Università degli Studi di Pisa

CORSO DI PERFEZIONAMENTO

"Strategie didattiche per promuovere un atteggiamento positivo verso la matematica e la fisica"

RELAZIONE DI TIROCINIO:

Laboratorio di crittografia

Giancarlo Ragucci

PREMESSA

Durante l'anno scolastico 2006/2007, all'interno del Progetto Lauree Scientifiche, ho collaborato col prof. Orazio Puglisi del dipartimento di matematica di Firenze alla progettazione e realizzazione del Laboratorio di Crittografia. Tale laboratorio è stato proposto alle scuole superiori dell'area fiorentina come una delle possibili attività offerte dal dipartimento. Le altre, consultabili seguendo il link corrispondente al progetto sulla pagina www.math.unifi.it sono:

- Laboratorio di probabilità
- Macchine che imparano da sole – Introduzione agli automi cellulari
- WIMS – Il server di matematica interattiva
- L'algebra della carta piegata – I legami tra algebra, geometria e origami
- Riga e compasso e algebra – Illustrazione dei legami tra costruzioni geometriche e metodi algebrici
- Geometrie non euclidee
- Il minimo e il massimo – Introduzione elementare ai problemi isoperimetrici

Io ho curato, fino ad oggi, quattro serie di incontri, presso:

- ITIS "Antonio Meucci" (Firenze)
- Liceo Scientifico "Niccolò Copernico" (Prato) – 2 serie di incontri
- Istituto "I. Newton – B. Russell" (Scandicci, Fi)

La partecipazione da parte degli studenti ai cinque incontri di cui era composto ogni laboratorio era facoltativa e, almeno per quel che riguarda le attività che ho svolto io, ha coinvolto alunni di classi diverse: in genere quarte e quinte. Per quanto possibile abbiamo cercato di mantenere una cadenza settimanale, con incontri di due ore ciascuno, in modo da avere da un lato una certa continuità ed evitare dall'altro che l'attività avesse un'incidenza eccessiva sul normale impegno

scolastico e non dei ragazzi. Nella stessa ottica ho cercato di non caricare di altro lavoro gli studenti: tutto (o quasi) è stato svolto nell'arco delle due ore di ogni incontro.

Aggiungo che, avendo sempre avuto una parte attiva durante gli incontri, le osservazioni che ho potuto fare sono decisamente ridotte rispetto a quelle che sarebbero state possibili se avessi assistito come "pubblico"; perciò, in quel che segue, devo limitarmi ad una relazione su quel che si è fatto e su quelle che sono le esigenze dei ragazzi che *credo* di aver avvertito. Manca, dunque, una visione dall'"esterno", forse più critica e completa di quella che ho avuto io.

> Un'avvertenza "tipografica": i paragrafi con margini maggiori (come questo) e carattere corsivo riportano frammenti di discussioni o spiegazioni fatte durante gli incontri.

Obiettivi generali

Per poter parlare, successivamente, della struttura che si è deciso di dare al laboratorio è d'obbligo, mi pare, partire da una breve descrizione dell'obiettivo che ci eravamo prefissi e che, certamente, non era quello di fornire conoscenze approfondite sulla crittografia moderna. L'idea principale, anzi, era quella di lasciare che da un'iniziale discussione corale emergessero come necessarie certe caratteristiche che un sistema di cifratura realmente utilizzabile deve o dovrebbe avere. Quindi tali idee sarebbero state tradotte in una collezione minima di richieste e formalizzate nella descrizione di un generico protocollo crittografico. Ma non si può parlare di crittografia senza parlare, almeno un po', di crittoanalisi. E così, man mano che il lavoro fosse proceduto, sarebbero state messe in evidenza alcune debolezze dei primi, ingenui sistemi crittografici. La nostra idea è che così facendo sarebbe emersa l'esigenza di ancorare un ideale protocollo a qualcosa, qualche problema difficilmente "aggirabile": il primo facilmente discutibile mi è parso il One Time Pad (con la generazione pseudocasuale della chiave); quindi sarebbero stati proposti alcuni semplici esempi di cifratura a chiave pubblica.
Vediamo quindi cosa è stato effettivamente realizzato.

