UNIVERSITA' DEGLI STUDI DI MILANO

Corso di Perfezionamento in

"Tecniche e didattica laboratoriali"

Crittografia e Grafi

Docente: Prof. Ottavio Rizzo

Anno Accademico 2008-2009

Autore:

Eugenio Tufino

Indice

Introduzione

La crittografia è un ottimo argomento per stimolare e arricchire l'istruzione matematica degli studenti. Gli studenti sono attratti dal mistero e dall' intrigo, e la crittografia può essere ben presentata in tal modo. Nella storia vi sono molteplici esempi in cui si sono utilizzate tecniche di crittografia. Altro aspetto importante è che gli studenti imparano a risolvere i problemi applicando i concetti matematici in modo autonomo e per tentativi.
La Crittografia è poi argomento di grande attualità, indispensabile nel difficile problema del trattamento dei dati riservati (per esempio, il bancomat o nel commercio elettronico sul web).
Dal punto di vista matematico, l'argomento ha il pregio di non richiedere pesanti prerequisiti e, d'altra parte, di introdurre rapidamente a problemi di ricerca tuttora aperti, come quelli collegati ai numeri primi.

In questa guida forniremo delle indicazioni per l'utilizzo dei grafi come esempio di crittografia a chiave pubblica. (Tale metodo viene chiamato Codice perfetto a chiave pubblica).

Il materiale che qui riassumiamo è stato presentato dal prof. O. Rizzo dell'Università di Milano in alcuni laboratori di matematica condotti nelle Scuole Superiori di Milano.
Una volta che i grafi sono stati forniti agli studenti, la strategia di soluzione è semplice in quanto consiste di addizioni (modulo n). La decrittazione del messaggio inoltre fornisce quella dimensione ludica che rende il laboratorio accattivante per gli studenti.

In appendice presentiamo alcuni grafi costruiti a partire da un sottoinsieme di punti chiamato "codice perfetto". Il "codice perfetto" è l'equivalente della chiave privata in un sistema di crittografia a chiave pubblica. Gli esempi proposti possono essere svolti da studenti delle Scuole Medie e classi Prime e Seconde delle Scuole Superiori. Nel laboratorio proposto agli studenti prima dell'introduzione dei grafi si sono svolte alcune applicazioni di crittografia a chiave privata. Elenchiamo in appendice lo schema seguito nel laboratorio.
Speriamo che questa guida possa aiutare gli insegnanti a presentare il laboratorio di crittografia nelle loro classi.

Problemi facili e difficili in matematica: Una breve digressione

La crittografia a chiave pubblica è collegata ad uno dei problemi irrisolti della matematica contemporanea: il problema ' P vs NP'.

Il modo più semplice per presentare tale problema è il seguente: "Esiste una domanda alla quale, in generale, una risposta esista ma sia estremamente difficile da calcolare mentre sia invece sempre facile verificare se la soluzione proposta è o meno corretta?"

Come esempio si può proporre il problema della colorazione delle mappe.

Si mostra una mappa particolare e si verifica con gli studenti che sono sufficienti due colori per colorare ogni regione in modo che una due qualsiasi regioni adiacenti non abbiano lo stesso colore. Successivamente si mostra una mappa come la seguente per cui sono necessari tre colori:

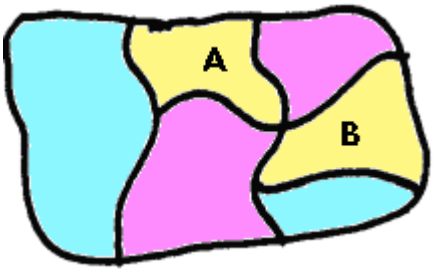


Figura 1 Mappa con tre colori

Sono sufficienti tre colori per colorare una qualsiasi mappa? La risposta è negativa, l'esempio classico di mappa per cui sono necessari quattro colori è il seguente:

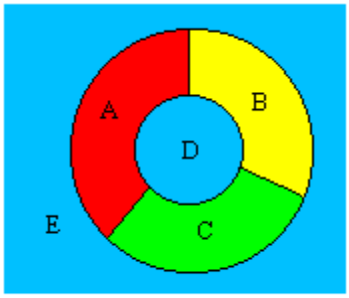


Figura 2 Mappa con quattro colori

A conclusione si cita il teorema dei quattro colori[1], importante teorema dimostrato nel 1976, per la cui dimostrazione si utilizzò pesantemente un calcolatore.

[1] Il teorema dei quattro colori afferma che data una superficie piana divisa in regioni connesse, come ad esempio una carta geografica politica, sono sufficienti quattro colori per colorare ogni regione facendo in modo che regioni adiacenti non abbiano lo stesso colore. Due regioni sono dette adiacenti se hanno almeno un segmento di confine in comune.

Crittografia a chiave pubblica

Per secoli uno degli assiomi fondamentali della crittografia è stato l'assoluta segretezza del metodo di codifica impiegato.

Infatti, i metodi utilizzati nella crittografia a chiave privata, gli unici in uso sino a tempi molto recenti, si possono descrivere come l'analogo del proteggere un messaggio chiudendolo in una scatola munita di una serratura; il mittente e il destinatario (e nessun altro) sono in possesso di una chiave che permette di chiudere (cifrare) e aprire (decifrare) la scatola.

Uno dei punti deboli di questo tipo di crittografia è che in una certa fase iniziale, mittente e destinatario devono scambiarsi la chiave (segreta) di cifratura, cosa che non è sempre possibile fare in modo del tutto sicuro.

Altro punto debole di un tale metodo è il grande numero di chiavi segrete necessarie nel caso di un sistema con molti utenti. Se n utenti devono comunicare con un sito centrale, come avviene in molte applicazioni commerciali, sono necessarie n chiavi. Se poi ciascun utente deve comunicare in modo riservato con ciascun altro utente, il numero di chiavi da generare cresce sempre più. Per un sistema con n utenti sono necessarie n(n-1)/2 chiavi. (Ad esempio per 1000 utenti sono necessarie 500000 chiavi).

Un esempio familiare è l'acquisto di un prodotto via internet attraverso la carta di credito. Tale acquisto avviene digitando ad un certo punto il numero della carta. Il collegamento tra il nostro computer (B) ed il server della compagnia da cui stiamo acquistando il prodotto (A) non è diretto ma passa attraverso altri soggetti intermedi (C) che potrebbero intercettare il numero. Occorre quindi crittare il numero della carta di credito ma in questo caso A e B non hanno potuto concordare una chiave da utilizzare.

La crittografia pubblica nacque con l'articolo di Diffie e Hellman nel 1976 [Diffie]. In tale articolo essi proponevano un sistema crittografico in cui era indispensabile rendere pubblica una parte dell'informazione. Riprendendo l'analogia precedente, la crittografia a chiave pubblica funziona come un lucchetto a scatto: chiunque lo può chiudere, ma solo il proprietario, in possesso della chiave, lo può aprire. Il metodo si può schematizzare nel seguente modo: ciascun utente sceglie una funzione crittografica che dipende da alcuni parametri, ma rende noti solo quelli che permettono di codificare i messaggi a lui diretti, mantenendo segreti quelli necessari alla decodifica. In questo modo, chiunque può spedire un messaggio all'utente in questione senza che questo, se intercettato da terzi, possa essere compreso.

Nella crittografia a chiave pubblica sono presenti due chiavi, una per cifrare i messaggi e una per decifrare. La chiave per cifrare è nota a tutti, mentre l'altra è segreta.

L'implementazione di tale metodo nella realtà poi si rivela non così semplice.

La prima implementazione, tuttora usata, è il sistema RSA (dai nomi, Rivest, Shamir e Adleman, che lo proposero nel 1977, [RSA]). Tale metodo si basa sul fatto che non sono noti efficienti metodi per calcolare i fattori primi di un numero molto grande, mentre, assegnati due numeri primi a e b, non presenta alcuna difficoltà il calcolo del prodotto n = ab. La chiave segreta è quindi costituita da questi due grandi numeri primi scelti dall'utente. La chiave segreta è il prodotto di questi numeri. (In realtà l'implementazione è più complicata ma qui stiamo semplificando). Visto che non esistono metodi efficienti di scomposizione, non si riesce ad ottenere la chiave segreta dalla chiave pubblica. Attualmente per i sistemi per i quali è richiesta un'alta sicurezza si utilizzano numeri primi di 90 cifra che moltiplicati danno origine a numeri di 200 cifre.

