Teoria dell'Informazione/RTI **Anno Accademico 2022–2023**

Lezione 13

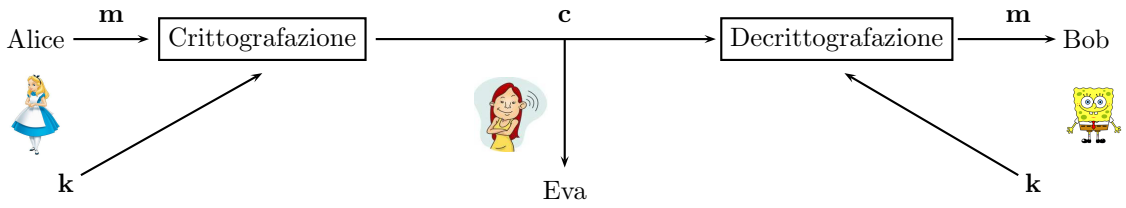
Ugo Vaccaro

In questa lezione vedremo alcune applicazioni della Teoria dell'Informazione alla Crittografia. Uno degli obiettivi principali della Crittografia è di dare la possibilità a due persone (comunemente designate con il nome di Alice e Bob) di scambiarsi informazioni su di un mezzo di comunicazione "non sicuro" (ovvero su di un mezzo in cui chiunque possa ascoltare ciò che viene trasmesso, anche malintenzionati...) in modo tale che *ogni* terza persona "curiosa" (o peggio...), comunemente designata con il nome di Eva, *non* possa comprendere ciò che Alice e Bob si dicono.

L'informazione che Alice intende mandare a Bob, chiamata generalmente "testo in chiaro", può essere un testo in italiano, dati numerici, o qualunque altra cosa. Poichè sappiamo che tutto si può codificare con sequenze di bits, assumeremo senza perdita di generalità alcuna che l'informazione che Alice intende trasmettere a Bob sia una qualche sequenza binaria $\mathbf{m} \in \{0,1\}^*$. Alice crittograferà il testo in chiaro $\mathbf{m}$ usando una "chiave segreta" (anch'essa rappresentabile mediante una qualche sequenza binaria $\mathbf{k} \in \{0,1\}^*$) nota *solo* ad Alice ed a Bob, ed utilizzando una qualche funzione f nota *a tutti* (ovvero anche ad eventuali malintenzionati). Spedirà, quindi, il corrispondente "testo cifrato" $\mathbf{c} = f(\mathbf{m}, \mathbf{k}) \in \{0,1\}^*$ sul canale di comunicazione non sicuro. Ciò che richiederemo è che il tutto abbia le seguenti proprietà fondamentali:

1. Bob, usando la chiave $\mathbf{k}$, può risalire al testo in chiaro $\mathbf{m}$ dopo aver ricevuto il testo cifrato $\mathbf{c}$;
2. Eva *nulla* può dedurre sul testo in chiaro $\mathbf{m}$ dalla conoscenza del testo cifrato $\mathbf{c}$.

Un sistema crittografico siffatto viene generalmente rappresentato dal seguente schema:



Vediamo come esprimere matematicamente le proprietà 1. e 2. prima esposte. Assumiamo che ciascun messaggio $\mathbf{m}$ venga scelto da Alice in accordo ad una distribuzione di probabilità $P_m = \{P_m(\mathbf{m}) : \mathbf{m} \in \{0,1\}^*\}$, così come $P_k = \{P_k(\mathbf{k}) : \mathbf{k} \in \{0,1\}^*\}$ denota la distribuzione di probabilità con cui Alice e Bob insieme scelgono la chiave $\mathbf{k}$. Le due distribuzioni di probabilità P_m, P_k e la funzione f che permette di calcolare il testo cifrato $\mathbf{c} = f(\mathbf{m}, \mathbf{k}) \in \{0,1\}^*$ naturalmente inducono una distribuzione di probabilità $P_c = \{P_c(\mathbf{c}) : \mathbf{c} \in \{0,1\}^*\}$ sui possibili testi cifrati, data da

$$\forall \mathbf{c} \in \{0,1\}^* \qquad P_c(\mathbf{c}) = \sum_{\mathbf{m},\mathbf{k}: f(\mathbf{m},\mathbf{k})=\mathbf{c}} P_m(\mathbf{m}) P_k(\mathbf{k}).$$

