altri usi della crittografia

- finora abbiamo usato la crittografia in modo classico: per nascondere il contenuto di un messaggio
- quindi ottenere una comunicazione "privata" su un canale "aperto"
- molti altri usi della crittografia
- utilizzare la crittografia per verificare l'integrità di un messaggio
- collegato anche all'autenticazione
- in questo momento ci interessa garantire l'integrità senza mascondere il contenuto del messaggio

- privacy $\neq$ integrità
- il fatto di cifrare non ci protegge da manipolazione del testo da parte di un avversario
- particolarmente chiaro nel caso di cifrari a flusso
- vero anche per cifrari a blocchi

MAC – message authentication code

- scopo: ogni modifica del messaggio da parte di un avversario viene rilevata
- serve - anche qui - un segreto comune alle due parti della comunicazione (Alice e Bob)
- Alice e Bob condividono una procedura (pubblica) e una chiave (privata)

MAC – message authentication code

- Alice deve trasmettere il messaggio x a Bob: usando la chiave k calcola una tag t per il messaggio:

$$t = \mathrm{mac}_k(x)$$

- Bob riceve (x, t)
- ha una procedura di verifica (dipendente dalla chiave)
- applicata alla coppia (x, t), la procedura dice a Bob se t è una tag corretta per il messaggio x

MAC – definizione formale

Un MAC è una 5-pla $(\mathcal{P}, \mathcal{T}, \mathcal{K}, \mathcal{M}, \mathcal{V})$ dove

1. $\mathcal{P}$ è un insieme finito di possibili messaggi
2. $\mathcal{T}$ è un insieme finito di possibili tag
3. $\mathcal{K}$, lo spazio delle chiavi, è un insieme finito di possibili chiavi
4. $\forall k \in \mathcal{K}$ c'è un algoritmo di generazione di tag $\text{mac}_k \in \mathcal{M}$ e un corrispondente algoritmo di verifica $\text{ver}_k \in \mathcal{V}$.
5. $\text{mac}_k : \mathcal{P} \to \mathcal{T}$ e $\text{ver}_k : \mathcal{P} \times \mathcal{T} \to \{V, F\}$ sono funzioni tali che $\forall x \in \mathcal{P}$ e $\forall y \in \mathcal{T}$ vale

$$\text{ver}_k(x, t) = \begin{cases} V & \text{se } t = \text{mac}_k(x), \\ F & \text{se } t \neq \text{mac}_k(x) \end{cases}$$

MAC – attacchi

- cosa vuol dire che un MAC "funziona"?
- all'avversario Eve dev'essere impossibile ottenere una falsificazione esistenziale
- vogliamo che a Eve sia impossibile produrre una coppia (x, t) che supera l'algoritmo di verifica
- per qualunque messaggio x – anche scelto da Eve (e per esempio privo di senso)

MAC da cifrari a blocchi

- idea base: usare un cifrario a blocchi
- la tag è la cifratura del messaggio $t = e_k(x)$
- si trasmette il testo in chiaro assieme al corrispondente testo cifrato
- Bob riceve (x, t); conosce la chiave k
- calcola la cifratura di x, $y = e_k(x)$
- accetta il messaggio se $y = t$, rifiuta altrimenti