Crittografia: opportunità e rischi

Prof. Antonio Lioy

< lioy @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

EU-GDPR art. 32

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento,

come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,

il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali

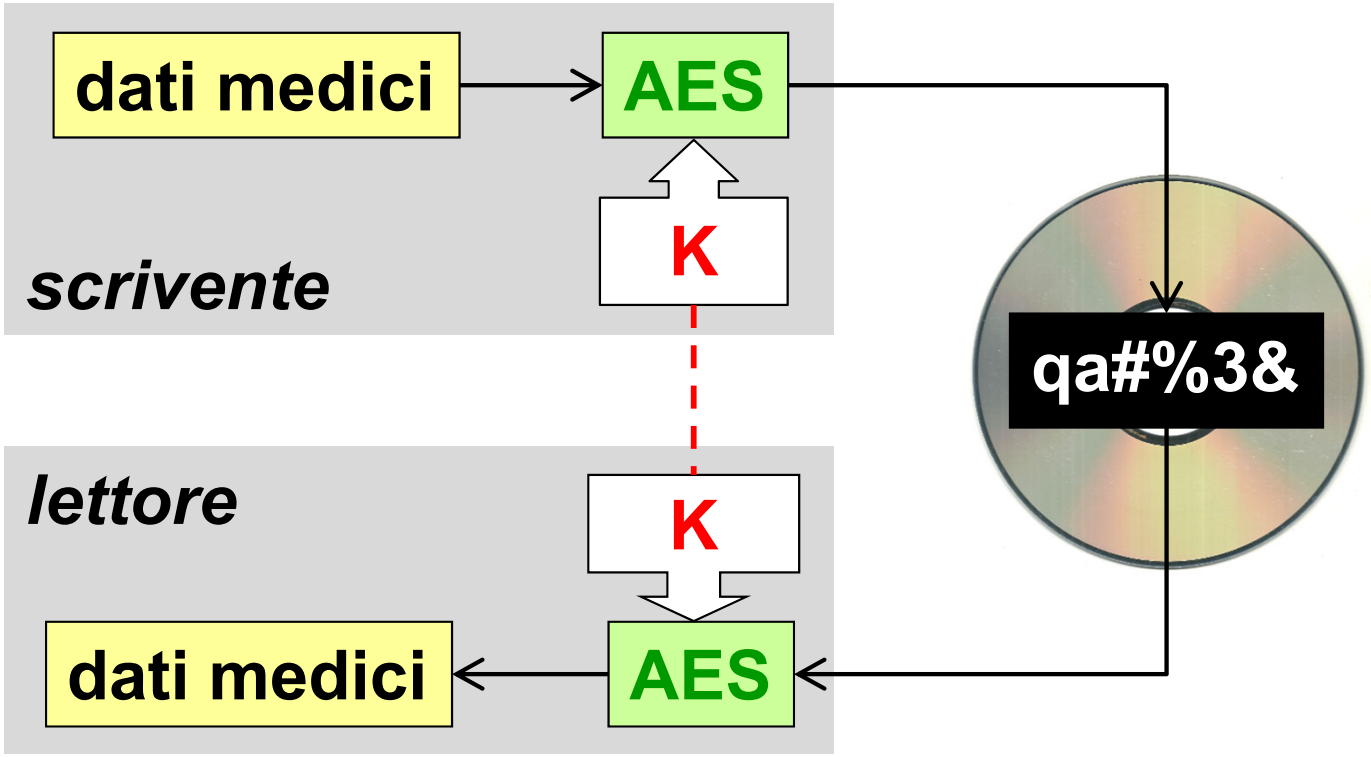
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Cifratura simmetrica (I)

- riservatezza delle trasmissioni
- chiave unica e comune a mittente e ricevente
- basso carico di elaborazione > OK cifratura veloce in rete
- problema: come condividere (in modo sicuro) la chiave segreta tra mittente e ricevente?

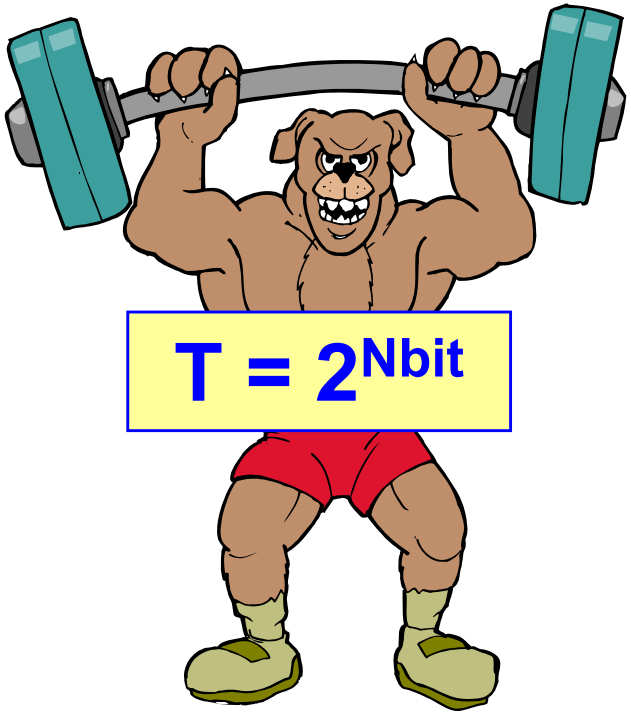
Cifratura simmetrica (II)

- riservatezza dei dati
- chiave unica e comune a scrivente / lettore
- basso carico di elaborazione > OK per grosse moli di dati
- problema: come conservare (in modo sicuro) la chiave?



