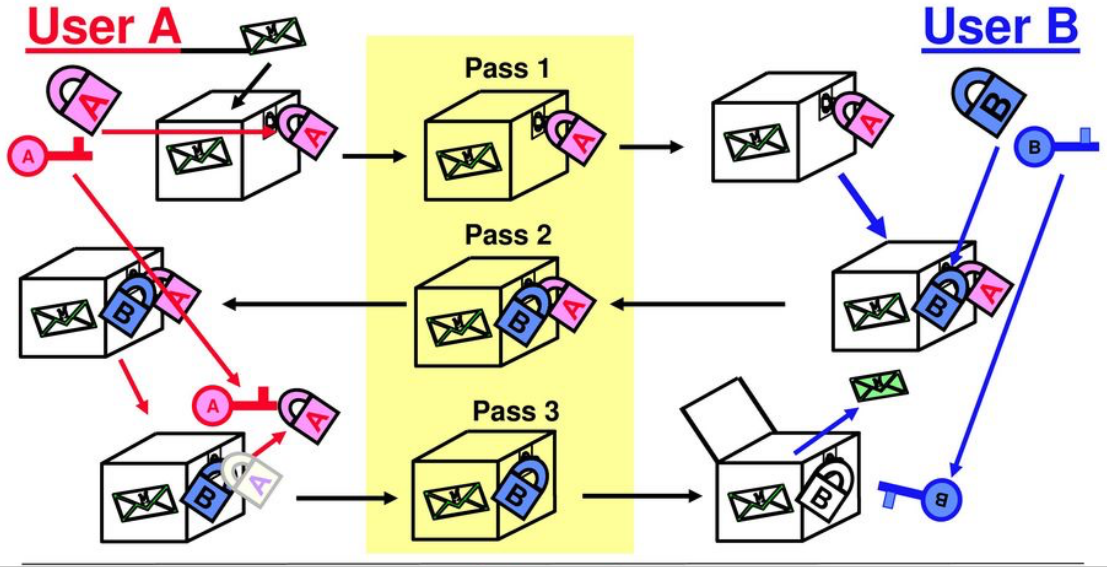
doppio lucchetto / 3-pass protocol



cifrario moltiplicativo

- in $\mathbb{Z}_n$, Alice sceglie e_A, d_A con $e_A d_A \equiv 1 \pmod{n}$
- in $\mathbb{Z}_n$, Bob sceglie e_B, d_B con $e_B d_B \equiv 1 \pmod{n}$
- messaggio $m \in \mathbb{Z}_n$:
- 1 pass $y_1 = m \cdot e_A \pmod{n}$
- 2 pass $y_2 = m e_A e_B \pmod{n}$
- 3 pass $y_3 = m e_A e_B d_A = m e_B \pmod{n}$
- Bob calcola $y_3 d_B = m$
- Problemi?
- chiunque può decifrare; $y_2 (y_1)^{-1} = e_B$
- $m = y_3 \cdot y_1 (y_2)^{-1}$

crittosistema di Massey-Omura

- Alice e Bob scelgono un gruppo ciclico G di ordine n
- spesso $G = \mathbb{F}_{2^k}^*$, $n = 2^k - 1$
- Alice sceglie e_A, d_A con $e_A d_A \equiv 1 \pmod{n}$
- Bob sceglie e_B, d_B con $e_B d_B \equiv 1 \pmod{n}$
- messaggio $m \in G$:
- 1 pass $y_1 = m^{e_A}$
- 2 pass $y_2 = m^{e_A e_B}$
- 3 pass $y_3 = m^{e_A e_B d_A} = m^{e_B}$
- Bob calcola $y_3^{d_B} = m$

esempio

- $G = \mathbb{F}_{2^5}^*$, $n = 2^5 - 1 = 31$, $\mathbb{F}_{32} \cong \mathbb{Z}_2[x]/(x^5 + x^2 + 1)$
- Alice sceglie $(e_A, d_A) = (7, 9)$; $7 \cdot 9 \equiv 1 \pmod{31}$
- Bob sceglie $(e_B, d_B) = (4, 8)$; $4 \cdot 8 \equiv 1 \pmod{31}$
- Alice vuole trasmettere il messaggio $01001 \to x^3 + 1$
- Alice calcola $y_1 = (x^3 + 1)^7 \equiv x^4 + x + 1 \pmod{x^5 + x^2 + 1}$
- Bob calcola $y_2 = y_1^4 = (x^4 + x + 1)^4 = x^3 + x$
- Alice calcola $y_3 = y_2^9 = (x^3 + x)^9 = x^3 + x^2 + x + 1$
- Bob decifra calcolando y_3^8 e riottiene $x^3 + 1$

autenticazione

- è indispensabile utilizzare ogni CS basato sul doppio lucchetto insieme a qualche forma di autenticazione
- l'attaccate Eve può sostituirsi a Bob senza problemi
- sceglie una coppia (e_E, d_E), intercetta le trasmissioni da Bob e sostituisce $m^{e_A e_B}$ con $m^{e_A e_E}$