Si assume che le distribuzioni di probabilità P_m, P_k, P_c e la funzione di crittografazione f siano note a tutti, anche alla malintenzionata Eva. Denotiamo con $\mathbf{M}$ la v.c. che assume come valori i messaggi $\mathbf{m} \in \{0,1\}^*$ in chiaro, in accordo alla distribuzione di probabilità P_m, con $\mathbf{K}$ la v.c. che assume come valori le chiavi $\mathbf{k} \in \{0,1\}^*$ in accordo alla distribuzione di probabilità P_k, e con $\mathbf{C}$ la v.c. che assume come valori i testi cifrati $\mathbf{c} \in \{0,1\}^*$ in accordo alla distribuzione di probabilità $P_{\mathbf{c}}$.

Le proprietà 1. e 2. prima descritte sono equivalenti a dire che

a) $\forall \mathbf{m}, \mathbf{m}' \in \{0,1\}^* \quad \forall \mathbf{k} \in \{0,1\}^* \quad$ vale che $\Pr\{\mathbf{M} = \mathbf{m}' | \mathbf{K} = \mathbf{k},\ \mathbf{C} = \mathbf{c} = f(\mathbf{m}, \mathbf{k})\} = \begin{cases} 1 & \text{se } \mathbf{m}' = \mathbf{m}; \\ 0 & \text{se } \mathbf{m}' \neq \mathbf{m}. \end{cases}$

b) $\forall \mathbf{m} \in \{0,1\}^* \quad \forall \mathbf{k} \in \{0,1\}^* \quad$ vale che $\Pr\{\mathbf{M} = \mathbf{m} | \mathbf{C} = \mathbf{c} = f(\mathbf{m}, \mathbf{k})\} = \Pr\{\mathbf{M} = \mathbf{m}\}$.

Il senso intuitivo delle proprietà a) e b) è ovvio. La a) essenzialmente afferma che noti la chiave $\mathbf{k}$ e il testo cifrato $\mathbf{c}$ computato a partire dal messaggio in chiaro $\mathbf{m}$ e dalla chiave $\mathbf{k}$, esiste un unico messaggio in chiaro compatibile con $\mathbf{k}$ e $\mathbf{c}$, ed esso è proprio $\mathbf{m}$. Per cui, una volta noti $\mathbf{k}$ e $\mathbf{c}$, Bob può con certezza risalire al messaggio in chiaro originale $\mathbf{m}$. Altrettanto ovvia è la proprietà b). Essa afferma che, noto solo il testo cifrato $\mathbf{c}$, la probabilità che il testo in chiaro sia un generico $\mathbf{m} \in \{0,1\}^*$ è esattamente pari alla probabilità *a priori* che il testo in chiaro sia $\mathbf{m} \in \{0,1\}^*$, ovvero la conoscenza di $\mathbf{c}$ *nulla* aggiunge a ciò che Eva già conosce e quindi nulla permette ad Eva di inferire su quale possa essere il possibile testo in chiaro originario.

In altri termini, le due proprietà di sopra affermano che

- i valori della v.c. $\mathbf{M}$ sono *univocamente determinati* una volta si conoscano i valori delle v.c. $\mathbf{K}$ e $\mathbf{C}$;
- la v.c. $\mathbf{M}$ è statisticamente indipendente dalla sola variabile casuale $\mathbf{C}$.

