Dalla *scitala* lacedemone alla firma digitale:
piccola storia della comunicazione protetta.

Vincenzo Calabrò
Liceo-Ginnasio "B.Russell" di Roma
v.calabro@iol.it
http://users.iol.it/v.calabro

Abstract

Scopo del presente modulo pluridisciplinare è quello di informare il lettore delle tematiche didattiche relative al progetto di compresenza di linguaggi non verbali e multimediali (LNVeM) svolto durante l'anno scolastico 2000-2001 secondo un piano di lavoro modulare. Le discipline coinvolte riguardano LNVeM, Diritto, Italiano, Latino e Matematica. Gli insegnanti che hanno partecipato al lavoro annuale mediante didattiche personalizzate sono stati Vincenzo Calabrò (coordinatore del gruppo), R.Martino, N.Marini, G.Infantino e F.Peronace. L'attività è stata svolta nella classe 2ª Sez. Ca indirizzo scientifico per un totale annuale di ore 33 durante il periodo Novembre 2000-Maggio 2001. Il modulo è stato completato con una valutazione finale mediante un test a risposta aperta. Il progetto completo in forma ipertestuale si trova all'URL: http://web.tiscali.it/vincal/

Premessa

Non c'è alcuna ragione per non essere d'accordo con il fatto che i mezzi di comunicazione, attraverso i quali la gente comunica al giorno d'oggi e in modo sempre più onnicomprensivo, influenzano la loro maniera di pensare e anche la società in cui essa vive. Dal punto di vista della comunicazione, se pensiamo al passato, è noto che possiamo individuare, a grandi linee, alcune rivoluzioni che si sono susseguite nel tempo. Esse riguardano:

- la ***rivoluzione chirografica*** avvenuta in seguito alla invenzione della scrittura, circa 3 000 anni prima di Cristo;
- la ***rivoluzione gutemberghiana*** avvenuta per mezzo dell'invenzione della stampa, intorno al 1 500 dopo Cristo;
- la ***rivoluzione elettronica*** avvenuta inseguito all'invenzione di alcuni dispositivi di telecomunicazione (telegrafo e radio) intorno alla metà del 1 800 dopo Cristo (televisione, personal computer e cellulari) fine 1 900.

Come conseguenza di queste rivoluzioni si è ottenuto un risultato di notevole importanza, e cioè che la circolazione delle informazioni è avvenuta ***a velocità sempre crescente*** fino ad arrivare a quella attuale che ha il suo limite relativistico nella velocità della luce (c=300 000 km/s). Ma non solo. Altro grande risultato è stato quello di ottenere una comunicazione sempre più ***a basso costo*** e sempre ***più pervasiva***. Tutto ciò ha portato recentemente all'idea che vi sia, in modo ineluttabile, un passaggio dalla cultura tipografica del libro cartaceo a quella dei *media elettronici* in forma digitale. Sembra interessante ricordare l'osservazione di Massimo Baldini, il quale nella sua ***Storia della Comunicazione*** afferma che «sino ad allora le notizie si erano mosse alla velocità del messaggero, cioè alla velocità delle gambe dell'uomo o del cavallo, della corrente dei fiumi o della locomotiva dei primi treni. Tutti i tentativi di trasmissione istantanea dei messaggi erano falliti». Ed è vero. Fu solo con Samuel Morse (l'inventore del codice Morse e del telegrafo elettrico a fili) che