Un testo di riferimento per la parte matematica della crittografia, che qui non affronteremo, è il classico libro di Koblitz, che è anche uno dei promotori dell'utilizzo della crittografia nelle Scuole Superiori.[Koblitz-1], [Koblitz-2]

Per approfondire le informazioni storiche suggeriamo la lettura del libro di Simon Singh, [Singh]. Si tratta di un testo divulgativo sulla storia della crittografia, scritto in modo accessibile e avvincente.

Introduzione ai grafi e Codice perfetto

I grafi da un punto di vista matematico sono definiti nel seguente modo:

Un grafo è un insieme di punti, chiamati vertici, e di linee che li connettono chiamati archi. L'intorno di un vertice consiste del vertice stesso e di tutti i vertici che sono connessi ad esso attraverso un arco.

Per introdurre i grafi agli studenti si è scelto di utilizzare come esempio intuitivo una mappa schematizzata di una città, dove i vertici sono dati dagli incroci delle strade.

Ciò consente di introdurre quello che chiameremo "Il Problema dei Gelatai", che consiste nel posizionare un gelataio negli incroci in modo che:

1. In ogni incrocio ci sia un gelataio oppure ce ne sia uno posto ad un isolato di distanza
2. Per ogni incrocio in cui non c'è un gelataio c'è un solo incrocio ad un isolato di distanza in cui lo si trova. Questo requisito si può giustificare con la necessità di non avere troppa concorrenza. Non si vuole cioè che ci siano due gelatai alla stessa distanza da un incrocio.

Il problema che si pone è allora capire come, assegnata la mappa della città (i.e. il suo grafo corrispondente), allocare i gelatai.

Supponiamo che la mappa di un quartiere sia rappresentabile dal seguente grafo costituito da 16 vertici. Il numero di lati supportati da un vertice è chiamato valenza del vertice.

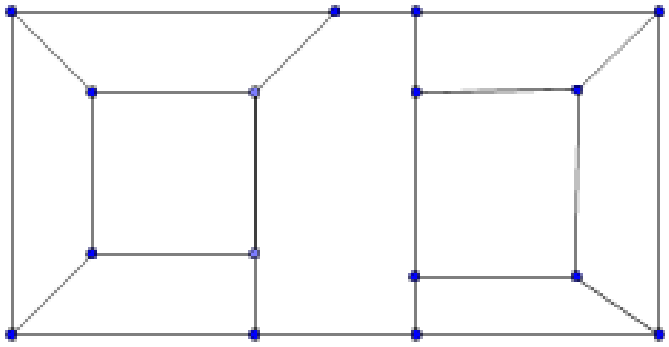


Figura 3 Grafo con 16 vertici

Definiamo in un grafo l'intorno di un vertice come l'insieme dei punti che sono connessi al vertice in questione tramite un arco, incluso lo stesso vertice.

E' opportuno fare diversi esempi del concetto di intorno utilizzando il grafo.

Un codice perfetto CP[2] del grafo assegnato è un sottoinsieme di vertici del grafo tale che ogni vertice, sia interno che esterno al sottoinsieme, appartenga all'intorno di un solo vertice del sottoinsieme CP. In altre parole ogni vertice del grafo è congiunto ad uno solo vertice del codice perfetto.

Non tutti i grafi hanno un codice perfetto ma quelli che useremo avranno sempre uno o più codice perfetto.

Definiamo in maniera più formale l'intorno ed il codice perfetto.

Indichiamo con v un vertice e con N(v) l'insieme costituito dai vertici collegati a v incluso il vertice stesso. In notazione insiemistica:

$$N(v) = \{incroci\ adiacenti\ a\ v\} \bigcup \{v\}$$

Il codice perfetto CP è un sottoinsieme dell'insieme V dei vertici del grafo:

$$CP \subset V = \{vertici\}$$

Tale che:

$$\forall\, v \in V, \quad l'intersezione\ CP \bigcap N(v)\ \grave{e}\ costituita\ da\ un\ solo\ elemento$$

[2] Il termine "codice perfetto" non viene dalla crittografia ma dalla teoria di correzione degli errori nei codici.

Determinare un codice perfetto è un problema che ha soluzione, il numero di combinazioni teoriche da provare è pari a 2^{16}=65536 per un grafo con 16 vertici. A questo numero si arriva considerando che per ciascun vertice si hanno due possibilità. Nel caso del problema del gelataio il Codice perfetto CP è una soluzione al problema dell'allocazione dei gelatai secondo le ipotesi esposte.

Un codice perfetto del grafo mostrato precedentemente è rappresentato nella figura seguente dove i vertici del codice perfetto sono indicati con cerchi di raggio più grande.

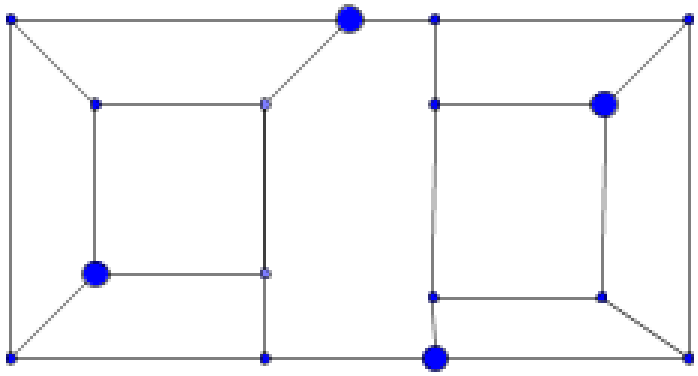


Figura 4 Un codice perfetto del grafo precedente

Sebbene determinare il codice perfetto a partire da un grafo sia un compito impegnativo, è facile verificare che sia oppure no soluzione. Questo ci rimanda alla questione NP vs P.

Crittografia con i grafi

Mostriamo ora come utilizzare i grafi e i codici perfetti per implementare un sistema a chiave pubblica. Questo metodo è stato introdotto da Koblitz e viene descritto nell'articolo "Cryptography as a Teaching Tool" [Koblitz-2].

Supponiamo di avere necessità di inviare una informazione cifrata perché in presenza di altre persone in ascolto. Un esempio familiare è l'acquisto di un prodotto via internet attraverso la carta di credito. Tale acquisto avviene digitando ad un certo punto il numero della carta. Il collegamento tra il nostro computer (B) ed il server della compagnia da cui stiamo acquistando il prodotto (A) non è diretto ma passa attraverso altri soggetti intermedi (C) che potrebbero intercettare il numero. Occorre quindi crittare il numero della carta di credito ma in questo caso A e B non hanno potuto concordare una chiave da utilizzare.

Fissiamo un intero n. Per esempio sia n=4 e si voglia comunicare un messaggio segreto per il quale siano possibili 4 valori: 0,1,2,3. Il messaggio da trasmettere è uno di questi quattro possibili valori.

Supponiamo di avere tre studenti: Andrea (A) che riceve la comunicazione da decifrare, Barbara (B) che invia la sua risposta cifrata, Carlo (C-nemico) che vuole intercettare e decifrare il messaggio segreto.

I tre studenti concordano la domanda, per la quale siano possibili quattro risposte. Una delle domande che si è proposto al laboratorio è stata la seguente: “Quale ragazzo ti piace?” Le possibili risposte siano per esempio: Carlo (=0), Davide (=1), Enrico (=2), Giovanni (=3).

Barbara risponde pubblicamente ma non vuole che Carlo sappia la risposta visto che è anche lui nella lista.

Altra possibile domanda. Quale materia preferisci? Matematica (=0), italiano (=1), inglese (=2), filosofia (=3).

Le regole del gioco sono le seguenti: Se Andrea e Barbara riescono a comunicare senza che Carlo decifri la risposta, allora Andrea e Barbara vincono. Se Carlo determina la risposta, allora Carlo vince mentre Andrea e Barbara perdono. (Andrea e Barbara perdono anche nel caso in cui B compia un errore aritmetico nella cifratura del messaggio).