Premessa al Primo incontro

Prima di cominciare l'attività, ogni volta, ho avuto un incontro preliminare con gli insegnanti che avrebbero fatto da tramite e seguito con gli alunni l'intero percorso. Dopo aver ascoltato le loro eventuali richieste o proposte, ho concordato un programma di massima sul modo di procedere. In realtà, alla resa dei conti, i laboratori si sono assomigliati molto e in ogni caso sono iniziati con un lavoro svolto dagli alunni. La consegna era di produrre, eventualmente in piccoli gruppi, un sistema di cifratura originale e descriverne per iscritto il funzionamento. Quindi uno o due giorni prima del primo incontro mi avrebbero fatto avere questo materiale.

Agli insegnanti ho chiesto di non dare alcuna spiegazione ulteriore: qualunque cosa gli allievi avessero prodotto sarebbe stato il nostro punto di partenza.

Devo dire che alcuni degli elaborati che ho ricevuto mi hanno decisamente sorpreso. La grande maggioranza, come mi aspettavo, consisteva in cifrature monoalfabetiche: qualcuno aveva sostituito ad ogni lettera del messaggio "in chiaro" un'altra lettera; altri avevano pensato ad altre associazioni:

- ad ogni lettera un numero (qualcuno già lavorando con i resti delle divisioni per 21 o 26)
- ad ogni lettera una funzione
- ad ogni lettera una coppia di lettere oppure una lettera o un numero
- ad ogni lettera un numero e poi ad ogni numero la sua immagine tramite una qualche funzione, più o meno complicata
- in un caso è stato proposto un protocollo steganografico: un messaggio immerso in un altro, innocuo, e una chiave di lettura consistente in istruzioni che spiegassero quali lettere leggere e quali saltare.
- Vari lavori erano evoluzioni del monoalfabetico in un sistema di tipo Vigenere. E in questo caso l'associazione lettera-numero è stata quella maggiormente usata.
- Infine due ragazzi in laboratori distinti hanno proposto il One Time Pad: uno dei due ne era palesemente a conoscenza per aver letto qualcosa a riguardo da qualche parte (credo *Codici e Segreti,* di Simon Singh). L'altro sembrava esserci arrivato autonomamente.

PRIMO INCONTRO

Dopo una breve presentazione, ho detto ai ragazzi che avremmo passato subito in rassegna i loro lavori. Anzi, lo avrebbero fatto loro. Nella prima fase mi sono limitato a chiedere chi volesse iniziare, invitando i primi volontari alla lavagna; in realtà, a dispetto dell'apparenza, cercavo di seguire un certo ordine in base al sistema ideato; dunque iniziando da qualcuno che avesse proposto il monoalfabetico.

Man mano che ciascuno descriveva il proprio sistema cercavo di stimolare gli altri a cercarne i difetti: il pubblico, in altre parole, avrebbe dovuto far la parte del "cattivo", di colui che vuol scassinare il sistema. Dunque le mie domande:

> *vi sembra efficace? Affidereste i vostri segreti (o il codice del bancomat) a questo sistema? Cosa accadrebbe se…? Come faccio a tornare indietro ritrovando il messaggio di partenza?*

Poi passavamo in rassegna un altro sistema e, oltre a domande simili alle precedenti iniziava ad insinuarsene qualcuna del tipo

> *questo sistema è più o meno "sicuro" del precedente? Hanno qualcosa in comune o sono essenzialmente diversi?*

Pian piano, con qualche stimolo da parte mia, si iniziava a riconoscere prima una certa analogia tra alcuni sistemi e poi una loro reale sovrapponibilità: i ragazzi cominciavano a rendersi conto che, benché avessero usato nomi diversi, molti di loro avevano prodotto esattamente lo stesso sistema. A questo punto si rendeva necessario identificare le caratteristiche del sistema che soggiaceva a tutti quelli presentati, indipendentemente dalla particolare realizzazione. Volevo però che le indicazioni venissero da loro. Dopo una breve discussione, in genere, si conveniva che, benché ognuno potesse essere eletto a sistema "tipo", quello in cui ad ogni lettera si faceva corrispondere un numero e poi su questo si eseguiva l'operazione desiderata, era in fin dei conti il più "semplice" da descrivere e, soprattutto, da modificare.