nel 1844 si inaugura negli Stati Uniti il primo collegamento telegrafico su filo tra Washington e Baltimora. E questa, afferma Baldini, «può essere assunta come la data di inizio della cultura dei media elettrici, di quella cultura, la nostra, in cui la tipografia ha visto venir meno il suo monopolio nel mondo della comunicazione». Abbiamo parlato di telegrafia attraverso i fili perchè in quella data la trasmissione dei segnali avveniva dentro dei fili di metallo. Solo alla fine del secolo (Heinrich Hertz, 1 888) vi fu il salto di qualità della trasmissione dei segnali nello spazio (si diceva allora, in modo scorretto, nell'*etere*) che anticipò di pochi lustri la trasmissione radio di onde elettromagnetiche nello spazio (Branly, Ducruet, Marconi, Popov). Fu solo con l'avvento del telegrafo, nota MacLuhan, che i messaggi poterono viaggiare più in fretta del messaggero. Baldini aggiunge altresì che «prima esisteva uno stretto rapporto tra le strade e la parola scritta. Con il telegrafo l'informazione si è staccata da materie solide come la pietra e il papiro, nello stesso modo in cui il denaro si era precedentemente staccato dalle pelli, dai lingotti e dai metalli per diventare carta. Il termine ***comunicazione*** è stato ampiamente usato con riferimento alle strade, ai ponti, alle rotte navali, ai fiumi e ai canali, prima di trasformarsi con l'era elettronica in ***movimento di informazione***». Il vocabolario (De Felice-Duro), alla voce comunicazione, dice testualmente: «l'***azione, il fatto di comunicare, e cioè di trasmettere e rendere partecipe***». Salvo alcuni usi isolati è comune soltanto nel significato di «portare a conoscenza, informare», soprattutto nella forma assoluta, senza specificazioni. ***Comunicazione*** è il fatto e il modo di portare a conoscenza, è la cosa stessa che si fa conoscere. Naturalmente si dipartono da queste poche ma interessanti considerazioni una serie di studi che sono allo stesso tempo importanti e straordinari. Si tratta di tutta una serie di rapporti molto profondi tra comunicazione e scienza, tra mondo dell'informazione e società che sono alla base di una enorme serie di studi che qui, come è facile comprendere, non è possibile affrontare. Accanto al potere e ai condizionamenti che la comunicazione esercita sulla società e sulla politica, una osservazione tra le tante ci sembra interessante proporla, a mo' di curiosità. E cioè che i torchi di Gutemberg diedero un contributo decisivo alla nascita della rivoluzione scientifica perchè la stampa permise di veicolare in modo efficace e innovativo i prodotti della cultura, mettendo a disposizione della scienza la raccolta delle informazioni, dei dati, che liberò gli scienziati dall'onere della copiatura manuale. Dal nostro punto di vista ci sono anche interessanti rapporti tra l'informazione e la comunicazione ***nascosta*** o ***segreta*** (ma noi, per meglio chiarire la terminologia, abbiamo preferito chiamarla «comunicazione ***protetta***», anche se spesso citeremo anche gli altri due aggettivi). La ragione è dovuta alla esigenza di rinnovati traffici commerciali e diplomatici, nonché di strumento al servizio di scopi militari e di spionaggio industriale. Ma non solo. Le nuove ragioni della ***comunicazione protetta***, sono altri e molto importanti. Queste ragioni hanno a che vedere con il tentativo di aiutare il cittadino, che vive in una società come quella attuale, che scruta e spia in continuazione le persone in modo tale da fornire sicurezza e protezione alla comunicazione per ragioni dovute alla privacy. Nel titolo del lavoro multimediale prodotto dalla classe 2°C a indirizzo scientifico compare l'acronimo ***PGP***. Si tratta di un programma gratutito per computer, ideato da Phil Zimmermann, che ha lo scopo di cifrare un messaggio (posto in forma digitale) in modo tale da renderlo illeggibile a tutti coloro i quali non sono i legittimi destinatari. PGP proviene dalle tre parole "Pretty Good Privacy" e nel mondo della informatica e della telematica rappresenta di fatto lo standard della crittografia mondiale. Nel mondo decine di milioni di utilizzatori lo adoperano ogni giorno per proteggersi da possibili intrusioni.Tenuto conto del quadro generale della Comunicazione e nella prospettiva di un approfondimento pluridisciplinare è di questo che qui si parlerà più in dettaglio.