Chi cifra (Barbara) la risposta non ha bisogno del codice perfetto. Barbara parte dal grafo che gli viene consegnato dagli insegnanti[3] e scrive su ciascun vertice un qualsiasi numero (scelto tra 0,1,2,3 se si utilizza la somma modulo 4) a caso a parte l’ultimo vertice (uno qualsiasi) il cui numero verrà scelto in modo che la somma modulo 4 complessiva di tutti i vertici dia il numero m da comunicare. Formalmente:

$$\sum_{v \in V} n_v = m \ (\text{modulo } n)$$

Considerando il grafo mostrato in precedenza, otteniamo per una risposta pari a m=3 ad esempio la seguente configurazione:

[3] In alternativa, avendo più tempo, gli studenti nel ruolo di Andrea potrebbero generare da sé i grafi con codice perfetto. Andrea dovrebbe, seguendo i passi 1-3, costruire un grafo a partire da un insieme di punti (16 punti nel nostro caso) assegnatogli dal docente, scegliendo il sottoinsieme che faccia da codice perfetto. Barbara e Carlo copiano poi il grafo costruito da Andrea. In questo modo Andrea, il ricevente del messaggio segreto, produce la sua chiave pubblica, in accordo alla teoria della crittografia a chiave pubblica.

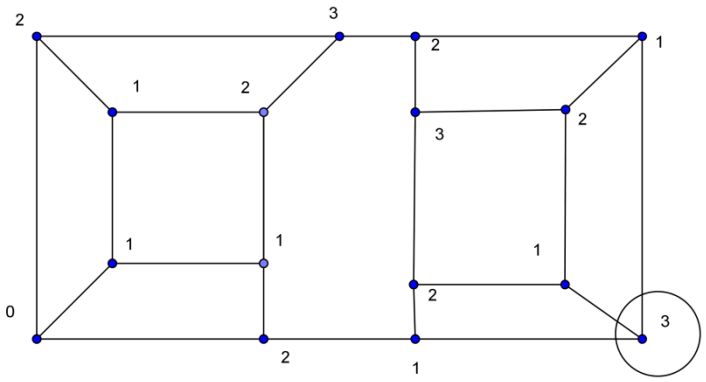


Figura 5 Grafo (C) che costruisce Barbara, scrivendo numeri qualsiasi associati a ciascun vertice, tranne l'ultimo numero (cerchiato in figura) che viene scelto in modo che la somma totale corrisponda alla sua risposta (m=3)

Osserviamo che trattandosi di una somma modulo 4, ogni volta che sommando un gruppo di numeri si arriva a quattro si ricomincia da zero. Questo grafo rimane segreto perché altrimenti sommando i numeri chiunque conoscerebbe la risposta. A partire da questo grafo Barbara costruisce un grafo (che rappresenta la chiave pubblica) in cui per ogni vertice scrive un numero che è pari alla somma dei numeri che si trovano sui vertici del suo intorno (incluso il numero associato al vertice stesso). Questo grafico sarà pubblico e mostrato agli altri studenti. In formule, a ciascun vertice associo un numero:

$$n'_v = \sum_{v \in N(v)} n_v \ (modulo\ n)$$

La costruzione di questo grafo trasformato (che chiamo grafo C') è quella più ostica per gli studenti, in quanto è comune che facciano errori nella somma o nella determinazione dei vertici dell'intorno. Facciamo un esempio: Considerato il vertice in basso a sinistra del grafo precedente, i suoi vertici vicini hanno numeri 2,1,2 che vanno sommati al valore associato al vertice stesso, che è zero. Quindi 2+1+2+0=1 (modulo 4). Si scriverà questo numero vicino al vertice considerato e così si farà per ogni vertice del grafo. Il grafo che otterremo sarà il seguente.

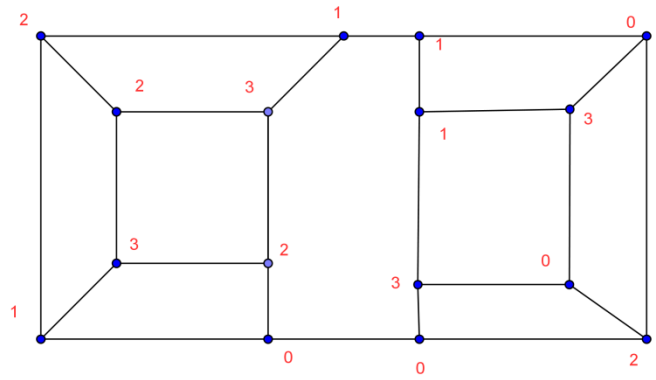


Figura 6 Grafo C' che costruisce Barbara a partire dal Grafo C, questo grafo è pubblico (nella spiegazione in classe è consigliabile utilizzare un colore diverso per i numeri di questo grafo)

Questo grafo è pubblico e rappresenta il messaggio cifrato.

Nel frattempo mentre Barbara cifra il messaggio - questa operazione richiede qualche minuto- Carlo (il nemico) cerca di determinare un codice perfetto nel grafo assegnato in figura 1, di cui gli è stata data una copia.

Il grafo C', una volta completato, viene mostrato sia ad Andrea che a Carlo. Il docente consegna ad Andrea il codice perfetto del grafo assegnato.

In fase di decifrazione Andrea riesce a determinare la risposta di Barbara (il numero m) utilizzando il codice perfetto (che corrisponde alla chiave privata), semplicemente sommando i numeri che si trovano sui vertici del codice perfetto nel grafo C'. Nel caso della figura 6 e figura 4 otteniamo: 3+1+0+3=7 (modulo 4) che corrisponde al m=3 scelto da Barbara inizialmente.

Possiamo formalizzare questa proprietà nel seguente modo:

Proprietà del codice perfetto: Se CP è un codice perfetto del grafo allora:

$$\sum_{v \in CP} n'_v = m \ (modulo\ n)$$

La dimostrazione si basa sul fatto che il codice perfetto rappresenta una partizione dell'insieme di vertici del grafo. Ogni vertice del grafo è collegato ad un solo vertice del codice perfetto. Nel grafo C' già compare la somma degli intorni. Allora sommando i numeri n'_v associati ai vertici del codice perfetto otteniamo la somma m del grafo C:

$$\sum_{v \in CP} n'_v = \sum_{v \in V} n_v = m \ \ (modulo\ n)$$

In appendice A riportiamo sei differenti grafi utilizzati nel laboratorio condotto nelle scuole. Per ciascun grafo viene fornito la versione con il codice perfetto da consegnare a chi decifra insieme ad altre tre repliche del grafo che devono essere date agli studenti suddivisi in gruppi da tre (A,B,C).
Osserviamo nuovamente che il codice perfetto rappresenta la chiave privata, il grafo nel suo complesso è la chiave pubblica.

Come costruire un grafo a partire dal suo codice perfetto?

In questa sezione descriviamo il metodo utilizzato per costruire dei grafi con codice perfetto.
Supponiamo di disporre un insieme di punti su un foglio. Questi rappresenteranno i vertici del grafo. Nei laboratori condotti abbiamo considerato codici perfetti costituiti da quattro vertici

(ordine 4), ciascuno di valenza 3. Ciò implica che il numero di vertici del grafo è costante e pari a 16.

Passo 1: Si sceglie un sottoinsieme di punti **CP** che rappresenti il codice perfetto. Nel nostro caso si scelgono 4 vertici.

Passo 2: Si tracciano delle linee (o archi) da ciascun punto non scelto (cioè non appartenente al codice perfetto) ad uno dei punti fissati, in modo che ogni vertice è connesso a esattamente uno dei vertici di **CP**. Se si vuole una valenza pari a tre, ciascun vertice del codice perfetto è collegato a tre vertici non del codice perfetto. Ciascun vertice di **CP** è il centro di una stella. I vertici non appartenenti a C sono i punti esterni della stella. (si veda la figura seguente)

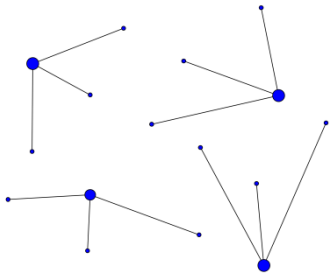


Figura 7 Passo 2 nella costruzione di un grafo. I pallini più grandi indicano i vertici del codice perfetto

Passo tre: Si tracciano delle linee addizionali tra i punti non di **CP**, in altre parole si collegano i punti esterni delle stelle tra di loro. Si possono collegare anche i punti esterni della stessa stella. Lo scopo è di rendere difficile la scoperta dei centri delle stelle, cioè l'individuazione del codice perfetto **CP**. **Bisogna fare attenzione a non disegnare alcun nuovo arco dal centro delle stelle verso i vertici**. Se questo accadesse allora non si avrebbe più un codice perfetto perché un vertice sarebbe collegato a due vertici del codice perfetto, e non varrebbe più la proprietà del codice perfetto dimostrata prima. Nei grafi generati ogni vertice ha valenza tre, anche quelli non appartenenti al codice perfetto.

