Rendiconti Sem. Mat. Univ. Pol. Torino
Vol. 80, 2 (2022), 99 – **??**

Alexander Saltuari

DIDATTICA DELLA CRITTOGRAFIA E RILETTURA CONSAPEVOLE DELLE COMPETENZE SCOLASTICHE

Abstract. In questo breve articolo viene illustrato un percorso didattico di Crittografia svolto al biennio del liceo scientifico-matematico Ettore Majorana di Roma. Nucleo centrale dell'attivitá didattica é la creazione da parte degli studenti di un protocollo asimmetrico inedito. Questo laboratorio mette in luce le peculiari opportunitá offerte dalla Crittografia in chiave didattica.

1. Percorso Didattico

Alla fine del canonico percorso di Crittografia, tradizionalmente incentrato su tecniche crittografiche a chiave pubblica, viene introdotto il protocollo di Diffie Hellman. Per indirizzare l'argomento nella direzione voluta, il metodo viene introdotto nel seguente modo (con l'ausilio di presentazioni animate):

> *Immaginate un mondo nel quale tutti sappiano moltiplicare ma nessuno sia capace di eseguire una divisione. In un mondo del genere, Alice e Bob possono costruirsi una chiave comune al riparo da intercettazioni malevole: i due condivideranno pubblicamente un numero intero positivo N, detto chiave pubblica, e sceglieranno, ciascuno per conto proprio, un numero naturale segreto, detto chiave privata. Indichiamo le due chiavi private con A e B. A questo punto, ciascuno dei due interlocutori manderá all'altro il prodotto tra la chiave pubblica e chiave privata. Intercettare questi messaggi senza saper dividere, non permette ad un ipotetico intercettatore di ricavare le chiavi private (in un tempo ragionevole). Ad Alice e Bob non resta che moltiplicare il prodotto ricevuto con la loro chiave privata: entrambi otterranno lo stesso risultato A*B*N, che potrá essere usato come chiave comune nelle future comunicazioni cifrate.*

Agli studenti viene quindi richiesto di riunirsi in gruppi e di inventare un loro metodo di cifratura, adatto ad essere usato in protocolli di comunicazione liberamente ispirati a quello appena visto: il sistema deve permettere a due interlocutori di comunicare in modo protetto, con il presupposto che nessuno scambio di informazioni é al riparo da intercettazioni. Gli alunni scoprono autonomamente di aver bisogno di una procedura matematica che sia facile da eseguire ma proibitiva da invertire. Vengono quindi elencati tutti gli argomenti che i ragazzi hanno giá svolto al biennio scientifico, alla ricerca di una coppia *facile-difficile* adatta allo scopo. Ciascun gruppo, una volta scelta la procedura matematica, é invitato a ideare un sistema di comunicazione crittograficamente sensato.

2. Attivitá in laboratorio e proposte

Il lavoro di analisi del curricolo, svolto in una classe seconda, ha portato alle seguenti proposte facile-difficile.

ANNO DI SVOLGIMENTO AL LICEO SCIENTIFICO	UNITÁ TEMATICA	COPPIA "FACILE-DIFFICILE"
1° anno	Calcoli in $\mathbb{N}$ e $\mathbb{Z}$	**Facile**: moltiplicare fra loro numeri primi **Difficile**: scomporre un numero in fattori primi
1° anno	Fattorizzazione di polinomi	**Facile**: moltiplicare fra loro polinomi irriducibili **Difficile**: scomporre polinomi in fattori irriducibili
1°/2° anno	Equazioni intere	**Facile**: creare un'equazione intera a partire dalle soluzioni irriducibili **Difficile**: risolvere un'equazione intera
2° anno	I radicali	**Facile**: creare radicali innestati (ad esempio radicali doppi) **Difficile**: riscrivere espressioni irrazionali in forma non innestata
2° anno	Sistemi lineari	**Facile**: creare un sistema lineare a partire dalle soluzioni **Difficile**: risolvere un sistema lineare
1° anno	Struttura delle Teorie (introduzione alle Geometria)	**Facile**: dimostrare un enunciato a partire dagli assiomi (sapendo che si tratta effettivamente di un teorema) **Difficile**: da un gruppo di affermazioni, capire quali sono gli assiomi e quali i teoremi

Nota bene: quest'ultima coppia derivava da una tipologia di esercizio svolta in classe il primo anno nella cornice dei sistemi formali, argomento introduttivo alla Geometria euclidea.

