



# Crittografia Moderna

A.A. 2025-26



Segretezza Perfetta: nozioni

# Segretezza perfetta

---

- ▶ Ci occuperemo di schemi di cifratura **perfettamente sicuri**



confidenzialità / riservatezza

- ▶ Avversari di potere computazionale **illimitato**
- ▶ Useremo definizioni matematiche precise e prove
- ▶ Nessuna assunzione!



Inerenti limitazioni  giustificano la necessità di assunzioni

- ▶ Useremo esperimenti ed algoritmi randomizzati



# Randomness

---

- ▶ La generazione di bit casuali è fondamentale
- ▶ La chiave segreta che Alice e Bob condividono deve essere scelta a caso.
- ▶ Se usassero un qualsiasi algoritmo deterministico alla fine Adv ne verrebbe a capo

**Non c'è segretezza senza randomness!**



# Come generare randomness?

---

- ▶ In principio, per pochi bit random, lanciando una moneta!
- ▶ Tecniche moderne procedono in due fasi
  - ▶ una discreta quantità di dati ad “alta entropia” viene raccolta



- ▶ i dati vengono elaborati per produrre una sequenza di bit quasi indipendenti e distribuiti quasi uniformemente
- ▶ Per la prima fase, occorre una sorgente di dati imprevedibili



# Sorgenti

---

## ▶ Input esterni

- ▶ ritardo dei dati in transito in rete
- ▶ tempi di accesso all'hard disk
- ▶ misure sulla pressione dei tasti
- ▶ misure sul movimento del mouse
- ▶ ...



dati “lontani” dalla  
distribuzione uniforme

## ▶ Fenomeni fisici

- ▶ misure del rumore nei dispositivi elettronici
- ▶ misure del decadimento radioattivo



# Estrazione di bit casuali

---

- ▶ Il processo di “livellamento” dei dati ad alta entropia è non banale. Ne mostriamo uno.
  - ▶ Supponiamo di disporre di una sequenza dei risultati del lancio di una moneta difettosa, rappresentata in binario
  - ▶ La moneta dà:

T=1 con probabilità $p$ C=0 con probabilità $(1-p)$
--

- ▶ I lanci sono **indipendenti** l'uno dall'altro
- ▶ Consideriamo i bit a coppie
- ▶ Se vediamo:

00	01	10	11	
scriviamo	/	0	1	/



# Estrazione di bit casuali

---

10	01	11	01	10	00	11	10	10	01
<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>1</u>	<u>1</u>	<u>0</u>

- ▶ la sequenza binaria calcolata è distribuita uniformemente
- ▶ Perché?
  - ▶ La probabilità che una coppia produca 0 è:  $(1-p) p$
  - ▶ La probabilità che una coppia produca 1 è:  $p (1-p)$
- ▶ La generazione e l'uso di random bit è cruciale per la sicurezza dei protocolli crittografici
  - ▶ Generatori di numeri casuali devono essere progettati per uso crittografico.
  - ▶ “General-purpose” non sono idonei.



# Definizioni

---

- ▶ Schema di cifratura: (Gen, Enc, Dec),  $M$  tale che  $|M| > 1$

  
spazio dei messaggi

- ▶ Gen: algoritmo *probabilistico* di generazione delle chiavi, restituisce  $k \in K$  in accordo ad una distribuzione di probabilità

  
spazio delle chiavi

- ▶ Enc: algoritmo *probabilistico* di cifratura, prende in input  $m \in M, k \in K$  e restituisce un cifrato  $c \in C$

  
spazio dei cifrati

- ▶ Dec: algoritmo deterministico di decifratura, prende in input  $c \in C, k \in K$  e restituisce  $m \in M$





# Notazioni

---

▶  $k \leftarrow \text{Gen}()$

▶  $c \leftarrow \text{Enc}_k(m)$

output di alg. probabilistici

▶  $c := \text{Enc}_k(m)$

▶  $m := \text{Dec}_k(c)$

output di alg. deterministici

▶ Useremo la notazione  $x \leftarrow S$  anche per denotare l'estrazione di un elemento da un insieme  $S$  in accordo alla distribuzione uniforme



# Condizione di correttezza perfetta

- ▶ Per ogni  $k \in K$ , per ogni  $m \in M$ , e qualsiasi  $c \leftarrow \text{Enc}_k(m)$ , risulta

$$\text{Dec}_k(c) = m, \text{ con probabilità } 1$$

Nei teoremi e nelle definizioni che seguono faremo riferimento alle distribuzioni di probabilità sugli insiemi  $K$ ,  $M$  e  $C$ .