Ricordiamo la definizione di entropia condizionata $H(X|Y)$ di una generica v.c. X data un'altra v.c. Y, con distribuzione congiunta $P(x,y)$:

$$H(X|Y) = \sum_{x,y} P(xy) \log \frac{1}{P(x|y)} \tag{1}$$

Così come la entropia $H(X)$ di una v.c. X rappresenta la incertezza (media) che si ha su quali valori la v.c. X assumerà, la entropia condizionata $H(X|Y)$ rappresenta la incertezza (media) che si ha su quali valori la v.c. X assumerà *dato* che si conoscono i valori assunti dalla v.c. Y. Una ben nota relazione tra $H(X)$ e $H(X|Y)$ è la seguente

$$H(X|Y) \leq H(X), \tag{2}$$

con eguaglianza $H(X|Y) = H(X)$ *se e solo se* X è statisticamente indipendente da Y, ovvero se e solo se $\forall x, y\ P(x|y) = P(x)$. La (2) è perfettamente intuitiva. Infatti, la conoscenza dei valori assunti da Y tutt'al più non ci dice nulla sui valori che può assumere X (nel caso in cui X è statisticamente indipendente da Y), ma in generale la conoscenza dei valori assunti da Y ci fà diminuire (in media) la nostra incertezza su X.

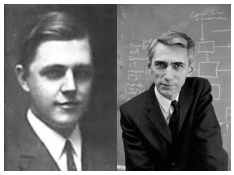
Inoltre, $H(X|Y) = 0$ *se e solo se* la v.c. X è determinata da Y, ovvero se e solo se $\forall y\ \exists!\ x$ tale che $P(x|y) = 1$ (in altri termini, $H(X|Y) = 0$ se e solo se esiste una funzione g per cui $X = g(Y)$).

Sulla base delle proprietà della entropia condizionata appena ricordate, le proprietà a) e b) sono equivalenti alle seguenti condizioni sulle variabili casuali $\mathbf{M}$, $\mathbf{C}$, e $\mathbf{K}$:

i) $H(\mathbf{M}|\mathbf{CK}) = 0$.

ii) $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$.

Le due condizioni i) e ii) vanno sotto il nome di *sicurezza perfetta* per un sistema crittografico. Di nuovo, il loro senso è intuitivo. La i) afferma che dati il messaggio cifrato e la chiave, l' incertezza che abbiamo sul messaggio originario è nulla, ovvero lo si può ricostruire con certezza. La ii) afferma che dato il solo messaggio cifrato (che è la sola cosa che Eva conosce), la incertezza che si ha sul messaggio originario in chiaro è esattamente uguale a quella di partenza, quindi il messaggio cifrato da solo *nulla* dice sul messaggio in chiaro.



Vernam Shannon

Vediamo come costruire un sistema crittografico che assicura sicurezza perfetta, ovvero che soddisfa sia i) che ii). Il sistema venne inventato da G.F. Vernam nel 1919 e la prova che esso garantisce sicurezza perfetta fu ideata da C.E. Shannon. Dato il messaggio in chiaro $\mathbf{m} = m_1 \dots m_N \in \{0,1\}^N$, composto da N bits, la chiave $\mathbf{k} = k_1 \dots k_N$ (anch'essa di N bits) viene scelta nell'insieme $\{0,1\}^N$, indipendentemente da $\mathbf{m}$ ed equiprobabilmente (cioè con probabilità pari a $1/2^N$). Il messaggio crittografato che verrà spedito sul canale non sicuro sarà calcolato da $\mathbf{m}$ e $\mathbf{k}$ nel modo seguente:

$$\mathbf{c} = c_1 \dots c_N = f(\mathbf{m}, \mathbf{k}) = (m_1 \oplus k_1) \dots (m_N \oplus k_N) = \mathbf{m} \oplus \mathbf{k} \tag{3}$$

dove $\oplus$ denota l'addizione modulo 2 in $\mathbb{Z}_2 = \{0,1\}$.