3. Protocolli degli studenti

Gli studenti, divisi in gruppi, hanno quindi cercato di progettare protocolli di comunicazione che utilizzassero sistemi di cifratura basati su una delle coppie facile/difficile individuate. Soltanto due gruppi sono riusciti a creare protocolli di comunicazione

funzionanti, le idee elaborate (sotto la guida e con l'aiuto dell'insegnante) sono state messe alla prova in "simulazioni di comunicazione"

3.1. Protocollo A

Questo sistema é basato sulla coppia "creare un'equazione a partire dalle soluzioni" - "risolvere l'equazione" e permette la trasmissione di un numero intero da Alice a Bob.

Il protocollo di comunicazione prevede che il mittente Alice comunichi al destinatario Bob l'intenzione di comunicare. Con la sua chiave privata k, Bob creerá un polinomio a coefficienti interi di radice k. I coefficienti verranno comunicati ad Alice e costituiscono la chiave pubblica del protocollo. Con un procedimento matematico "difficile da invertire" come richiesto agli studenti, Alice "nasconderá" un numero intero n all'interno di un nuovo polinomio a coefficienti interi, generato a partire da n e dal polinomio pubblico. Trasmetterá infine i coefficienti del nuovo polinomio a Bob, che, grazie alla sua chiave privata, sará in grado di trovare n.

Riassumendo, il sistema prevede i seguenti parametri:

Parametro pubblico	Chiave pubblica : coefficienti interi del polinomio P
Parametro privato (di Bob)	La radice k di P ($k \in \mathbb{R}$)
Parametro privato (di Alice)	Durante i calcoli Alice usa un polinomio privato Q a coefficienti interi: si tratta di un polinomio che serve soltanto a "generare rumore" e non deve avere caratteristiche particolari.
Messaggio trasmesso da Alice a Bob	Il messaggio é costituito da una serie di numeri interi: si tratta dei coefficienti del polinomio che "nasconde" il messaggio n.

In basso lo schema di comunicazione e il meccanismo di cifratura proposti dal gruppo 1 degli studenti:

PASSAGGI	INTERCETTATO
1) Alice comunica a Bob che gli vuole mandare un numero intero.	Sí
2) Bob crea un polinomio P a coefficienti interi di cui solo lui conosce la radice k (k é un numero reale qualsiasi).	No
3) Bob trasmette i coefficienti del suo polinomi ad Alice	Sí
4) Alice moltiplica il polinomio P per un polinomio privato Q a coefficienti interi e aggiunge al prodotto l'intero n che vuole trasmettere a Bob.	No
5) Alice manda a Bob i coefficienti del polinomio $S = P \cdot Q + n$	Sí
6) Bob inserisce in S, al posto della variabile la radice k, calcola quindi $S(k)$. Dal momento che k annulla $P \cdot Q$, ottiene proprio n.	No

Come si vede, i due polinomi privati P e Q servono da "veicolo" a n, che viene nascosto all'interno del prodotto $P \cdot Q$. In classe il sistema é stato messo alla prova: il gruppo di lavoro si é diviso in due (Alice e Bob) e il resto della classe ha svolto il ruolo di "intercettatore malevolo". Nel lavoro di laboratorio, il protocollo ha subito mostrato la sua vulnerabilitá e giá al secondo tentativo alcuni studenti avevano capito

che per ricavare n bastava calcolare il resto della divisione $S : P$ (i polinomi S e P sono entrambi pubblici).