Il "*Progetto didattico per la compresenza di Linguaggi e altre discipline*" previsto dal curricolo quinquennale al 2° anno del nostro liceo nell'indirizzo scientifico, che viene proposto qui di seguito, vuole mettere in evidenza il fatto che viviamo in pieno la cosiddetta "rivoluzione della scuola dell'Autonomia" che attiene alla sfera delle nuove prassi didattiche di cui questo progetto ne è un segmento, modesto ma significativo e, soprattutto, indicativo della nuova tendenza verso la quale la scuola moderna italiana si è incamminata.

Introduzione

Questo lavoro è stato progettato e realizzato dalla classe 2°C a indirizzo scientifico del Liceo Ginnasio "B. Russell" di Roma durante l'anno scolastico 2000/01. Il progetto è stato coordinato dal sottoscritto, che è stato l'insegnante di *Linguaggi non verbali e multimediali.* Mi assumo per intero la responsabilità del lavoro prodotto, in quanto sono stato il docente della disciplina di riferimento. In base al curricolo del liceo, ho avuto l'obbligo istituzionale di presentare al Consiglio di Classe il Progetto inerente al modulo relativo alle compresenze nel quale si inserisce questo lavoro. Nonostante siano trascorsi pochi anni dall'introduzione nella scuola delle nuove tecnologie, sembrano ormai lontani i tempi in cui il computer in classe aveva scatenato atteggiamenti irrazionali ed emotivi da parte di molti operatori scolastici: si trattino essi di scetticismo, di timori oppure di facili entusiasmi. Nel liceo *Russell* è ormai prassi consolidata che la stragrande maggioranza del corpo docente ha accettato di inserire, all'interno della propria didattica, l'uso del computer, inteso come strumento didattico per il conseguimento di obiettivi didattici ed educativi, non certo come fine. Quasi nessuno contesta più il valore formativo delle esperienze educative condotte in classe con le nuove tecnologie e, in particolare, con la multimedialità e la comunicazione in rete. Il valore formativo delle nuove tecnologie che permettono la *comunicazione* è insito nelle funzioni che si svolgono all'interno del processo di insegnamento e di apprendimento. La tecnologia in generale, e la multimedialità in particolare, consentono di sviluppare meglio, o di potenziare più specificamente, alcune capacità degli studenti in modo efficace e direi pure automatico. Certo il personal computer non è, e non rappresenta la panacea a tutti i mali della scuola. Tuttavia il lavoro degli studenti al computer stimola l'esercizio di funzioni importanti permettendo di acquisire abitudine alla gestione dei "processi" piuttosto che alla assimilazione passiva e recettiva di contenuti. Se poi la tecnologia viene adoperata come strumento al servizio della didattica, cioè come supporto alle attività della classe, allora l'apprendimento diventa più efficace e significativo. Da questo punto di vista il prodotto multimediale che la classe ha costruito, in collaborazione con i docenti delle diverse discipline, rappresenta un esempio di didattica aperta all'uso delle nuove tecnologie.

Il lavoro svolto ha lo scopo di fornire al lettore, nella metafora di Internet "navigatore" nei mari della produzione ipertestuale e iconica del progetto, concretamente e al di fuori delle nebulosità di principio, uno sguardo panoramico sul tema della comunicazione (segreta, o meglio, protetta). Si tratta, com'è noto, di un particolare tipo di comunicazione in cui fra emittente e destinatario si creano delle condizioni, più o meno clandestine, di complicità e di forte intesa in modo tale da celare la comunicazione medesima in forme più o meno nascoste. Mi riferisco ai vari tipi di comunicazione che vanno sotto il nome di gergo, crittografia, steganografia e, in genere, di tutte quelle forme di comunicazione che, per un motivo o per un altro, emittente e destinatario non sono disposti a rendere palese ad altri il contenuto dei loro messaggi. Tuttavia, sbaglierebbe clamorosamente colui che pensasse che l'intero lavoro annuale svolto potesse essere considerato un'idea pittoresca, magari originale , per riempire di contenuti un segmento di curricolo previsto dalla scuola dell'autonomia. In realtà, l'attività svolta è il risultato di un lavoro impegnativo e concreto, effettuato nell'arco dell'intero biennio, sul tema più vasto e generale della Comunicazione e che ha trovato nel corso del secondo anno, per una felice coincidenza, alcuni insegnati molto motivati a tentare di tracciare un percorso culturale didatticamente interessante e spendibile sul piano della motivazione degli studenti. La ragion d'essere del lavoro riguarda lo svolgimento del curricolo del 2° anno di liceo scientifico che si svolge presso il Liceo Ginnasio "B. Russell" di Roma e previsto dal corso di LNVeM, nel quale un modulo di 33 ore è destinato, obbligatoriamente, alla progettazione e allo sviluppo di un Progetto di compresenze che vari docenti devono effettuare per andare incontro a un preciso dovere che la nuova Scuola