Una volta che siano noti il testo cifrato $\mathbf{c}$ e la chiave $\mathbf{k}$, Bob può risalire univocamente al messaggio in chiaro $\mathbf{m}$, semplicemente calcolando $\mathbf{c} \oplus \mathbf{k}$. Infatti, dalla (3)

$$(\mathbf{c} \oplus \mathbf{k}) = (m_1 \oplus k_1) \oplus k_1 \dots (m_N \oplus k_N) \oplus k_n = m_1 \dots m_N = \mathbf{m},$$

in quanto $k_i \oplus k_i = 0$, $\forall i$. Quindi la condizione i) è soddisfatta. Per provare la ii), ovvero che $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$ (il che corrisponde al fatto che la conoscenza del solo testo cifrato *nulla* dice sul messaggio in chiaro), osserviamo innazitutto che dalla conoscenza di $\mathbf{m}$ e $\mathbf{c}$ possiamo risalire alla chiave $\mathbf{k}$. Infatti

$$(\mathbf{m} \oplus \mathbf{c}) = m_1 \oplus (m_1 \oplus k_1) \dots m_N \oplus (m_N \oplus k_n) = k_1 \dots k_N = \mathbf{k},$$

da cui ne segue che

$$H(\mathbf{K}|\mathbf{MC}) = 0. \tag{4}$$

Inoltre, poichè la chiave $\mathbf{k}$ è scelta in $\{0,1\}^N$, indipendentemente da $\mathbf{m}$ e con probabilità $1/2^N$ ciascuna , vale che

$$H(\mathbf{K}|\mathbf{M}) = H(\mathbf{K}) = \log 2^N = N. \tag{5}$$

Ricordiamo la definizione di mutua informazione $I(X;Y)$ tra due variabili casuali e la mutua informazione condizionata, ed alcune delle loro proprietà.

$$I(X;Y) = \sum_{x,y} P(xy) \log \frac{P(x|y)}{P(x)} = \sum_{x,y} P(xy) \log \frac{1}{P(x)} - \sum_{x,y} P(xy) \log \frac{1}{P(x|y)} = H(X) - H(X|Y) \tag{6}$$

$$I(X;Y) = \sum_{x,y} P(xy) \log \frac{P(x|y)}{P(x)} = \sum_{x,y} P(xy) \log \frac{P(xy)}{P(y)P(x)} \tag{7}$$

$$= \sum_{x,y} P(xy) \log \frac{P(y|x)}{P(y)} = H(Y) - H(Y|X) = I(Y;X) \tag{8}$$

$$I(X;Y|Z) = \sum_{x,y,z} P(xyz) \log \frac{P(x|yz)}{P(x|z)} = H(X|Z) - H(X|ZY) \tag{9}$$

$$I(X;YZ) = I(X;Y) + I(X;Z|Y) = H(X) - H(X|YZ) \tag{10}$$

Osserviamo che $I(X;Y) \geq 0$, con uguaglianza se e solo se X e Y sono statisticamente indipendenti.

Passiamo ora alla prova che $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$. Osserviamo innanzitutto che

$$\begin{aligned} I(\mathbf{K};\mathbf{C}|\mathbf{M}) &= H(\mathbf{K}|\mathbf{M}) - H(\mathbf{K}|\mathbf{CM}) && \text{(dalla (9))} \\ &= H(\mathbf{K}|\mathbf{M}) && \text{(dalla (4))} \\ &= H(\mathbf{K}) && \text{(in quanto } \mathbf{K} \text{ è indipendente da } \mathbf{M}) \\ &= N && \text{(poichè } \mathbf{K} \text{ è uniformemente distribuita in } \{0,1\}^N) \end{aligned} \tag{11}$$

Vale inoltre

$$\begin{aligned} I(\mathbf{C};\mathbf{MK}) &= I(\mathbf{C};\mathbf{M}) + I(\mathbf{C};\mathbf{K}|\mathbf{M}) && \text{(dalla (10))} \\ &= I(\mathbf{C};\mathbf{M}) + I(\mathbf{K};\mathbf{C}|\mathbf{M}) \\ &= I(\mathbf{C};\mathbf{M}) + N && \text{(dalla (11))} \end{aligned}$$