3.2. Protocollo B

Questo sistema é basato sulla coppia “moltiplicare fra loro numeri primi - scomporre un intero in fattori primi".

Il sistema permette ad A di trasmettere una sequenza di k interi positivi a B. Il protocollo prevede che il mittente Alice, comunichi al destinatario Bob l'intenzione di comunicare, informandolo della lunghezza complessiva k del messaggio in chiaro. Bob provvede a creare la chiave pubblica (che dipende da k e dalla chiave privata di Bob) e a trasmetterla. Alice adotterá un procedimento matematico (difficile da invertire in assenza della chiave privata, come richiesto agli studenti), combinando il messaggio con la chiave pubblica. Trasmetterá il numero cosí ottenuto a B, che, grazie alla sua chiave privata, sará in grado di ricostruire il messaggio di A.

Il sistema prevede i seguenti parametri pubblici e privati

Parametro pubblico	Lunghezza k del messaggio in chiaro (k é il numero di interi positivi che Alice vuol mandare a Bob)
Parametro pubblico	La chiave pubblica vera e propria: m interi positivi $I_1, I_2, \ldots, I_m$ (spediti da Bob ad Alice), con $m > k$
Parametri privati (di Bob)	m numeri primi m vettori linearmente indipendenti $v_1, v_2, \ldots, v_m$, con $v_j \in \mathbb{N}^m$.
Parametro privato (di Alice)	Alice sceglie in modo arbitrario k interi tra gli m pubblici: la selezione puó essere affidata al caso ed é opportuno che venga modificata ad ogni trasmissione.
Messaggio trasmesso da Alice a Bob	Si tratta di un unico numero intero positivo. Il procedimento matematico progettato dagli studenti genera numeri enormi: i ragazzi stessi hanno quindi coniato l'appellativo di “mostro" a indicare il messaggio trasmesso da Alice.

Dopo vari tentativi e proposte, il gruppo di studenti ha gettato le basi del sistema descritto in basso. Come vedremo, mancano ancora alcune parti fondamentali:

Questo protocollo, ideato fin qui a partire da un'idea originale dei ragazzi, ha posto gli studenti di fronte a due importanti interrogativi:

1. É possibile per Bob ricostruire $a_1, a_2, \ldots, a_k$ a partire da $H_1, H_2, \ldots, H_m$?

2. Gli interi $I_1, I_2, \ldots, I_m$ che Bob trasmette ad Alice, vanno costruiti con qualche criterio?

Per gli studenti, la situazione non era del tutto chiara da un punto di vista matematico. Per questo motivo si é passati ad un esempio numerico, immaginando la seguente comunicazione:

PASSAGGI	INTERCETTATO
1) Alice comunica a Bob che gli vuole mandare una sequenza composta esattamente da k numeri interi positivi (in seguito indicheremo con $a_1, a_2, \ldots, a_k$ il messaggio che Alice vuole trasmettere a Bob)	Si
2) Bob sceglie m numeri primi "grandi", con $m > k$ e li combina a creare m interi $I_1, I_2, \ldots, I_m$ (vedremo in seguito che la creazione degli interi I_h dovrá essere fatta "con giudizio"). Esempio: avendo scelto 6 numeri primi $p_1, p_2, \ldots, p_6$, potrebbe creare $I_1 = p_1^{10} p_2 p_5^6$, $I_2 = p_1^2 p_6$ e $I_3 = p_1 p_2 p_3 p_4 p_5 p_6$ cosí via.	No
3) Bob trasmette ad Alice gli interi $I_1, I_2, \ldots, I_m$ (in forma "espansa" non fattorizzata)	Si
4) Alice estrae da $I_1, I_2, ..., I_m$ una sottosequenza di k termini (vale infatti che $k < m$) mantenendo l'ordine relativo della sequenza originale. Indichiamo la sottosequenza con $J_1, J_2, \ldots, J_k$.	No
5) Ricordiamo che Alice vuole mandare a Bob la sequenza $a_1, a_2, \ldots, a_k$. Per fare questo trasmette al suo interlocutore il "numero mostro" $M = (I_1)^{a_1}(I_2)^{a_2} \cdots (I_k)^{a_k}$ (non in forma fattorizzata ma espansa).	No
6) Bob sa che M si scompone soltanto negli m numeri primi scelti da lui all'inizio. Ció gli consente in breve tempo di fattorizzare $M = P_1^{H_1} P_2^{H_2} \cdots P_m^{H_m}$. **Attenzione: gli esponenti $H_1, H_2, \ldots, H_m$ non sono "il messaggio di Alice" $a_1, a_2, \ldots, a_k$.**	No