dell'Autonomia impone a tutti i docenti che insegnano questa "area disciplinare" inserita ufficialmente nei nuovi curricoli liceali.

Nel licenziare il lavoro, frutto di impegno comune con altri quattro docenti di discipline diverse coinvolti nell'*avventura*, come docente presentatore del Progetto, oso sperare che esso venga accolto con l'attenzione che merita un'iniziativa sicuramente originale e per molti aspetti inusuale ma portatrice, a mio avviso, di un concreto contributo culturale alla formazione dei giovani che mi sento di definire utile. Utile non solo perchè finalizzato a far comprendere ai giovani l'importanza del tema della comunicazione nelle sue linee più generali, ma anche perchè le tematiche trattate sono e saranno vieppiù importanti per l'uso che la comunicazione fa e farà nella società contemporanea. Non sta a me giudicare se il lavoro che qui presento come conclusione di una fatica annuale è valido o meno. Quello che a me sta a cuore, come insegnante della classe, riguarda due aspetti che mi preme porre all'attenzione del lettore interessato. In primo luogo, esso ha la pretesa di giustificare l'attività svolta durante l'intero anno scolastico e di andare incontro all'esigenza di verificare la ***qualità*** dell'insegnamento svolto attraverso la certificazione del lavoro, che è stato costruito faticosamente di giorno in giorno. Concretamente questo significa che i Colleghi coinvolti hanno prodotto un lavoro che è la testimonianza concreta di un impegno che li ha coinvolti in prima persona, con interesse. Mi sento di affermare, senza tema di smentita, che essi hanno lavorato con impegno e aperta collaborazione. Più di questo non mi è consentito dire. Non è questa la sede adatta per parlare delle difficoltà organizzative incontrate durante l'intero anno scolastico che, com'è noto, sono difficoltà oggettive, nel nostro caso dovute agli impedimenti relativi all'inserimento nell'orario ufficiale delle lezioni delle compresenze stesse. In secondo luogo, questo ipertesto mostra il frutto di due anni di lavoro nel campo dell'utilizzo delle nuove tecnologie. Gli studenti hanno collaborato, con spirito aperto e motivata attenzione. Anche qui dico la stessa cosa che ho detto prima: non sta a me giudicare il livello e la qualità dell'ipertesto. Esso è il frutto di un lavoro non certo approfondito che manifesta grandi limiti e una inevitabile improvvisazione che è il frutto contemporaneo da una parte della difficoltà inerente al tema trattato e, dall'altro, degli ostacoli che inevitabilmente sorgono nel momento in cui diventa necessario affrontare temi quasi sconosciuti nella tradizione scolastica italiana come, per esempio, quelli che si riferiscono agli aspetti matematici della crittografia. Anzi. Il numero delle ore svolto è stato modesto, gli obiettivi didattici programmati non avevano come scopo quello di insegnare a far diventare gli studenti "esperti di pacchetti applicativi" per produrre pagine web professionali. Da questo punto di vista mi sento soddisfatto del livello di conoscenze e competenze che gli allievi hanno dimostrato di possedere nel campo della produzione ipermediale. Se poi il lavoro svolto avrà sviluppato anche curiosità, che presuppone un ulteriore interesse nei prossimi anni per la tematica affrontata, mi riterrò ancora più soddisfatto.