D'altra parte

$$\begin{aligned} N + I(\mathbf{C};\mathbf{M}) &= I(\mathbf{C};\mathbf{MK}) \\ &= H(\mathbf{C}) - H(\mathbf{C}|\mathbf{MK}) && \text{(dalla (10))} \\ &\leq H(\mathbf{C}) \leq \log 2^N = N, \end{aligned}$$

ovvero $I(\mathbf{C};\mathbf{M}) = 0$, il che, dalla (6) equivale a dire che

$$H(\mathbf{M}) = H(\mathbf{M}|\mathbf{C}),$$

che è quanto volevamo provare.

Abbiamo quindi visto che è possibile costruire un sistema crittografico che assicura sicurezza perfetta, il che è molto interessante. Purtroppo il sistema crittografico descritto soffre di una severa limitazione che lo rende poco utilizzabile in pratica. La limitazione consiste nel fatto che per crittografare un messaggio lungo N bits abbiamo usato una chiave di pari lunghezza N. Il che non è sempre possibile nelle situazioni pratiche dove il messaggio da spedire può anche essere molto lungo (si immagini una conversazione...). Purtroppo, questa limitazione non è una caratteristica solo del sistema crittografico prima descritto, infatti è possibile provare che ne soffrono *tutti* i sistemi crittografici che assicurano sicurezza perfetta.

Teorema 1 *In ogni sistema crittografico che soddisfa i) e ii) vale che*

$$H(\mathbf{K}) \geq H(\mathbf{M}). \tag{12}$$

Dimostrazione. Dalla i) sappiamo che $H(\mathbf{M}|\mathbf{CK}) = 0$ e dalla ii) sappiamo che $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$. Pertanto

$$\begin{aligned} H(\mathbf{MK}|\mathbf{C}) &= H(\mathbf{M}|\mathbf{C}) + H(\mathbf{K}|\mathbf{MC}) \\ &= H(\mathbf{M}) + H(\mathbf{K}|\mathbf{MC}) \\ &= H(\mathbf{K}|\mathbf{C}) + H(\mathbf{M}|\mathbf{KC}) && \text{(espandendo differentemente l'entropia } H(\mathbf{MK}|\mathbf{C})) \\ &= H(\mathbf{K}|\mathbf{C}) \end{aligned}$$

Da ciò otteniamo

$$H(\mathbf{K}) \geq H(\mathbf{K}|\mathbf{C}) = H(\mathbf{M}) + H(\mathbf{K}|\mathbf{MC}) \geq H(\mathbf{M}).$$

□

Visto che la (12) deve valere per ogni distribuzione di probabilità sui messaggi (e quindi anche nel caso essi siano distribuiti uniformemente in $\{0,1\}^N$, nel qual caso $H(\mathbf{M}) = N$) l'unica possibilità è che $H(\mathbf{K}) \geq N$. D'altra parte $H(\mathbf{K}) \leq \log(\#\text{possibili chiavi})$ per cui segue che $(\#\text{possibili chiavi}) \geq 2^{H(\mathbf{K})} \geq 2^N$ e quindi occorreranno almeno N bits per rappresentare ogni chiave. Ricapitolando, abbiamo provato che in *ogni* sistema crittografico che assicura sicurezza perfetta, per poter crittografare messaggi $\mathbf{m}$ lunghi N bits occorrono chiavi $\mathbf{k}$ di lunghezza (almeno) pari a N.

Vediamo qualche altra conseguenza delle proprietà dei sistemi crittografici che assicurano sicurezza perfetta.