PASSAGGI
1) Alice: "Voglio mandarti due numeri"
2) Bob sceglie 4 numeri primi $p_1 = 7; p_2 = 17; p_3 = 23; p_4 = 31$ e costruisce i seguenti interi: $I_1 = (p_1)^3(p_2)^2(p_3)^1(p_4)^2 = 2.191.004.081$, $I_2 = (p_1)^2(p_2)^0(p_3)^3(p_4)^0 = 1.459.759$, $I_3 = (p_1)^1(p_2)^1(p_3)^1(p_4)^2 = 2.630.257$ e $I_4 = (p_1)^2(p_2)^1(p_3)^1(p_4)^2 = 18.411.799$.
3) Bob trasmette ad Alice i suoi quattro interi 2.191.004.081, 1.459.759, 2.630.257, 18.411.799
4) Alice sceglie la sottosequenza I_2, I_4, per cui $J_1 = 1.459.759$ e $J_2 = 18.411.799$. Il messaggio che Alice vuole trasmettere a Bob é la successione $a_1 = 3$, $a_2 = 2$. Calcola quindi il numero "mostro" $M = (J_1)^{a_1}(J_2)^{a_2} = (1.459.759)^3(18.411.799)^2 = \ldots$
5) Alice trasmette a Bob il mostro 1.054.474.143.018.021.481.705.479.223.038.079.
6) Bob scompone M in $M = 7^{10}17^2 23^{11}31^4$.

Dopo breve discussione, gli studenti hanno riconosciuto che il problema si riduceva alla risoluzione del sistema riportato in basso nelle incognite $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ (si tratta degli esponenti applicati ai quattro interi di Bob, sono previsti quindi anche gli zeri per gli interi che Alice ha scartato). Eliminando i valori nulli, si ottiene il "messaggio" a_1, a_2.

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \begin{pmatrix} 3 & 2 & 1 & 2 \\ 2 & 0 & 3 & 0 \\ 1 & 1 & 1 & 2 \\ 2 & 1 & 1 & 2 \end{pmatrix} = (10, 2, 11, 4)$$

La soluzione del sistema é $\alpha_1 = 0, \alpha_2 = 3, \alpha_3 = 0, \alpha_4 = 2$, per cui il messaggio di Alice

ricostruito da Bob é la successione $3,2$.

Gli studenti sapevano che il sistema lineare aveva soluzione soltanto se la matrice era non singolare. Rispolverando il concetto di dipendenza lineare (svolto in classe), la classe si é dimostrata capace di perfezionare il protocollo nel seguente schema operativo:

