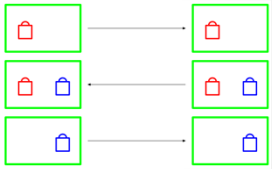
Doppio lucchetto

Il protocollo del doppio lucchetto

- A mette il suo messaggio per B in una scatola, che chiude con un lucchetto e invia a B.
- B mette il suo lucchetto alla scatola e la rispedisce ad A.
- A toglie il suo lucchetto e rispedisce la scatola a B.
- B toglie il suo lucchetto e legge il messaggio.
- La scatola non viaggia mai senza lucchetto
- Ne A ne B ha dovuto inviare all'altro la chiave del proprio lucchetto.
- E' possibile comunicare con sicurezza senza dover effettuare un preventivo scambio delle chiavi ! ! !



Proposte di implementqzione

- Prime operazioni da effettuare:
  - Definizione dell'alfabeto dei messaggi (caratteri)
  - Definizione dell'alfabeto del crittosistema (interi)
  - **Mappatura** dell'alfabeto dei messaggi nell'alfabeto del crittosistema
  - Tipi di mappatura:
    - 1 a 1 (un carattere – un numero)
      - ASCII 'A' = 65 …
      - Posizione del carattere nell'alfabeto 'A'=0 'B'=1 …
    - n a 1 (n caratteri un numero)
      - $c_1c_2c_3 = c_1*n^2+c_2n+c_3$
      - … numeri molto grandi

Doppio lucchetto (Cesare)

- Utente A usa Ke(A) per crittare e invia a B
- Utente B usa Ke(B) per cittare e rimanda ad A
- Utente A usa Kd(A) per decrittare e rimanda a B
- Utente B usa Kd(B) per decrittare
- Primo caso: mappatura 1 a 1
  - Sensibile ad analisi di frequenza
  - Individuato un carattere si individua automaticamente Kd
  - Facile attacco Forza Bruta
- Secondo caso: mappatura n a 1
  - Meno sensibile ad analisi di frequenza
  - Meno sensibile ad attacco Forza Bruta (molte più possibili chiavi)
  - Individuata una sequenza di caratteri si individua automaticamente Kd

Funzioni per Cesare

- f(x) = x+Ke mod n
- $f^{-1}(x)$ = x+Kd mod n
- $f^{-1}(f(x))$ = x

- Kd = n - Ke

Z_n con n primo

	0	1	2	3	4	5	6	7	8	9	10
f(x) = 5x mod n	0	5	10	4	9	3	8	2	7	1	6
f^{-1}(x) = 9f(x) mod n	0	1	2	3	4	5	6	7	8	9	10

- f(x) "mescola" l'insieme dei valori
- $f^{-1}(x)$ "riordina" l'insieme dei valori
- Le due funzioni sono moltiplicazioni modulo n
- 5 è intesa come Ke
- 9 è il reciproco di 5 modulo 11 è intesa come Kd
- (in PARI/GP:
  - 5 % 11 vale 5
  - 1/5 % 11 vale 9