Teorema 2 *In ogni sistema crittografico che soddisfa i) e ii) vale che*

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{M}) - H(\mathbf{C}). \tag{13}$$

Dimostrazione. Consideriamo la quantità $H(\mathbf{KMC})$ ed usiamo sia l'osservazione che il testo cifrato è univocamente determinato dal testo in chiaro e dalla chiave, ovvero che $H(\mathbf{C}|\mathbf{KM}) = 0$, che il fatto che la chiave ed il testo in chiaro sono scelti indipendentemente uno dall'altro, ovvero che $H(\mathbf{KM}) = H(\mathbf{K}) + H(\mathbf{M})$. Abbiamo allora

$$H(\mathbf{KMC}) = H(\mathbf{KM}) + H(\mathbf{C}|\mathbf{KM}) = H(\mathbf{KM}) = H(\mathbf{K}) + H(\mathbf{M}). \tag{14}$$

D'altra parte, il fatto che il testo in chiaro è univocamente determinato dal testo cifrato e dalla chiave ci dice che $H(\mathbf{M}|\mathbf{KC}) = 0$, da cui

$$H(\mathbf{KMC}) = H(\mathbf{KC}) + H(\mathbf{M}|\mathbf{KC}) = H(\mathbf{KC}). \tag{15}$$

Mettendo tutto insieme otteniamo che

$$\begin{aligned} H(\mathbf{K}|\mathbf{C}) &= H(\mathbf{KC}) - H(\mathbf{C}) && (\text{poichè } H(\mathbf{KC}) = H(\mathbf{C}) + H(\mathbf{K}|\mathbf{C})) \\ &= H(\mathbf{KMC}) - H(\mathbf{C}) && (\text{dalla (15)}) \\ &= H(\mathbf{K}) + H(\mathbf{M}) - H(\mathbf{C}) && (\text{dalla (14)}). \end{aligned}$$

□

La (13) ci quantifica, quindi, l'incertezza che l'avversario ha sulla possibile chiave segreta, una volta che abbia intercettato il testo cifrato.

Supponiamo ora di avere un sistema crittografico in cui valga solo la proprietà che $H(\mathbf{M}|\mathbf{CK}) = 0$, ovvero che è possibile risalire al messaggio in chiaro dalla conoscenza del testo cifrato e della chiave. Possiamo provare che l'informazione $I(\mathbf{C};\mathbf{M})$ che il testo cifrato dà sul testo in chiaro è pari almeno a $H(\mathbf{M}) - H(\mathbf{K})$, per cui se si usasse una chiave con entropia inferiore a $H(\mathbf{M})$, a partire dal testo cifrato avremmo sicuramente un'informazione non nulla sul testo in chiaro. Abbiamo che

$$I(\mathbf{K};\mathbf{M}|\mathbf{C}) = H(\mathbf{K}|\mathbf{C}) - H(\mathbf{K}|\mathbf{MC}) = H(\mathbf{M}|\mathbf{C}) - H(\mathbf{M}|\mathbf{KC}) = H(\mathbf{M}|\mathbf{C})$$

da cui otteniamo che

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{M}|\mathbf{C}) + H(\mathbf{K}|\mathbf{MC}) \geq H(\mathbf{M}|\mathbf{C}),$$

e quindi $H(\mathbf{K}) \geq H(\mathbf{K}|\mathbf{C}) \geq H(\mathbf{M}|\mathbf{C})$. D'altra parte

$$I(\mathbf{C};\mathbf{M}) = I(\mathbf{M};\mathbf{C}) = H(\mathbf{M}) - H(\mathbf{M}|\mathbf{C}) \geq H(\mathbf{M}) - H(\mathbf{K})$$

il che è esattamente ciò che intendevamo provare.

In virtù della (12), sistemi crittografici che rispettano entrambe le condizioni i) e ii) sono poco pratici, per cui è ragionevole studiare sistemi in cui la condizione di sicurezza ii) è indebolita, ovvero si richiede soltanto che l'incertezza sul messaggio in chiaro, dato il solo messaggio cifrato, sia "abbastanza" grande, ovvero sia almeno pari a $H(\mathbf{M}) - \epsilon$, per qualche opportuno $\epsilon > 0$. Non è difficile vedere che, anche in questo caso, si possono ottenere limitazioni inferiori all'entropia della chiave, ovviamente più deboli di quelli espressi dalla (12).