PASSAGGI	INTERCETTATO
1) Alice comunica a Bob che gli vuole mandare una sequenza composta esattamente da k numeri interi positivi (in seguito indicheremo con $a_1, a_2, ..., a_k$ il messaggio che Alice vuole trasmettere a Bob)	Si
2) Bob sceglie m numeri primi "grandi", con $m > k$ e li combina a creare m interi $I_1, I_2, \ldots, I_m$ scegliendo m "vettori degli esponenti" $v_1, v_2, ...v_m$ linearmente indipendenti. Esempio: con $m = 3$, i vettori collegati a $I_1 = p_1^{10} p_2 p_3^6$, $I_2 = p_1^2 p_3$, $I_3 = p_1 p_2 p_3$ sono $v_1 = (10,1,6)$, $v_2 = (2,0,1)$, $v_3 = (1,1,1)$.	No
3) Bob trasmette ad Alice gli interi $I_1, I_2, ..., I_m$ (in forma "espansa" non fattorizzata)	Si
4) Alice estrae da $I_1, I_2, ..., I_m$ una sottosequenza di k termini $J_1, J_2, ..., J_k$, mantenendo l'ordine relativo della sequenza originale.	No
5) Alice trasmette al suo interlocutore il "numero mostro" $M = (J_1)^{a_1}(J_2)^{a_2} \cdots (J_k)^{a_k}$ (in forma non fattorizzata).	Si
6) Bob sa che M si scompone soltanto negli m numeri primi scelti da lui all'inizio. Ció gli consente in breve tempo di fattorizzare $M = P_1^{H_1} P_2^{H_2} \cdots P_m^{H_m}$. Bob risolve il sistema lineare scritto in basso nelle incognite $\alpha_1, \alpha_2, \ldots, \alpha_m$ $(\alpha_1, \alpha_2, \ldots, \alpha_m) \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1m} \\ v_{21} & v_{22} & \cdots & v_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mm} \end{pmatrix} = (H_1, H_2, \ldots, H_m)$ Eliminando i termini nulli dalla sequenza $\alpha_1, \alpha_2, \ldots, \alpha_m$, Bob ricava il messaggio di Alice.	No

Per mancanza di tempo, il laboratorio relativo a questo protocollo (con comunicazioni svolte tra studenti e contestuali tentativi di infrangere il codice, tutti effettuati con l'ausilio di piccoli programmi scritti dall'insegnante), é stato molto breve e non ha permesso un'analisi profonda del meccanismo da parte della classe. É comunque rimarchevole sottolineare la ricchezza tematica di questo laboratorio e specialmente del meccanismo inventato: in esso sono confluiti un tema squisitamente aritmetico di prima superiore (la scomposizione in fattori primi) e uno degli argomenti principali di Algebra della classe seconda, la risoluzione dei sistemi lineari (con particolare attenzione alla questione della dipendenza lineare). La necessitá di scrivere un programma in Python che permettesse di fattorizzare interi "pescando" da un insieme prefissato di primi, é un'opportunitá didattica che non é stata colta per mancanza di tempo: una pianificazione di piú ampio respiro puó senz'altro prevedere un'ultima fase dedicata al coding (l'algoritmo necessario al calcolo é di facile implementazione).

4. Osservazioni finali

Questo percorso laboratoriale di Crittografia Moderna, ha permesso alle ragazze e ai ragazzi che hanno partecipato di fare “Matematica sulla Matematica" e, a tratti, “Matematica contro la Matematica", cioé di utilizzare in chiave costruttiva alcuni limiti di calcolo noti ai ragazzi. Questo percorso ha stimolato la creativitá degli studenti ed ha permesso loro di rileggere le competenze e le conoscenze acquisite a scuola in una veste nuova: le domande “cosa so fare?" e “cosa non so fare?" si sono quindi riunite in un’unica competenza di livello superiore, gettando le basi per uno sviluppo tematico ricco e profondo. Alla fine del percorso gli studenti si sono sentiti “professionisti della Matematica", il che ha avuto un effetto motivazionale di evidente valore: a questo livello scolastico, soltanto la Crittografia offre queste possibilitá didattiche.

Alexander Saltuari,
Responsabile del progetto LICEO MATEMATICO,
LICEO STATALE “ETTORE MAJORANA"
via C. Avolio, 111 – 00128 Roma
e-mail: alexander.saltuari@liceomajorana.edu.it

Lavoro pervenuto in redazione il 15.04.2022.