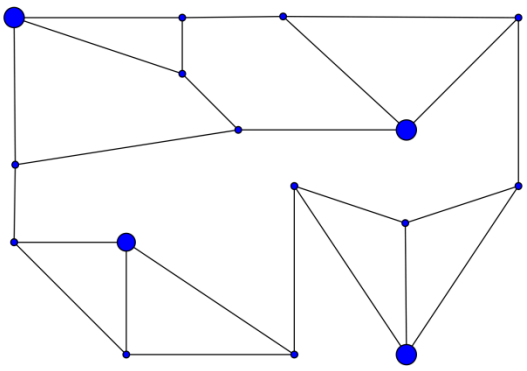


Figura 8

Come programma per disegnare i grafi si è utilizzato GeoGebra [GeoGebra]. Si tratta di un programma di geometria dinamica e algebra, di facile utilizzo, distribuito ed utilizzabile

liberamente. GeoGebra consente di ingrandire le dimensioni dei punti definendo lo stile, caratteristica che abbiamo utilizzato per rappresentare i vertici del codice perfetto. Inoltre i punti e le linee possono essere spostati per rendere il grafo finale più simmetrico.

Conclusioni

Il laboratorio si è rivelato efficace e coinvolgente per le diverse classi a cui è stato proposto. (Le classi erano costituiti da una trentina di studenti per volta). Occorre avere abbastanza tempo per poter fare qualche esempio prima di mettere gli studenti all'opera. In particolare è necessario spiegare nel dettaglio e più volte come costruire il grafo C' a partire dal grafo C. Inoltre è opportuno che ci siano più insegnanti che possano assistere e controllare il lavoro svolto. Per poter svolgere il laboratorio in poco tempo è necessaria un'attenta pianificazione e organizzazione.

Circa due o tre studenti per classe sono riusciti a trovare il codice perfetto del grafo assegnato. I grafi con sedici punti, come quelli proposti, risultano un po' troppo semplici per studenti di classi seconde delle Scuole Superiori. Per tali classi si potrebbero proporre grafi con un numero maggiore di vertici, ma bisogna fare attenzione a non esagerare altrimenti si appesantisce troppo il compito di chi deve cifrare il messaggio generando il grafo C' (allungando inevitabilmente i tempi).

Riferimenti

[Koblitz-1] N. Koblitz, A Course in Number Theory and Cryptography, Graduate Texts in Mathematics 114, Springer, New York 1987

[Singh] S. Singh, Codici e segreti, Rizzoli 1997

[Diffie, Hellman] W. Diffie, M.E.Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 1976

[RSA] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Comm. ACM 1978

[Koblitz-2] Cryptography as a Teaching tool
http://www.math.washington.edu/~koblitz/crlogia.html

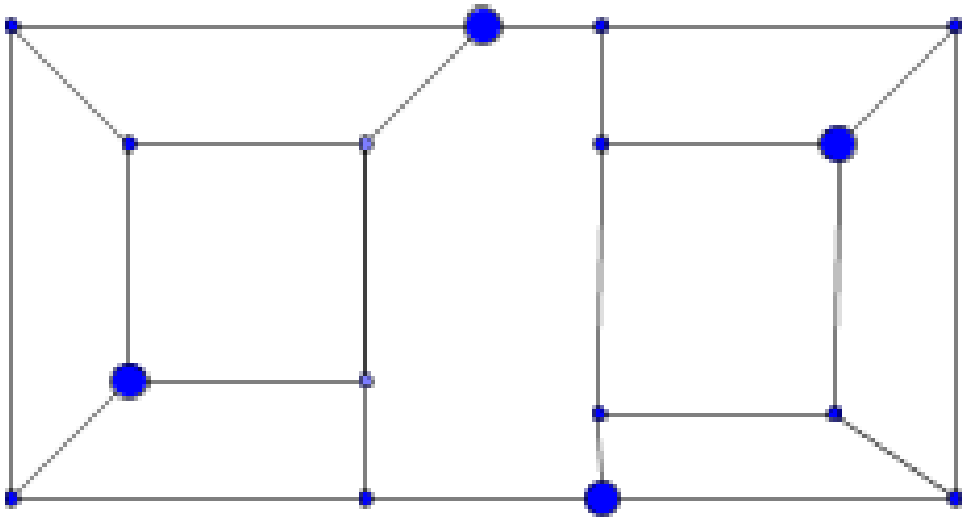
[GeoGebra] GeoGebra - Dynamic Mathematics for Schools, http://www.geogebra.org/

Appendice A - Grafi con codice perfetto

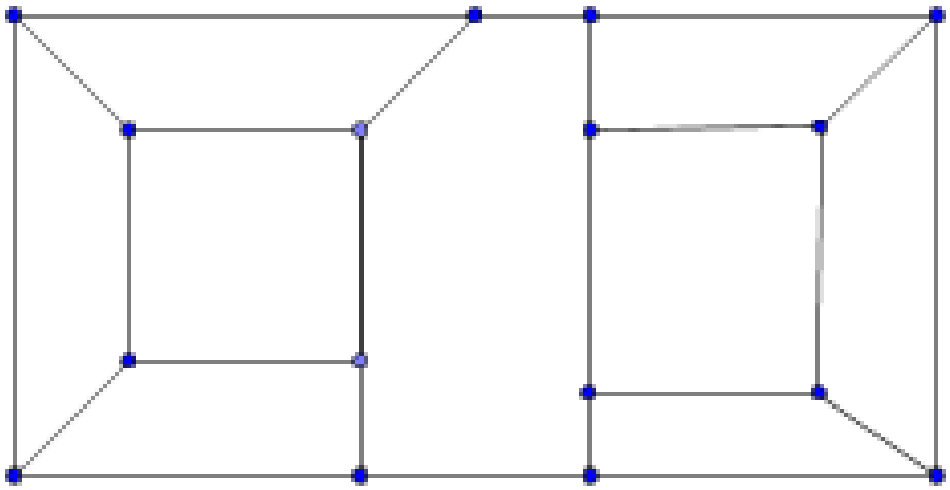
In questa appendice forniamo sei differenti grafi utilizzati durante il laboratorio. Nella copia 1.a è indicato il codice perfetto che va consegnato ad Andrea al momento opportuno. La copia 1.b è il grafo da consegnare sin dall'inizio a Carlo (il nemico). La copia 1.c viene utilizzata da Barbara per codificare la sua risposta, questo grafo non va mostrato. Infine, la copia 1.d corrisponde al grafo C', in cui il messaggio viene cifrato. Questa copia viene mostrata ad Andrea e Carlo.

Quindi a ciascun gruppo di studenti vengono date queste quattro copie del grafo.

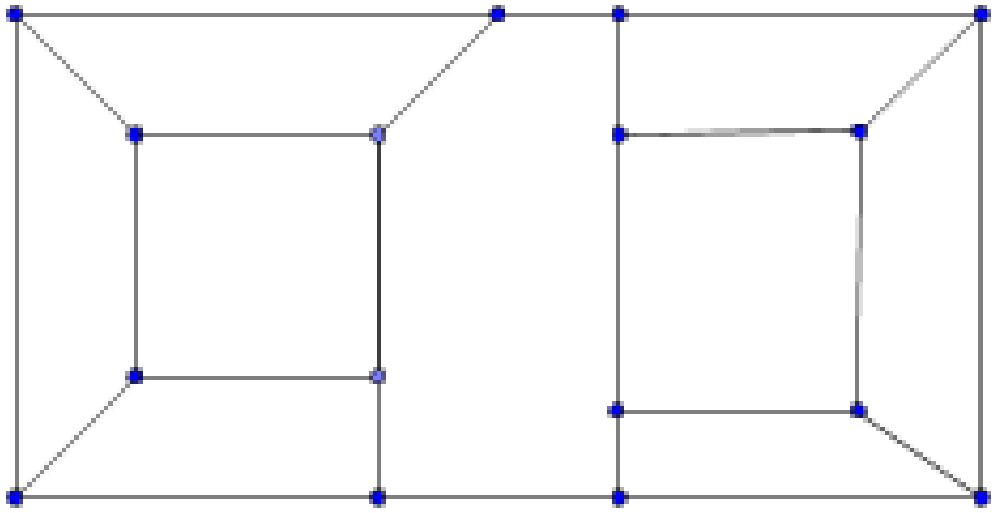
Grafo 1.a (Codice perfetto, SOLO a chi decifra)



