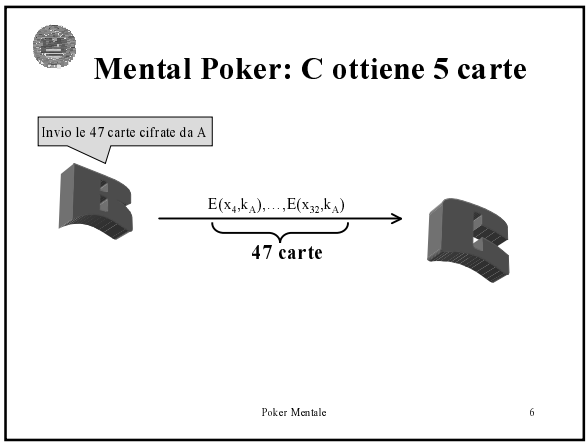
$\xleftarrow{E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)}$

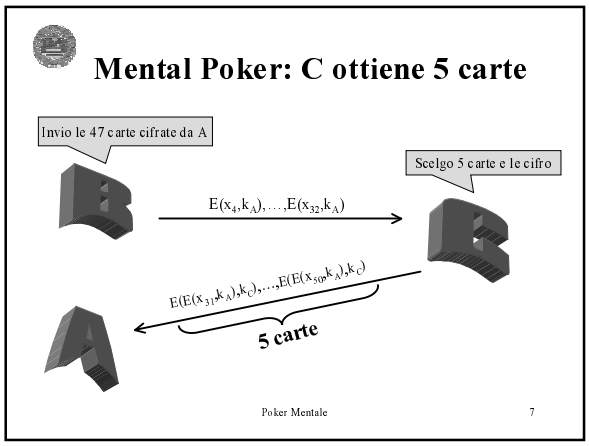
Decifro i 5 valori

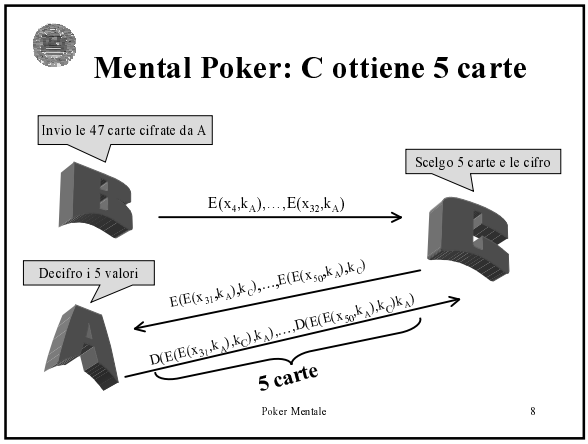
$\xrightarrow{E(x_5,k_B),\ldots,E(x_2,k_B)}$

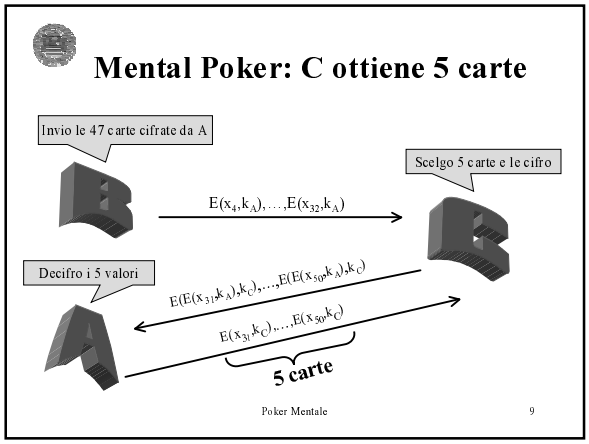
Decifro i 5 valori
$x_5,\ldots,x_2$

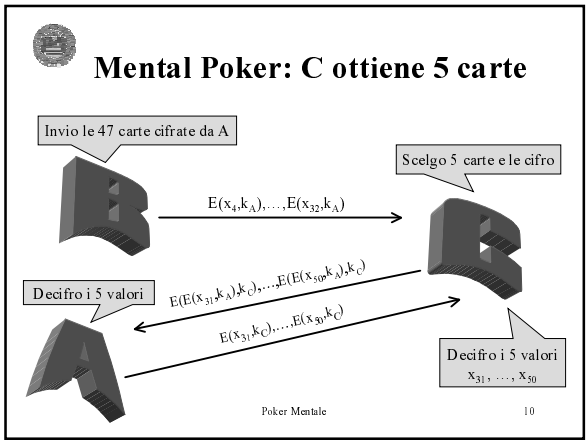
Poker Mentale 5

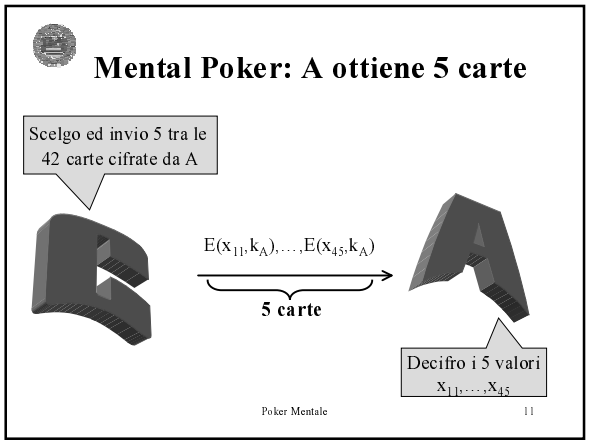

Mental Poker: C ottiene 5 carte
Invio le 47 carte cifrate da A
$E(x_4,k_A),\ldots,E(x_{32},k_A)$
47 carte
Poker Mentale 6


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
Poker Mentale 7


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
Poker Mentale 8


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
$E(E(x_{31},k_A),k_C),\ldots,E(E(x_{50},k_A),k_C)$
$E(x_{31},k_C),\ldots,E(x_{50},k_C)$
5 carte
Poker Mentale 9


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
$E(E(x_{31},k_A),k_C),\ldots,E(E(x_{50},k_A),k_C)$
$E(x_{31},k_C),\ldots,E(x_{50},k_C)$
Decifro i 5 valori
$x_{31}, \ldots, x_{50}$
Poker Mentale 10


Mental Poker: A ottiene 5 carte
Scelgo ed invio 5 tra le 42 carte cifrate da A
$E(x_{11},k_A),\ldots,E(x_{45},k_A)$
5 carte
Decifro i 5 valori
$x_{11},\ldots,x_{45}$
Poker Mentale 11