1. DISCIPLINE COINVOLTE

•Linguaggi non verbali e multimediali (LNVeM)
•Storia
•Italiano
•Diritto
•Matematica

2. MOTIVAZIONI

Il Progetto mira ad arricchire l'offerta formativa della scuola dell'Autonomia nella convinzione che le tematiche inerenti alla comunicazione e alle innovazioni tecnologiche che interessano lo scambio

di informazioni possano e debbano svolgere un ruolo positivo e trainante per la valorizzazione delle potenzialità cognitive e comunicative degli allievi anche in relazione all'utilizzo del computer.

3. OBIETTIVI SPECIFICI

- acquisizione della capacità critica di lettura delle variegate fonti di documentazione;
- valorizzazione delle potenzialità cognitive e comunicative;
- conoscenza e padronanza del mezzo informatico nella sua valenza strumentale e metodologica;
- distinguere forme di comunicazione fornita dai media tradizionali con strumenti digitali;
- saper integrare documenti di diversa tipologia per la produzione di ipertesti;

4. GIUSTIFICAZIONI

Perché la Crittografia? Diciamo che al giorno d'oggi la Crittografia, un tempo ritenuta appannaggio dei soli agenti segreti e del mondo diplomatico, sta sempre di più entrando nella vita di tutti i giorni. Essa sta cambiando il nostro rapporto con la società e con i nostri simili:

- perché garantisce la nostra privacy nell'era della comunicazione digitale in quanto è la sola risorsa che può dare assicurazione alla riservatezza di ogni comunicazione;
- perché garantisce la certezza dell'identità di un corrispondente, intesa come garanzia che ogni messaggio provenga realmente da colui (mittente) che afferma esserne l'autore;
- perché garantisce la certificazione, intesa come garanzia che ogni messaggio giunga al legittimo destinatario completamente integro e senza possibilità che sia stato intenzionalmente o per errore intercettato e/o modificato durante la spedizione;
- perché garantisce, con la firma digitale, l'autenticazione e la certificazione di documenti in formato elettronico come e meglio di quanto le firme tradizionali non facciano per i documenti cartacei.

E non è poco, si badi bene. In un mondo sempre più immerso nell'era della comunicazione digitale questo potente strumento è l'unico in grado di garantire certezza e sicurezza

5. PREREQUISITI

In relazione alla produzione di un ipertesto si richiede la conoscenza del funzionamento del mezzo informatico e di alcuni programmi applicativi

6. CONTENUTI

Produzione di un ipertesto col concorso delle seguenti discipline:

a) Storia: la comunicazione militare nella Grecia e nella Roma di Cesare con la scitala;.

b) Italiano: lo studio del percorso della comunicazione dall'antichità ai nostri giorni;

c) Diritto: un esempio di protocollo diplomatico che utilizza tecniche di cifratura nascosta o segreta;

d) Matematica: esempi di algoritmi e di funzioni adoperate nella crittografia;

e) LNVeM: l'uso di programmi applicativi per la codifica e decodifica di testi cifrati e la firma digitale;

7. ATTIVITÀ

Le attività didattiche saranno svolte principalmente in laboratorio multimediale alla presenza dei docenti che collaborano all'iniziativa mediante ricerche in rete con Internet di documenti e fonti di

informazione in grado di ripercorrere il cammino storico che va dai geroglifici egiziani alla firma digitale dei nostri tempi. Successivamente verranno svolte attività di redazione di un ipertesto che certifichi i risultati del lavoro. Le compresenze avranno lo scopo di permettere una riflessione più adeguata dal punto di vista delle conoscenze disciplinari che sarà necessario indagare. E' ovvio che le compresenze potranno sviluppare meglio e più approfonditamente le questioni che hanno più rilevanza sul piano culturale, e non si tralascerà occasione di permettere agli allievi di ripercorrere soprattutto storicamente il cammino che ha portato l'umanità a comunicare mediante codici e linguaggi diversi da quelli che comunemente si adoperano nella vita di tutti i giorni.