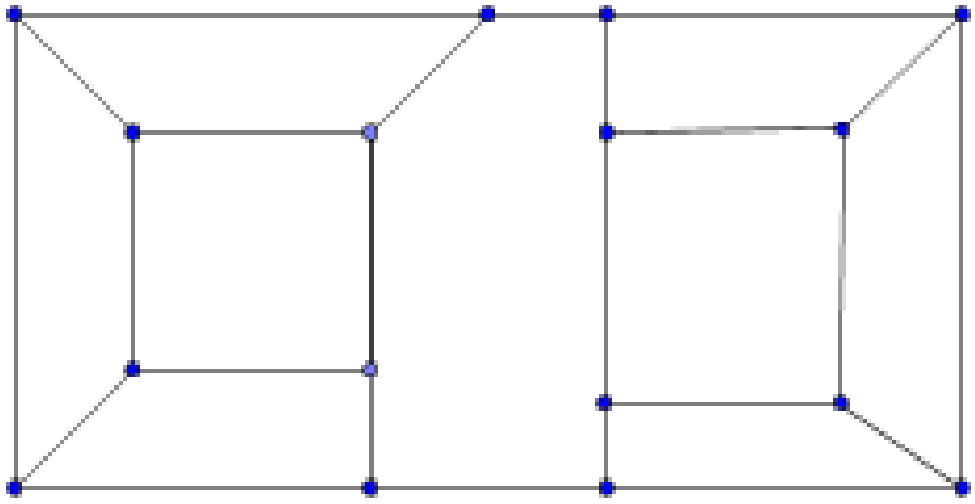
Grafo 1.b (da dare al NEMICO, che deve individuare il codice perfetto)



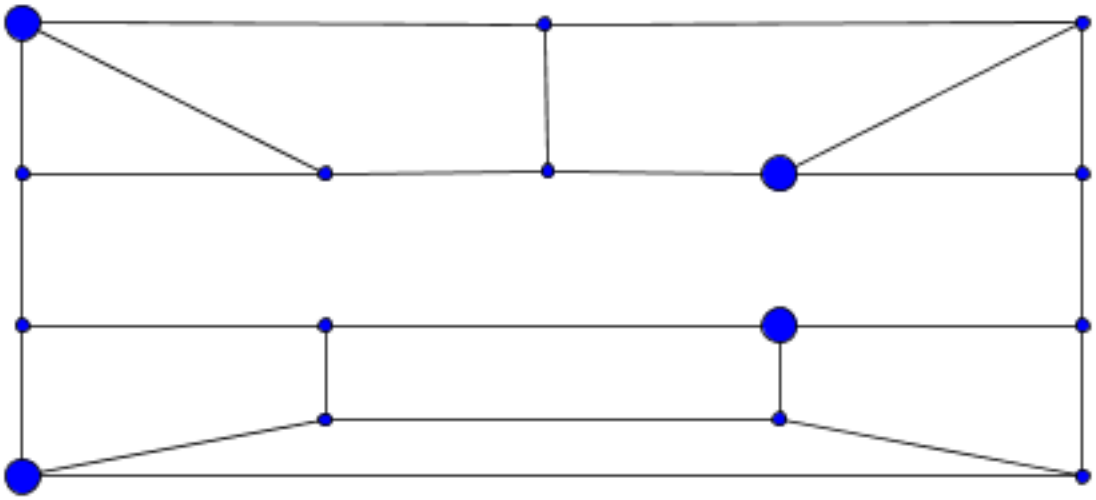
Grafo 1.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



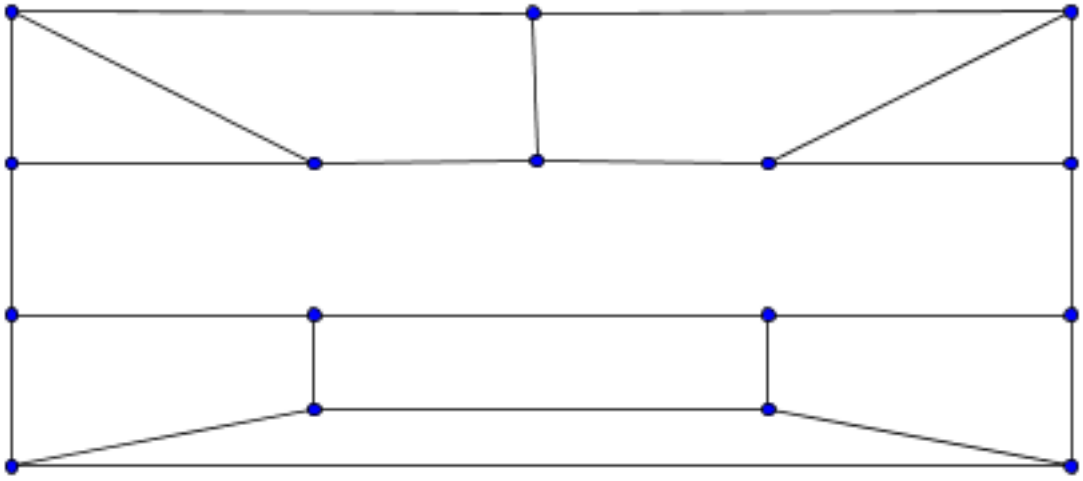
Grafo 1.d (Grafo C', da rendere PUBBLICO)



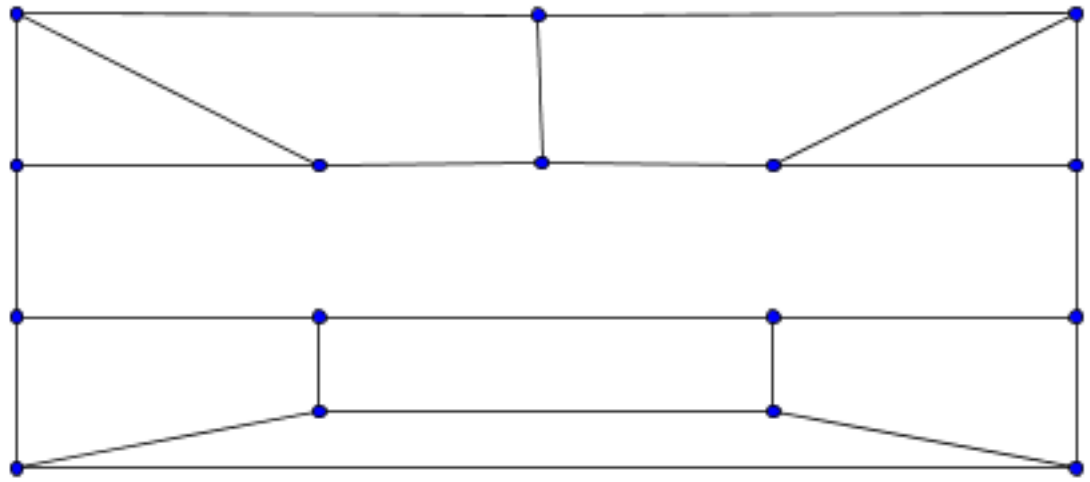
Grafo 2.a (Codice perfetto, da dare SOLO a chi decifra)