La distribuzione su  $K$  dipende da  $\text{Gen}()$

 assumeremo uniforme

La variabile casuale  $\mathbf{K}$  denoterà l'output di  $\text{Gen}()$



# Variabili casuali

---

- ▶ La variabile casuale **M** denoterà il messaggio “in chiaro”

La  $\Pr[\mathbf{M} = m]$  è la probabilità che  $m$  debba essere cifrato



Non dipende dallo schema di cifratura. Riflette la frequenza dei differenti messaggi che le parti si inviano, così come l'incertezza che l'avversario Adv ha su di essi.

e.g., Adv può sapere che i messaggi sono solo due e che:

$$\Pr[\mathbf{M} = \text{“andiamo a cena oggi”}] = 0.7$$

$$\Pr[\mathbf{M} = \text{“usciamo domani”}] = 0.3$$

- ▶ Le variabili casuali **K** ed **M** si assumono **indipendenti**
- 



# Variabili casuali

---

- ▶ Fissato uno schema di cifratura ed una distribuzione su  $M$  si determina una distribuzione sullo spazio dei cifrati  $C$ , ottenuta

- ▶ da  $k$  generata tramite  $\text{Gen}()$
- ▶ scegliendo  $m$  in accordo alla distribuzione su  $M$
- ▶ calcolando  $c \leftarrow \text{Enc}_k(m)$



- ▶ La variabile casuale  $C$  denoterà l'output del processo di cifratura

- ▶ Nota che  $C = \text{Enc}_K(M)$



# Esempio

---

## ► Consideriamo lo Shift Cipher

$$K = \{0, \dots, 25\}, \Pr[\mathbf{K}=k] = 1/26, \text{ per ogni } k \in K$$

Sia data su  $\mathbf{M}$  la distribuzione:  $\Pr[\mathbf{M} = a] = 0.7$  e  $\Pr[\mathbf{M} = z] = 0.3$

Qual è la probabilità che il cifrato sia B?

Ci sono solo due possibilità:  $m = a$  e  $k = 1$ , oppure  $m = z$  e  $k = 2$

Poiché le variabili casuali  $\mathbf{M}$  e  $\mathbf{K}$  sono indipendenti, risultano:

$$\Pr[\mathbf{M} = a \wedge \mathbf{K} = 1] = \Pr[\mathbf{M} = a] \cdot \Pr[\mathbf{K} = 1] = 0.7 \cdot 1/26$$

$$\Pr[\mathbf{M} = z \wedge \mathbf{K} = 2] = \Pr[\mathbf{M} = z] \cdot \Pr[\mathbf{K} = 2] = 0.3 \cdot 1/26$$

Pertanto,

$$\begin{aligned} \Pr[\mathbf{C} = B] &= \Pr[\mathbf{M} = a \wedge \mathbf{K} = 1] + \Pr[\mathbf{M} = z \wedge \mathbf{K} = 2] \\ &= 0.7 \cdot 1/26 + 0.3 \cdot 1/26 = 1/26 \end{aligned}$$



# Esempio

---

## ► Consideriamo lo Shift Cipher

Qual è invece la probabilità che il messaggio in chiaro sia “a”, dato il cifrato B?

Usando il teorema di Bayes, risulta:

$$\begin{aligned}\Pr[\mathbf{M} = a \mid \mathbf{C} = B] &= \frac{\Pr[\mathbf{C} = B \mid \mathbf{M} = a] \cdot \Pr[\mathbf{M} = a]}{\Pr[\mathbf{C} = B]} \\ &= \frac{\Pr[\mathbf{C} = B \mid \mathbf{M} = a] \cdot 0.7}{1/26}\end{aligned}$$

Ma  $\Pr[\mathbf{C} = B \mid \mathbf{M} = a] = 1/26$  perché, se  $\mathbf{M} = a$ , l'unico modo per ottenere  $\mathbf{C} = B$  è che  $\mathbf{K} = 1$  (che accade con prob.  $1/26$ )

$$\text{Pertanto, } \Pr[\mathbf{M} = a \mid \mathbf{C} = B] = \frac{1/26 \cdot 0.7}{1/26} = 0.7$$



# Ulteriore esempio

---

## ► Ancora lo Shift Cipher

- Sia data su  $\mathbf{M}$  la distribuzione:

$$\Pr[\mathbf{M} = \text{kim}] = 0.5, \quad \Pr[\mathbf{M} = \text{ann}] = 0.2 \text{ e } \Pr[\mathbf{M} = \text{boo}] = 0.3$$

Qual è la probabilità che  $\mathbf{C} = \text{DQQ}$ ?

