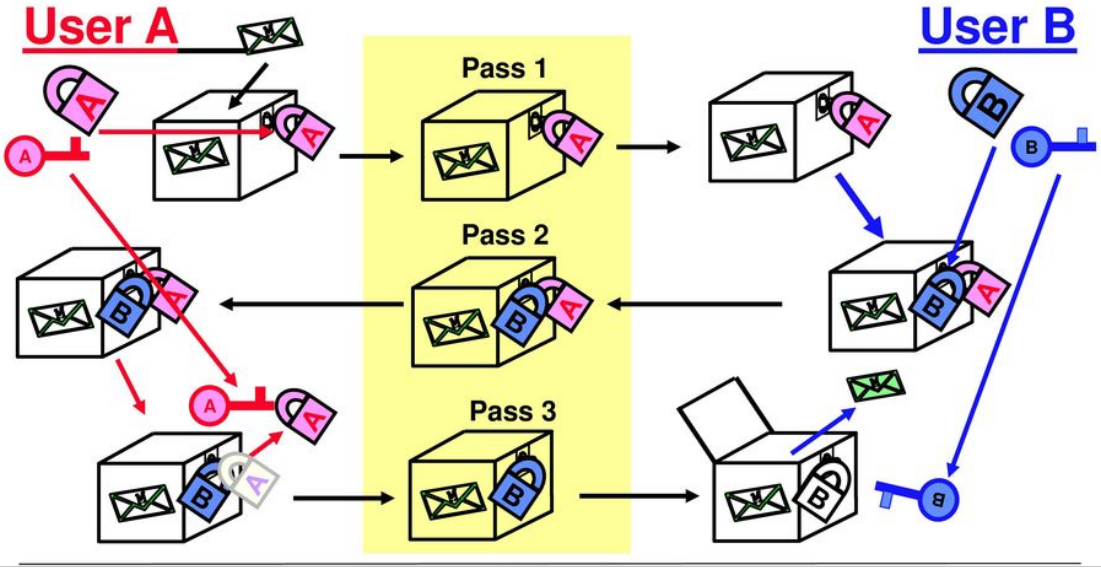
doppio lucchetto / 3-pass protocol



crittosistema di Shamir/Massey-Omura

- Alice e Bob scelgono un gruppo ciclico G di ordine n
- spesso $G = \mathbb{Z}_p^*$, $n = p - 1$, (Shamir)
- o $G = \mathbb{F}_{2^k}^*$, $n = 2^k - 1$ (Massey-Omura)
- 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-Shamir

- $G = \mathbb{Z}_{41}^*$, $n = 40$.
- Alice sceglie $(e_A, d_A) = (3, 27)$; $3 \cdot 27 \equiv 1 \pmod{40}$
- Bob sceglie $(e_B, d_B) = (13, 37)$; $13 \cdot 37 \equiv 1 \pmod{40}$
- Alice vuole trasmettere il messaggio 10
- Alice calcola $y_1 = 10^3 \equiv 16 \pmod{41}$
- Bob calcola $y_2 = 16^{13} \equiv 37 \pmod{41}$
- Alice calcola $y_3 = 37^{27} \equiv 16 \pmod{41}$
- Bob decifra calcolando y_3^{37} e riottiene 10

esempio-Massey-Omura

- $G = \mathbb{F}_{2^5}^*$, $n = 2^5 - 1 = 31$, $\mathbb{F}_{32} \cong \mathbb{Z}_2[x]/(x^5 + x^2 + 1)$
- 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 $\rightarrow x^3 + 1$
- 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 $m^{e_A e_E}$

protocolli

- un protocollo è costituito da una serie di passi (step) e coinvolge due o più persone (parti, entità) allo scopo di svolgere un incarico
- proprietà
  - ogni persona coinvolta deve conoscere il protocollo in anticipo
  - ogni partecipante deve eseguire le disposizioni del protocollo
  - il protocollo non deve essere ambiguo
  - il protocollo deve essere completo
- un protocollo crittografico è un protocollo che utilizza la crittografia

protocolli

- le parti si chiamano Alice, Bob, Carol, Davide,...
- a volte c'è un super-user chiamato Trent
- abbiamo già visto esempi di protocolli
  - scambio della chiave
  - scelta di un crittosistema e trasmissione di un messaggio cifrato
  - firma digitale

secret splitting – divisione di un segreto

- solo il presidente della ACME conosce la ricetta della ACME-cola^{TM}
- se comunica la ricetta a un suo collaboratore, questi la può rivendere alla concorrenza
- si vuole un metodo che consenta di dividere l'informazione fra due o più collaboratori
- in modo che l'informazione che si dà a un singolo non consenta di risalire alla ricetta completa
- ma solo la conoscenza di ogni "parte" di informazione permetta di ricostruire il segreto

secret splitting

- Trent vuole dividere un segreto fra Alice e Bob
- il segreto è un messaggio M – che pensiamo come una stringa binaria di lunghezza l
- Trent genera in maniera casuale un'altra stringa binaria r di lunghezza l
- calcola lo XOR fra M e r:

$$s = M \oplus r$$

- comunica r ad Alice e s a Bob
- Alice e Bob insieme possono ricostruire $M = s \oplus r$
- ma la conoscenza solo di s o solo di r non dà alcuna informazione su M
- di fatto, Trent cifra il messaggio con un one-time pad e dà il testo cifrato a Bob e la chiave ad Alice; abbiamo provato che l'one-time pad è a segretezza perfetta

secret splitting

- questo schema si generalizza immediatamente
- se Trent deve dividere il segreto M fra k "collaboratori" $A_1, A_2, \ldots A_k$
- genera $k-1$ stringhe binarie $r_1, r_2, \ldots r_{k-1}$ di lunghezza l
- calcola $s = M \oplus r_1 \oplus r_2 \cdots \oplus r_{k-1}$
- comunica r_1 a A_1, r_2 a A_2, $\ldots r_{k-1}$ a A_{k-1}e s a A_k
- in questo protocollo, l'unico modo per ricostruire il segreto è avere accesso a tutte le informazioni parziali