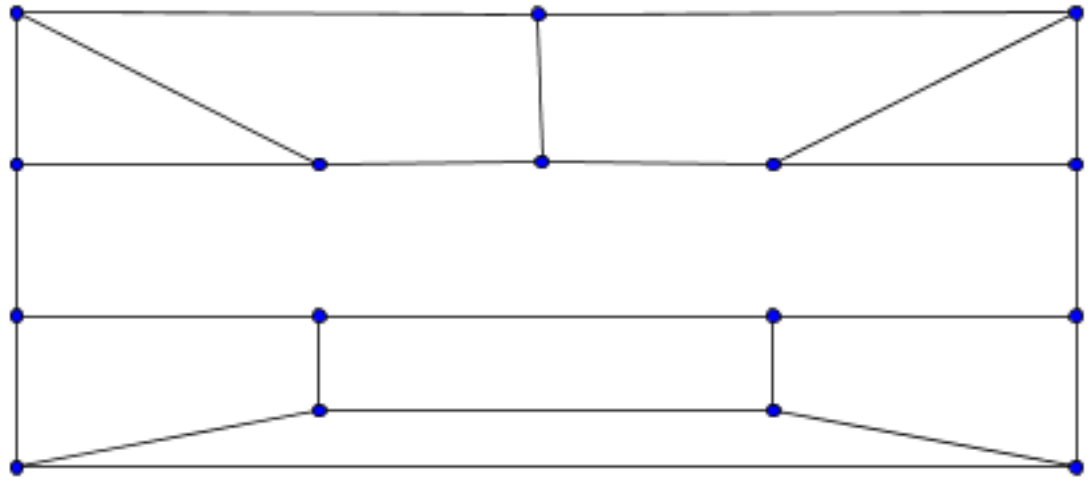
Grafo 2.b (da dare al NEMICO, che deve individuare il codice perfetto)



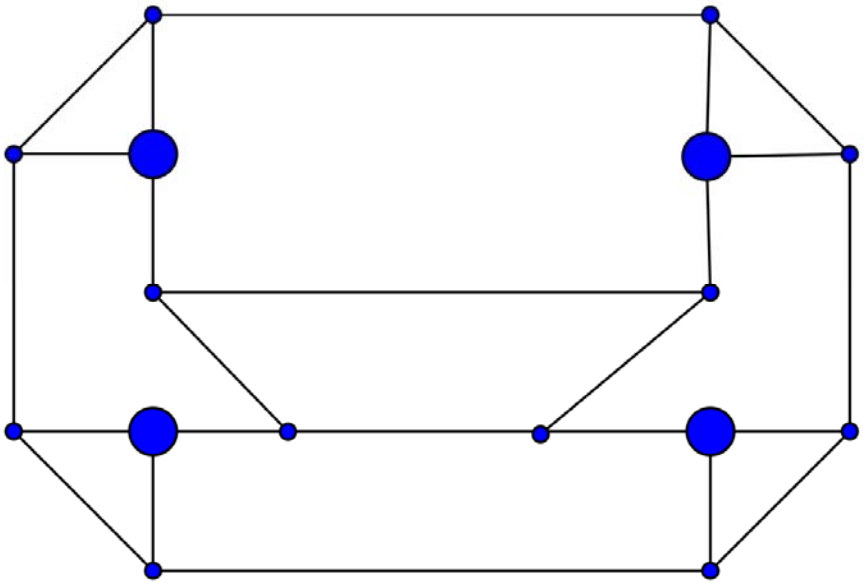
Grafo 2.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



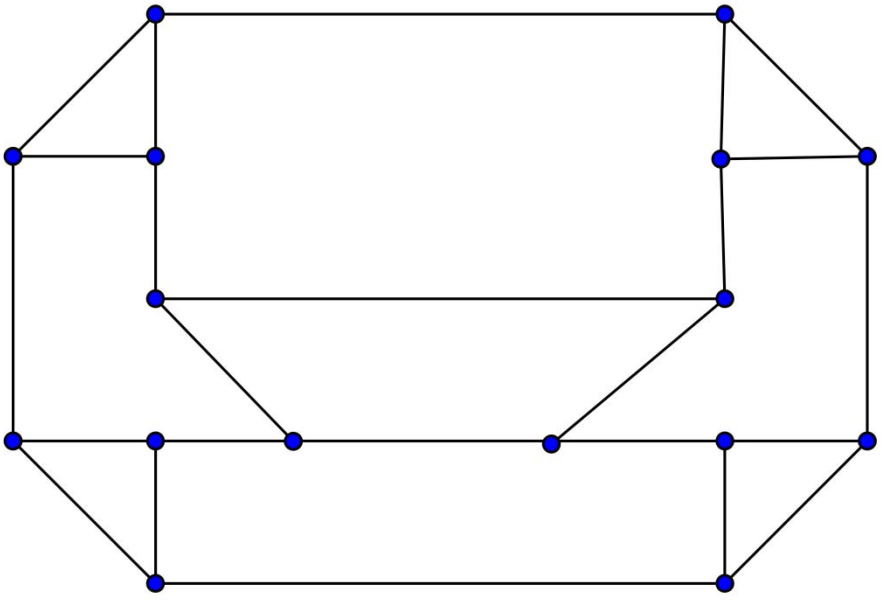
Grafo 2.d (Grafo C', da rendere PUBBLICO)



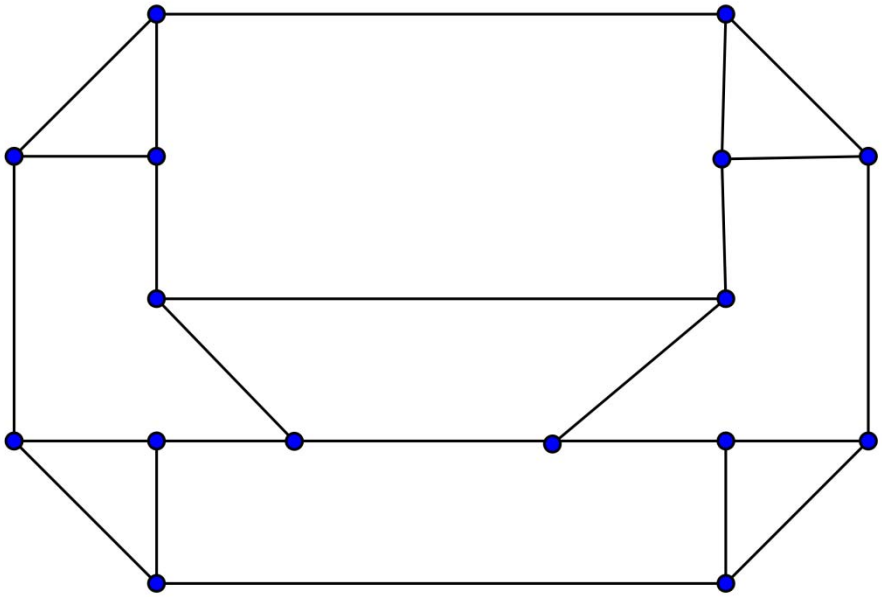
Grafo 3.a (Codice perfetto, SOLO a chi decifra)



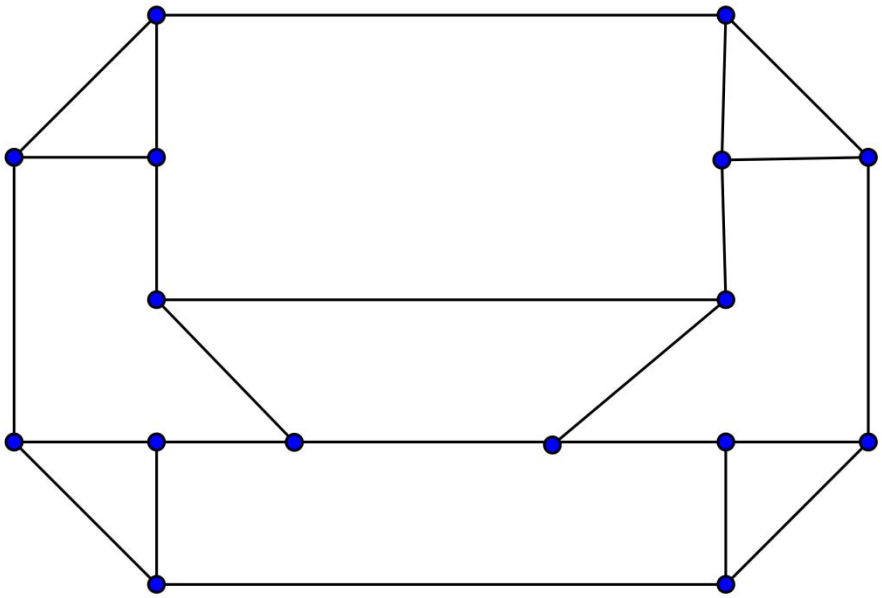
Grafo 3.b (da dare al NEMICO, che deve individuare il codice perfetto)