Ci sono soltanto due possibilità:  $\mathbf{M} = \text{ann}$  e  $\mathbf{K} = 3$ , oppure  $\mathbf{M} = \text{boo}$  e  $\mathbf{K} = 2$

Pertanto,

$$\begin{aligned} \Pr[\mathbf{C} = \text{DQQ}] &= \Pr[\mathbf{M} = \text{ann} \wedge \mathbf{K} = 3] + \Pr[\mathbf{M} = \text{boo} \wedge \mathbf{K} = 2] \\ &= 0.2 \cdot 1/26 + 0.3 \cdot 1/26 = 0.5 \cdot 1/26 \\ &= 1/2 \cdot 1/26 \\ &= 1/52 \end{aligned}$$



# Ulteriore esempio

---

Similmente, usando il teorema di Bayes, risulta:

$$\begin{aligned}\Pr[\mathbf{M} = \text{ann} \mid \mathbf{C} = \text{DQQ}] &= \frac{\Pr[\mathbf{C} = \text{DQQ} \mid \mathbf{M} = \text{ann}] \cdot \Pr[\mathbf{M} = \text{ann}]}{\Pr[\mathbf{C} = \text{DQQ}]} \\ &= \frac{1/26 \cdot 0.2}{1/52} = 0.4\end{aligned}$$

essendo  $\Pr[\mathbf{C} = \text{DQQ} \mid \mathbf{M} = \text{ann}] = 1/26$ , dato che solo  $\mathbf{K} = 3$  produce  $\mathbf{C} = \text{DQQ}$ .





# Segretezza perfetta

---

- ▶ **Scenario: Adv conosce**
  - ▶ la distribuzione di probabilità su  $M$
  - ▶ lo schema di cifratura
  - ▶ **non** conosce la chiave  $k$
  - ▶ può ascoltare/vedere la comunicazione

Per ottenere segretezza perfetta, l'osservazione del cifrato non dovrebbe fornire alcuna informazione aggiuntiva ad Adv sul messaggio in chiaro. Cioè:

**Il cifrato non dovrebbe rivelare ad Adv  
nulla in più al di là di ciò che già sa**



# Segretezza perfetta

---

Definizione 2.3. Uno schema di cifratura (Gen, Enc, Dec) con spazio dei messaggi  $M$  è perfettamente segreto se

- ▶ per ogni distribuzione di probabilità su  $M$
- ▶ per ogni messaggio  $m \in M$
- ▶ e per ogni cifrato  $c \in C$  per cui risulta  $\Pr[C=c]>0$ , si ha:

$$\Pr[ \mathbf{M} = m \mid \mathbf{C} = c ] = \Pr[ \mathbf{M} = m ]$$



# Definizione equivalente

---

- ▶ Possiamo fornire una definizione equivalente richiedendo che la distribuzione di probabilità dei cifrati **non dipenda** dal messaggio in chiaro

- ▶ Formalmente, per ogni  $m, m' \in M$  e per ogni  $c \in C$

$$\Pr[\text{Enc}_{\mathbf{K}}(m) = c] = \Pr[\text{Enc}_{\mathbf{K}}(m') = c]$$

dove le prob sono calcolate sulle possibili scelte

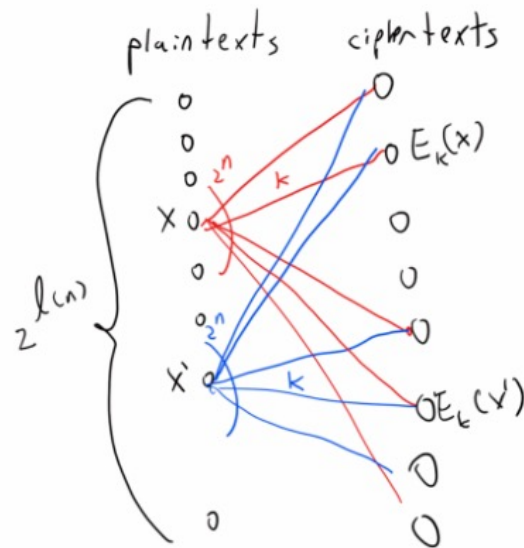
- ▶ della chiave  $k$
- ▶ dei bit casuali utilizzati da  $\text{Enc}_k()$