Prima di passare oltre si rendeva necessario analizzare la "sicurezza" del protocollo: in parte lo avevamo fatto durante le esposizioni ma era necessario mettere una parola definitiva sulla questione.

> *Prendete un testo scritto in italiano: senza leggerlo, immaginate di trovare più lettere "e" o lettere "q"?*

Da qui una rapida discussione e la decisione che, forse, un'analisi delle frequenze avrebbe potuto, se non scardinare, almeno indebolire il protocollo. Quindi proseguivamo:

> *al di là di quello specifico che abbiamo trovato, quali caratteristiche pensate debba avere un protocollo affinché, quanto meno, possa funzionare?*

Per uno dei gruppi il passaggio a questo secondo stadio del lavoro è stato semplificato dal lavoro di due ragazze; avevano proposto il seguente sistema:

> *Ad ogni lettera dell'alfabeto si associ un numero da 1 a 26 e si converta così il messaggio in una sequenza di numeri; per leggibilità e comodità nella fase successiva, ogni numero va scritto aggiungendo davanti uno o due zeri in modo che, alla fine, ciascuno risulti scritto con tre cifre: quindi se A diventa 001 allora Z diventa 026.*
>
> *La cifratura avviene applicando a ciascun numero la funzione:* $f(x)= x^2 + 3x - 1$ *e poi scrivendo il risultato ancora con tre cifre.*

Mancavano, in effetti, le istruzioni per la fase di decifratura. Chiesi a tutti di pensarci e quando l'avessero trovata indicare agli altri la procedura corretta. Ben presto si resero conto dell'esistenza di una difficoltà, arrivando da soli a riconoscere nell'*iniettività* una caratteristica irrinunciabile di ogni funzione cifrante. A questo punto i ragazzi si convincevano del fatto che per far crittografia si deve usare una funzione iniettiva.

Il passo successivo consisteva nell'analizzare Vigenere. In ogni laboratorio ho trovato almeno una persona che lo aveva sfruttato, magari senza saperlo, nel proprio metodo e dunque siamo partiti dalla sua descrizione. Uno dei lavori tipici era presentato grosso modo così:

> *Ad ogni lettera si faccia corrispondere, ordinatamente, un naturale da 1 a 26. Si prenda come chiave una qualunque sequenza di numeri; ad esempio:* **3,17,9,21**.

Supponiamo, poi, che le prime lettere del messaggio corrispondano alla sequenza: 7, 1,19,19,5,20,16,5…

La cifratura avviene nel modo seguente:

- *la prima lettera del messaggio cifrato è quella che corrisponde a 7 +* **3***=10;*
- *la seconda è quella che corrisponde a: 1 +* **17***=20;*
- *la terza è quella che corrisponde a: 19 +* **9***=28; però 28>26. In questo caso la lettera è quella che corrisponde a 28-26=2;*
- *la quarta è quella che corrisponde a: 19 +* **21***=40; come prima si fa corrispondere a 40-26=14;*
- *per la quinta si ricomincia daccapo.*

Con un sistema di questo tipo è facile osservare, e *facevo osservare*, due cose apparentemente antipatiche:

- *che due lettere distinte possono essere cifrate nello stesso modo* (cade l'iniettività?)
- *che alla stessa lettera del messaggio in chiaro possono corrispondere due cifratura diverse* (non è più neanche una funzione?)

Eppure, soprattutto ma non esclusivamente, chi aveva proposto il sistema era pronto a giurare che la fase di decifratura si poteva fare ed era sicuramente non ambigua. Qui spostavo l'attenzione dei ragazzi su una questione apparentemente banale ma lasciata nell'ombra:

esattamente, cosa stiamo cifrando? Su chi agisce una funzione di cifratura?