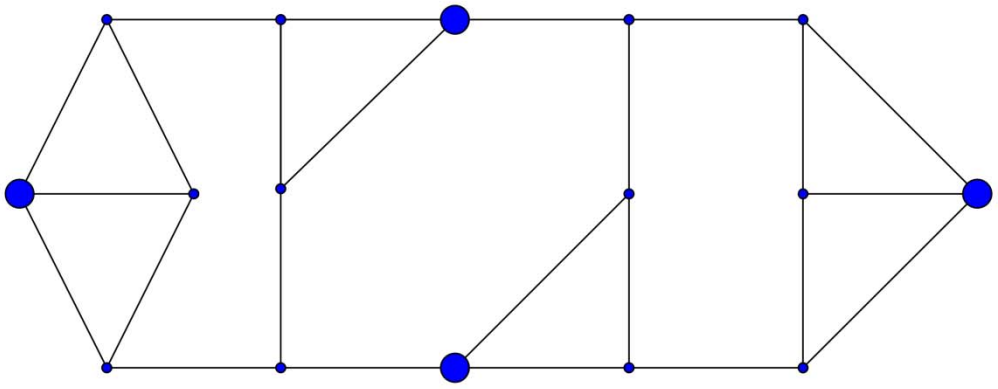
Grafo 3.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



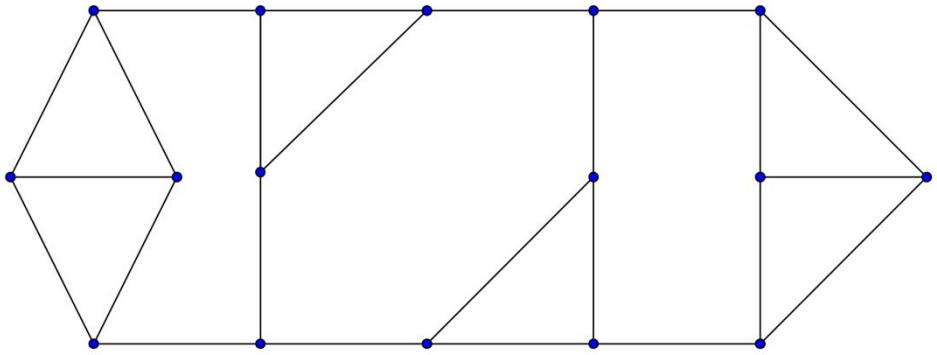
Grafo 3.d (Grafo C', da rendere PUBBLICO)



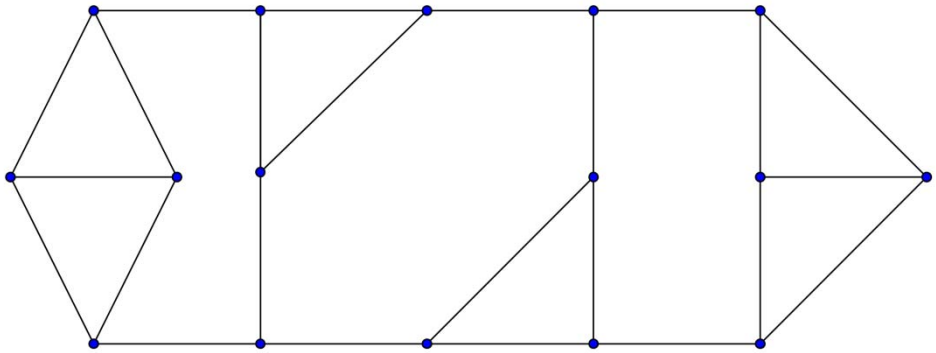
Grafo 4.a (Codice perfetto, da dare SOLO a chi decifra)



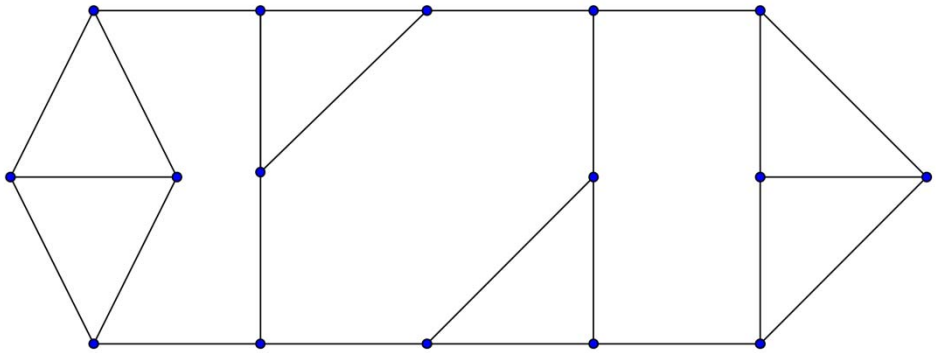
Grafo 4.b (da dare al NEMICO, che deve individuare il codice perfetto)



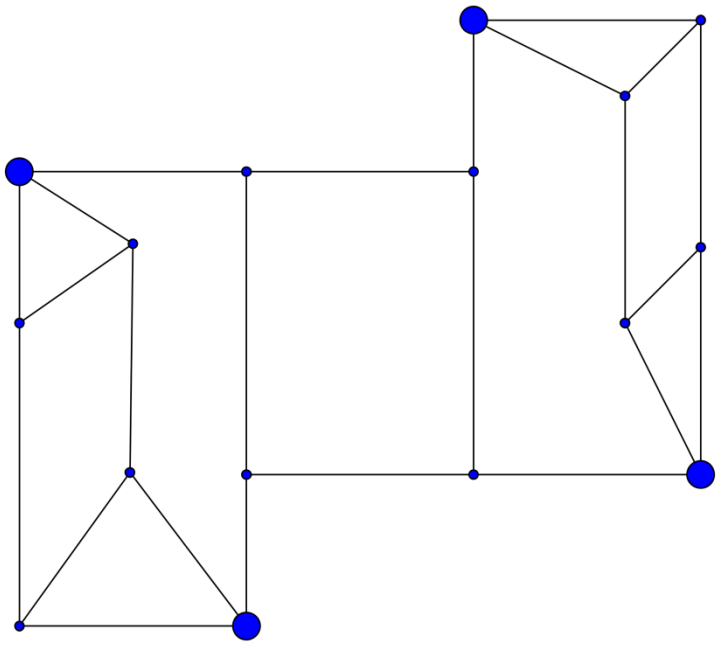
Grafo 4.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



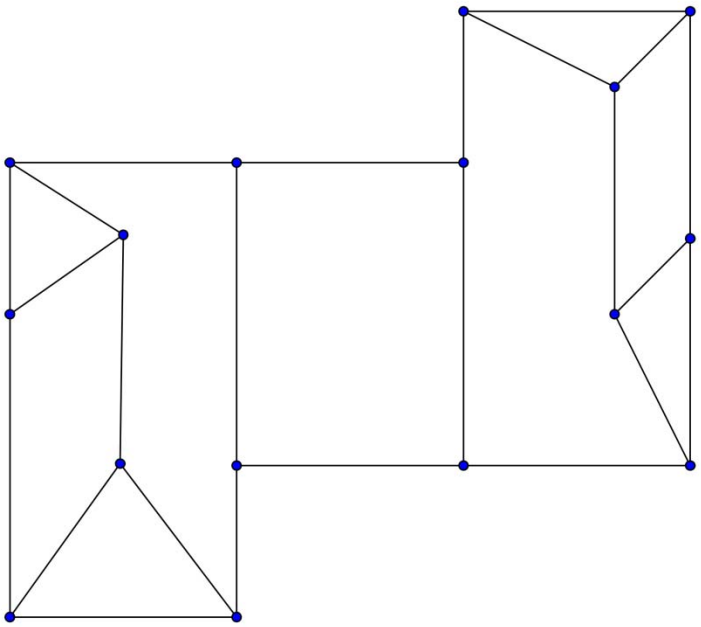
Grafo 4.d (Grafo C', da rendere PUBBLICO)