Lunghezza delle chiavi segrete

- **se:**
  - l'algoritmo di crittografia è stato ben progettato
  - le chiavi - lunghe Nbit (128…256 bit) - sono tenute segrete
- **… allora l'unico attacco possibile è l'attacco esaustivo (o brute force) che richiede un numero di tentativi pari a**

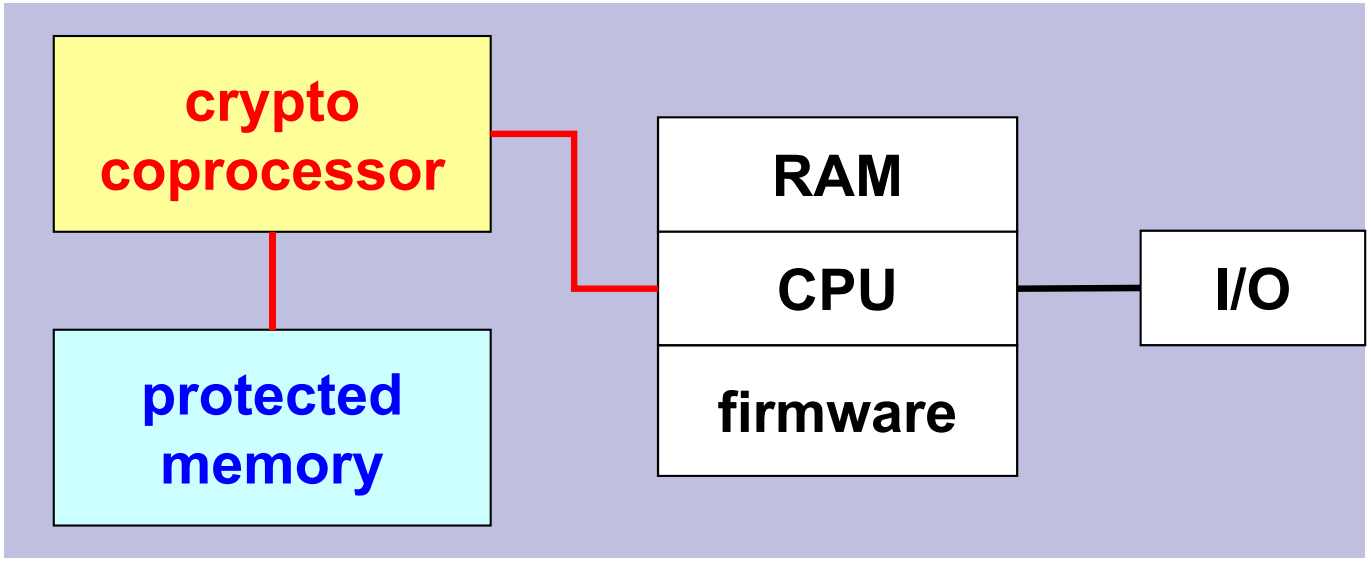


Conservazione / recupero delle chiavi

- **provare tutte le possibili chiavi (?!)**
- **… per ottenere accesso illecito o illegale ai dati cifrati**
- **… o per decifrare i dati quando si "perde" la chiave ☹**
- **implementare un sistema di cifratura che depositi una copia di ogni chiave in uno specifico deposito sicuro**
  - es. doppia password di accesso (due persone indipendenti)
- **usare specifici sistemi:**
  - dispositivi hardware
    - HSM (Hardware Security Module)
  - servizi cloud (es. Google, Amazon) con controllo accessi per l'uso delle chiavi
    - KMS (Key Management Service)
- **ma questo non esclude atti individuali (rischio!)**

HSM (Hardware Security Module)

- **acceleratore crittografico per server**
  - memoria protetta per chiavi crittografiche
  - capacità autonome di cifratura (per firma digitale e segretezza dei dati)
- **varie forme: scheda PCI o dispositivo esterno (USB, SCSI, …) o dispositivo di rete IP (netHSM)**
- **API per integrazione in vari servizi**



Autenticazione ed integrità

- verifica che i dati (trasmessi o memorizzati) siano autentici e non modificati
- chiave unica e comune a mittente e ricevente
- bassissimo carico di elaborazione > OK per rete e dischi