# Rappresentazione grafica

Se consideriamo messaggi e cifrati di lunghezza  $l(n)$ , con  $n$  lunghezza della chiave, possiamo rappresentare la condizione con un grafo bipartito

- aggiungiamo un arco, etichettato con chiave  $k$ , tra il nodo  $x$  e il nodo  $c$  se  $c = \text{Enc}_k(x)$



- $x$  ed  $x'$  hanno esattamente lo stesso insieme di nodi vicini

Immagine ripresa da: B. Barak,  
*Introduction to Theoretical Computer Science*  
Capitolo 21

# Definizione equivalente

---

- ▶ La precedente condizione implica
  - ▶ è impossibile distinguere una cifratura di  $m$  da una di  $m'$ , poiché le distribuzioni sui cifrati sono le stesse
  - ▶ un cifrato non rivela alcuna informazione sul messaggio in chiaro

**Lemma 2.5** Uno schema di cifratura (Gen, Enc, Dec) con spazio dei messaggi  $M$  è perfettamente segreto **se e solo se** per ogni  $m, m' \in M$  ed ogni  $c \in C$  risulta:

$$\Pr[\text{Enc}_K(m) = c] = \Pr[\text{Enc}_K(m') = c]$$




# Dimostrazione

---

- ▶ Proviamo che, se la condizione vale, **allora** lo schema è perfettamente segreto. Fissiamo una distribuzione su  $M$  e sia  $c$  tale che  $\Pr[C = c] > 0$ .
- ▶ se  $\Pr[M = m] = 0$ , allora banalmente

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \rightarrow 0$$

$= 0$

  $\Pr[M = m \mid C = c] = \Pr[M = m]$

- ▶ se  $\Pr[M = m] > 0$ , invece, notiamo che

$$\Pr[C = c \mid M = m] = \Pr[\text{Enc}_K(M) = c \mid M = m] = \Pr[\text{Enc}_K(m) = c]$$

Sia  $\delta_c = \Pr[\text{Enc}_K(m) = c]$ . Se la condizione del lemma vale, per ogni  $m$ '



# Dimostrazione

---

risulta:

$$\Pr[\text{Enc}_K(m') = c] = \Pr[\mathbf{C} = c \mid \mathbf{M} = m'] = \delta_c$$

Applicando il teorema di Bayes,

$$\Pr[\mathbf{M} = m \mid \mathbf{C} = c] = \frac{\Pr[\mathbf{C} = c \mid \mathbf{M} = m] \cdot \Pr[\mathbf{M} = m]}{\Pr[\mathbf{C} = c]}$$

$$= \frac{\Pr[\mathbf{C} = c \mid \mathbf{M} = m] \cdot \Pr[\mathbf{M} = m]}{\sum_{m' \in M} \Pr[\mathbf{C} = c \mid \mathbf{M} = m'] \cdot \Pr[\mathbf{M} = m']}$$

$$= \frac{\delta_c \cdot \Pr[\mathbf{M} = m]}{\delta_c \cdot \sum_{m' \in M} \Pr[\mathbf{M} = m']}$$

$$= \Pr[\mathbf{M} = m]$$

Pertanto lo  
schema è  
perfettamente  
segreto

1



# Dimostrazione

---

- ▶ Viceversa, sia lo schema perfettamente segreto. Sia  $M$  **uniformemente distribuita**. Per il teorema di Bayes, per ogni  $c$  tale che  $\Pr[C = c] > 0$  e per ogni  $m$ , possiamo scrivere

$$\Pr[M = m \mid C = c] \cdot \Pr[C = c] = \Pr[C = c \mid M = m] \cdot \Pr[M = m]$$