8. MEZZI E STRUMENTI TECNOLOGICI

a) parte hardware
- videoproiettore
- personal computer in rete

b) parte software
- powerpoint
- browser

c) parte cartacea
Alcuni saggi e volumi specifici;
Fotocopie;

9. TEMPI

- 11 ore per l'U.D. relativa alla compresenza con Storia;
- 11 ore per l'U.D. relativa alla compresenza con Italiano;
- 8 ore per l'U.D. relativa alla compresenza con Diritto;
- 3 ore per l'U.D. relativa alla compresenza con Matematica.

Calendario degli interventi didattici

	Ottobre	Novembre	Dicembre	Gennaio	Febbraio	Marzo	Aprile	Maggio
Compresenze con il docente di Italiano 11 h			3	2	2	2	2	
Compresenze con il docente di Storia 11h			1	3	2	2	1	2
Compresenze con il docente di Diritto 8h				1	2	2	1	2
Compresenze con il docente di Matematica 3h							1	2

10. VERIFICHE E VALUTAZIONE

- colloqui in situazione;
- test scritti con diversa tipologia di domande (vero/falso, a risposta chiusa, ecc..);
- produzione al computer di un questionario sottoforma di pagina web contenente 12 domande relative a tutte le discipline coinvolte.

Questionario di valutazione a risposta chiusa delle condizioni di uscita degli studenti. Ecco gli strumenti predisposti per la verifica sommativa, sintonizzate secondo la griglia di valutazione d'Istituto. Di seguito viene presentato il testo della prova finale.

Prova di accertamento finale relativa al "Progetto compresenze" del corso di Linguaggi
Classe 2° C (ind. scient.) - 22 Maggio 2001 h. 11.10-12.10

Costruisci a tuo piacimento con Front Page 2000 una pagina web che contenga sia il testo, sia le risposte al questionario curando anche la grafica e l'estetica della pagina.

I. Compresenza Italiano-LNVeM

1. Quali sono le differenze maggiori tra lingua e dialetto?
2. Che cos'è un codice?
3. Quali sono i sei fattori della comunicazione secondo Jakobson?

II. Compresenza Storia-LNVeM

1. Etimologia e significato/i della parola «crittografia»
2. Breve storia della «scitala lacedemone»
3. Definizioni dei seguenti termini: «cifratura, decifrazione, decrittazione»

III. Compresenza Diritto-LNVeM

1. Il commercio elettronico *e-commerce* rappresenta una rivoluzione nel sistema di scambio di merci: perché ci possa essere validità e certezza contrattuale si ricorre alla "Firma Digitale". Spiega come opera e come si applica tale sistema
2. Si sente parlare qualche volta di "pirateria informatica" che produce software illegalmente. Alla luce della legge n.633 del 22 Aprile 1941 sulla "Protezione del Diritto d'Autore e di altri diritti connessi al suo esercizio" esponi le tue impressioni facendo anche riferimento alla più recente Normativa dell'Unione Europea
3. La legge n.675 del 31 Dicembre 1996 sulla "Tutela delle persone rispetto al trattamento dei dati personali" è comunemente detta "legge sulla privacy". Analizza e commenta brevemente il trattamento dei "dati sensibili"

IV. Compresenza Matematica-LNVeM

1. Costruisci un diagramma a blocchi che traduce l'algoritmo della risoluzione di un sistema lineare di due equazioni in due incognite
2. Funzioni invertibili e non invertibili
3. Sistemi di numerazione posizionali e sistemi di numerazione additivi.

Griglia di valutazione

Test a risposta multipla (12 risposte aperta). Risultati:
0-3 fortemente insufficiente
4-5 insufficiente
6-7 sufficiente
8-9 ottimo
10 eccellente
Criteri per la determinazione dei livelli di prestazione raggiunti nei test a risposta multipla.
I 10 quesiti sono ripartiti (in %) sui seguenti obiettivi:

- 6 mirati alla valutazione della conoscenza;
- 2 mirati alla valutazione della competenza;
- 2 mirati alla valutazione della capacità.

Roma, 9 Giugno 2001 prof. Vincenzo Calabrò