Per non soffrire dei dubbi che ci poneva il nuovo sistema di norma tornavamo al monoalfabetico e analizzavamo lì la situazione. In breve e senza sorprese si osservava che, lì, quel che veniva cifrato era una lettera alla volta:

a parità di sistema usato, le prime lettere delle due frasi "oggi è giovedì" e "oggi è una bella giornata" vengono sempre, inevitabilmente cifrate nello stesso modo, ovunque si trovino nel testo.

Fatto ciò, senza troppi intoppi, si arrivava a identificare il baco apparente del sistema di Vigenere nel fatto che *noi* non avevamo ben individuato quale fosse l'unità di cifratura in quel caso: non una sola lettera ma un numero di lettere pari alla lunghezza della chiave.

Dunque in questo caso non è più vero che "oggi è giovedì" e "oggi è una bella giornata" vengono sempre cifrate nello stesso modo: dipende dalla posizione occupata nel testo.

Devo notare che, benché sugli appunti che ho scritto per i ragazzi, ho cercato di rispettare un certo formalismo, nelle chiacchierate in aula ho sempre affidato certe questioni ad immagini e a gesticolazioni. Il motivo era che non volevo appesantire gli incontri: nella stessa ottica non era richiesto (né vietato), per esempio, che prendessero appunti.

Quindi ci limitavamo ad osservare che, semplicemente, cambia l'insieme su cui si lavora, non il metodo.

Certo, qui l'analisi delle frequenze sembra molto più complicata, però, forse…

E se volessimo metterci definitivamente al riparo da tale analisi?

Da Vigenere il passo al One Time Pad era breve. Ho proposto il protocollo nella versione di Vernam:

La chiave è una sequenza di bit, lunga almeno come il messaggio

La cifratura avviene facendo la somma modulo 2 senza riporto (o, come in genere si dice, facendo lo Xoring) fra chiave e messaggio

La decifratura, facendo lo Xoring tra messaggio cifrato e chiave:

Una volta presentata l'idea con un esempio, proponevo una formalizzazione introducendo un operatore binario per lo Xoring, $\oplus$.

Dunque, se $\boldsymbol{m}$ *è il messaggio in chiaro,* $\boldsymbol{c}$ *quello cifrato e* $\boldsymbol{k}$ *la chiave, valgono:*

$\boldsymbol{c} = \boldsymbol{m} \oplus \boldsymbol{k}$ (cifratura)

$\boldsymbol{m} = \boldsymbol{c} \oplus \boldsymbol{k}$ (decifratura)

Ora, come risultato non dimostrato, avvertivo gli studenti che il One Time Pad è un sistema dotato di segretezza perfetta, ovviamente dandone loro la definizione. Lasciavo, però, che l'intuito e alcune gesticolazioni li convincessero che, forse, quanto affermavo poteva avere qualche fondo di verità.

Arrivati qui, in genere, erano esaurite le due ore di tempo. Giusto qualche minuto per discutere del problema fondamentale dello scambio delle chiavi fra mittente e destinatario:

Per usare il One Time Pad (che a questo punto sembra essere molto più sicuro dei precedenti) devo necessariamente dotare entrambi gli interlocutori della stessa chiave. Come faccio?

Poi mostravo il protocollo di Diffie ed Hellmann per un tale scambio, eseguito, però, con cassette, lucchetti e chiavi reali. Lasciavo come "compito" per casa quello di trovare un sistema per tradurre il protocollo in qualcosa di fruibile da un computer e poterlo così usare, ad esempio, su internet.