- ▶ La segretezza perfetta  $\Pr[M = m \mid C = c] = \Pr[M = m]$  implica

$$\cancel{\Pr[M = m]} \cdot \Pr[C = c] = \Pr[C = c \mid M = m] \cdot \cancel{\Pr[M = m]}$$

ovvero

$$\Pr[C = c] = \Pr[C = c \mid M = m]$$

- ▶ Pertanto, per ogni  $m, m'$  e per ogni  $c$  tale che  $\Pr[C = c] > 0$

$$\Pr[\text{Enc}_K(m) = c] = \Pr[C = c] = \Pr[\text{Enc}_K(m') = c].$$





# Perfetta indistinguibilità

---

- ▶ Possiamo dare ancora un'altra definizione di segretezza perfetta equivalente alle precedenti
  - ▶ basata su un esperimento che coinvolge Adv e un Challenger C
- ▶ Informalmente
  - ▶ Adv sceglie due messaggi in chiaro,  $m$  ed  $m'$
  - ▶ C sceglie uniformemente a caso uno dei due e lo cifra usando una chiave  $k$  casuale
  - ▶ Il cifrato ottenuto  $c$  viene dato ad Adv
  - ▶ Adv dà in output una sua ipotesi su quale dei due è stato cifrato
  - ▶ Adv ha successo se la sua ipotesi è corretta



# Perfetta indistinguibilità

---

- ▶ Uno schema di cifratura è perfettamente indistinguibile se nessun Adv può avere successo con probabilità  $> \frac{1}{2}$
- ▶ Osservazioni:
  - ▶ un Adv che ipotizza a caso ha successo con probabilità  $\frac{1}{2}$  ,  
richiediamo che Adv non disponga di una strategia migliore
  - ▶ non poniamo alcun limite al potere computazionale di Adv



# Esperimento $\text{PrivK}_{A,\Pi}^{eav}$

---

Sia  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  uno schema di cifratura con spazio dei messaggi  $\mathcal{M}$ .  
Sia  $A$  un Adv (i.e., un algoritmo che mantiene uno stato)

$\text{PrivK}_{A,\Pi}^{eav}$

- $A$  dà in output una coppia di messaggi  $m_0, m_1$
- $C$  genera  $k$  tramite  $\text{Gen}()$  e sceglie uniformemente a caso il bit  $b$  in  $\{0,1\}$
- $C$  calcola  $c \leftarrow \text{Enc}_K(m_b)$ , detto **cifrato di sfida**, e lo passa ad  $A$
- $A$  dà in output un bit  $b'$
- L'output dell'esperimento è 1 se  $b' = b$ , 0 altrimenti. Se l'output è 1,  $A$  ha successo.



# Definizione

---

Definizione 2.6. Uno schema di cifratura (Gen, Enc, Dec) con spazio dei messaggi  $M$  è perfettamente indistinguibile se, per ogni  $A$ , risulta:

$$\Pr[ \text{PrivK}_{A,\Pi}^{eav} = 1 ] = 1/2$$



Risultato dell'esperimento

È possibile dimostrare che vale il seguente

Lemma 2.7. Uno schema di cifratura  $\Pi$  è perfettamente segreto **se e solo se** è perfettamente indistinguibile.



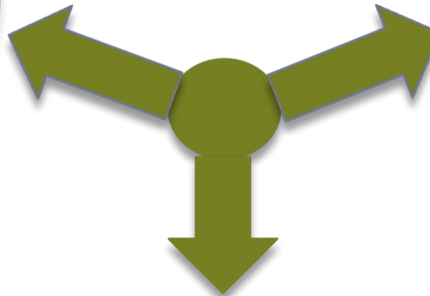
# Conclusione

---

- Disponiamo di tre definizioni di segretezza perfetta equivalenti!

per ogni distribuzione su  $M$ ,  
per ogni  $m \in M$  e per ogni  $c$   
tale che  $\Pr[C = c] > 0$   
 $\Pr[M = m \mid C = c] = \Pr[M = m]$

per ogni  $m, m' \in M$  ed ogni  $c \in C$   
 $\Pr[\text{Enc}_K(m) = c] = \Pr[\text{Enc}_K(m') = c]$



Per ogni Adv  $A$ ,

$$\Pr[\text{PrivK}_{A, \Pi}^{eav} = 1] = 1/2$$