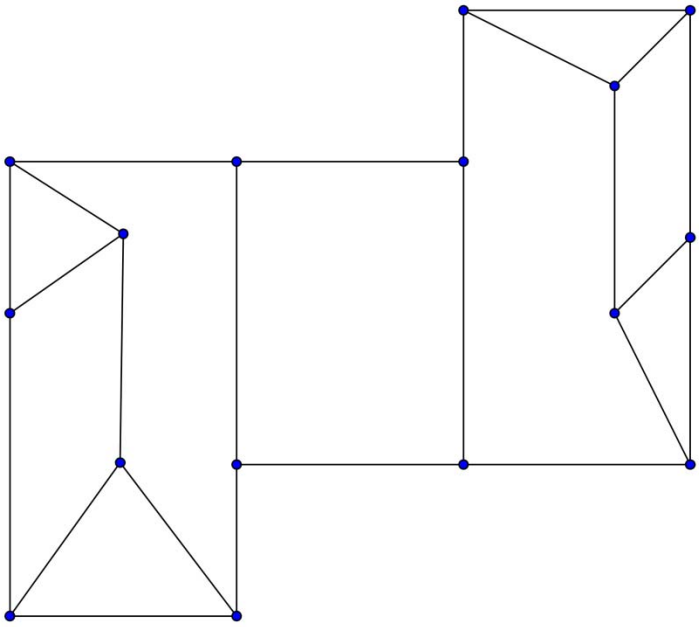
Grafo 5.a (Codice segreto, da dare SOLO a chi decifra)



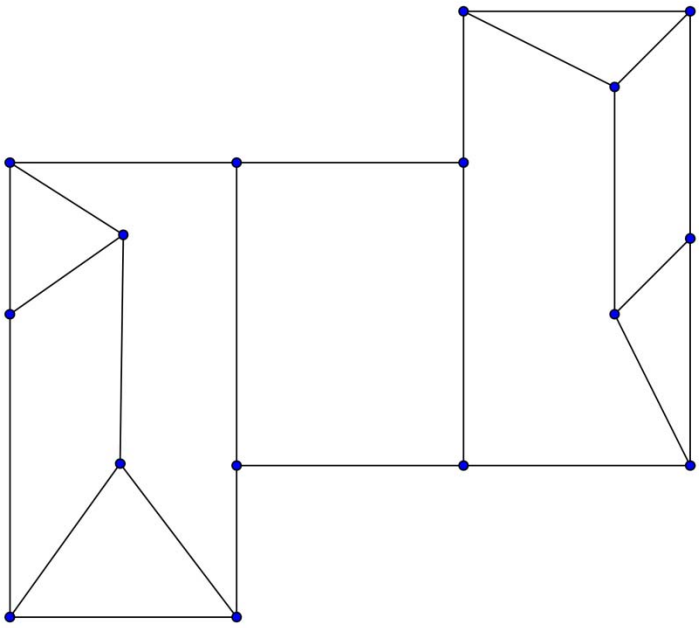
Grafo 5.b (da dare al NEMICO, che deve individuare il codice perfetto)



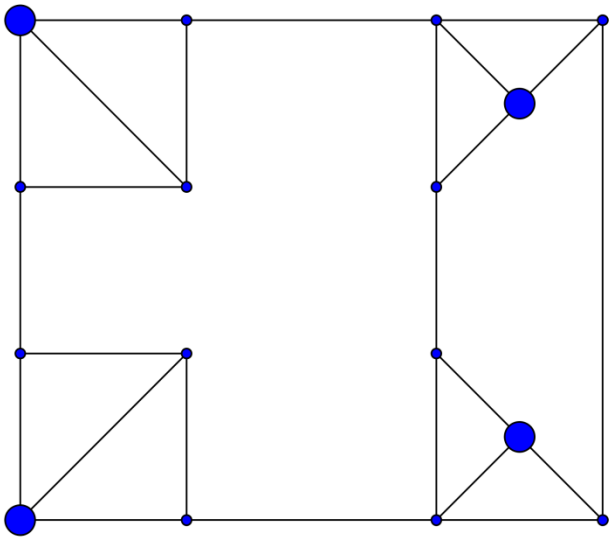
Grafo 5.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



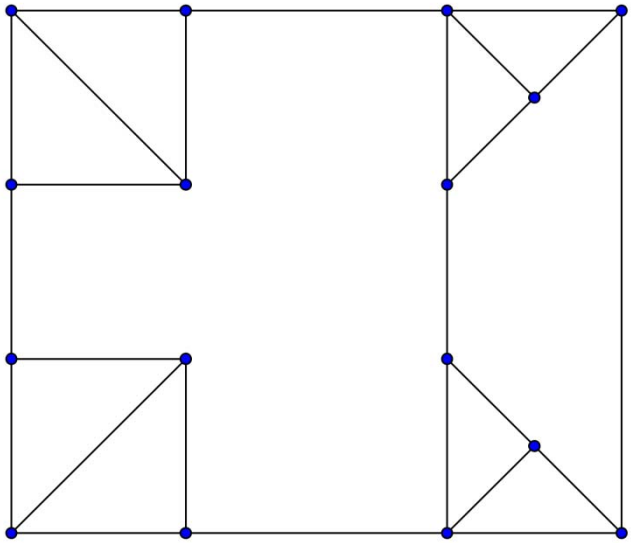
Grafo 5.d (Grafo C', da rendere PUBBLICO)



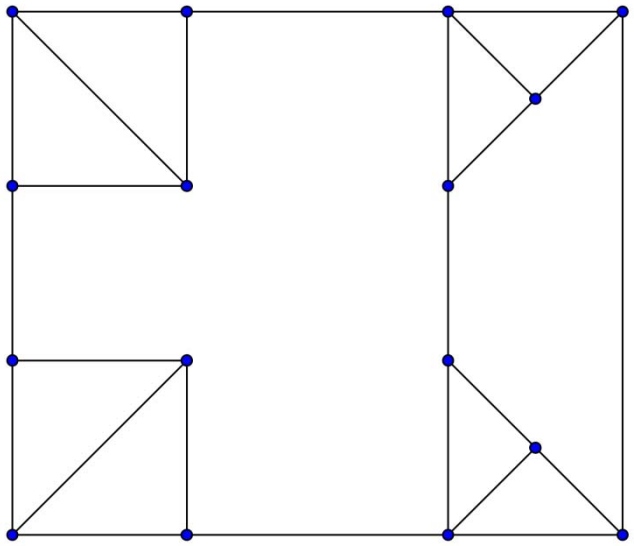
Grafo 6.a (Codice segreto, da dare SOLO a chi decifra)



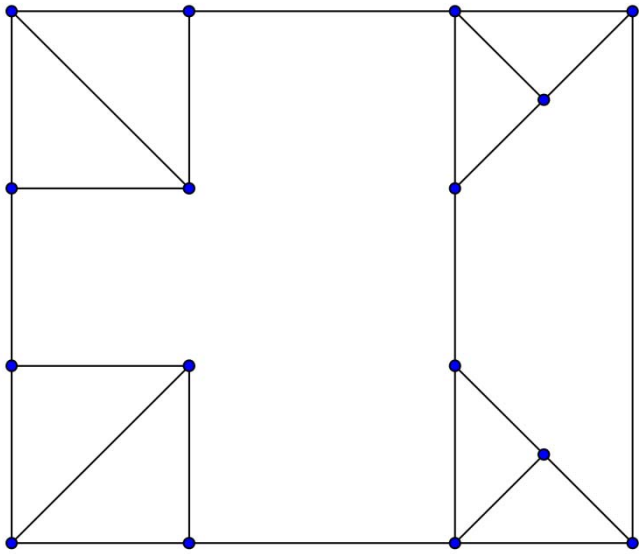
Grafo 6.b (da dare al NEMICO, che deve individuare il codice perfetto)



Grafo 6.c (Grafo C, per chi codifica il messaggio, da tenere SEGRETO)



Grafo 6.d (Grafo degli C', da rendere PUBBLICO)



Appendice B - Schema degli argomenti illustrati nel Laboratorio

Lo schema del laboratorio presentato agli studenti è il seguente:

Crittografia (Parte I) (2 ore)

Introduzione alla crittografia

Presentazione di metodi crittografici (a chiave privata) sotto forma di giochi (utilizzando una moneta, due monete, tre carte, etc.)

Problemi facili / difficili in matematica

Teoria dei grafi attraverso semplici esempi

Utilizzare i grafi per trasmettere segretamente le informazioni. Gli studenti in gruppi di tre proveranno a trasmettere e decifrare i messaggi utilizzando i grafi preparati dal docente

Crittografia (Parte II) (2 ore)

Aritmetica modulare (o aritmetica dell'orologio)

Il cifrario di Cesare

Decifrare dei messaggi cifrati con ruote di carta costruite appositamente