SECONDO INCONTRO

Il secondo incontro si apriva, quindi, riprendendo la discussione delle chiavi. In genere qualcuno era sempre in grado di fornire la soluzione, usando, appunto, il One Time Pad. Se così non succedeva, la indicavo io:

A vuole inviare la chiave K a B. Costruisce una sequenza di bit, S_A*. Analogamente B costruisce la sua sequenza,* S_B *Quindi:*

A invia $C_A = K + S_A$ *(A mette il lucchetto)*

B riceve C_A *e invia* $C_{A,B} = C_A + S_B$ *(B mette il lucchetto)*

A riceve $C_{A,B}$ *invia* $C_B = C_{A,B,A} = C_{A,B} + S_A$ *(A toglie il lucchetto)*

B riceve C_B *e ottiene K, da:* $K = C_B + S_B$ *(B toglie il lucchetto)*

Quindi una provocazione:

> *visto che l'OTP ha segretezza perfetta, anziché usarlo per lo scambio di una chiave, perché non lo usiamo per inviare direttamente il messaggio desiderato usando il protocollo precedente?*

Quindi il terzo stadio del nostro percorso:

> *Cosa dobbiamo ammettere che conosca un eventuale "curioso"? È legittimo pensare che,* almeno*, possa vedere i messaggi* (*cifrati*) *che sono passati sul canale pubblico!*

Con poco sforzo i ragazzi pervenivano al risultato inatteso: conoscendo C_A ,$C_{A,B}$ e C_B si può risalire in modo immediato al messaggio e alle due chiavi usate dagli interlocutori.

Qui c'era lo spazio per definire una volta per tutte quale sia l'assunto di base dal quale si parte a far crittografia:

> *Del metodo usato dobbiamo sempre far conto che chiunque conosca tutti i dettagli; tutti a meno di uno o più parametri che non devono mai essere comunicati a terzi e che, in qualche modo, garantiranno la sicurezza del sistema.*

Il resto dell'incontro era destinato alle verifiche: in aula computer i ragazzi si sono cimentati nella rottura di sistemi monoalfabetici (con un software che avevo scritto per l'occasione) e di quello di Vigenere (in questo caso usando un applet disponibile su internet all'indirizzo: http://www.math.ucsd.edu/~crypto/programs.html).

TERZO INCONTRO

Se nei primi due incontri avevo cercato di suggerire o, meglio, *lasciar emergere* alcune semplici idee di base per la crittografia limitando l'analisi a metodi "storici", dal terzo incontro in poi volevo gettar le basi per arrivare ai metodi e a qualche risultato relativamente recenti. Dunque

> *lo scenario complessivo cambia: il computer entra di diritto in gioco ed oggi non ha praticamente senso pensare a crittosistemi che non ne prevedano l'uso in modo estensivo. Aumenta, dunque, la capacità di calcolo di chi vuole cifrare ma parallelamente aumenta anche la capacità di calcolo di chi vuole infrangere il sistema. Dunque se ci accordiamo sul fatto che vogliamo usare funzioni invertibili e che dobbiamo ammettere che tutte le informazioni, eccetto i parametri che costituiscono la chiave, possano essere noti a terze parti, dobbiamo metterci al riparo, quanto meno, da un potenziale attacco a "forza bruta" perpetrato per mezzo di un calcolatore.*

Nell'incontro precedente avevano, di fatto, rotto alcuni sistemi proprio col computer…

> *Ma cosa riesce a calcolare un computer in tempi "ragionevoli"?*

Con questo genere di approccio passavo ad un quarto stadio: discutere, sommariamente, della complessità di algoritmi distinguendoli in polinomiali ed esponenziali; ciò, ovviamente, dopo aver mostrato con esempi numerici (e una suggestiva immagine sullo spessore ottenibile dal piegar un foglio di carta successivamente per 51 volte) quale fosse la differenza sostanziale di un algoritmo di un tipo ed uno dell'altro. Ne seguiva un accordo essenzialmente unanime nel chiamar "veloci" i primi e "lenti" i secondi. Quindi fornivo i canonici esempi elementari di algoritmi polinomiali: addizione, sottrazione, moltiplicazione e divisione. E alcuni degli altrettanto canonici esempi di algoritmi di cui non si conosce (se esiste) una versione polinomiale: fattorizzazione, problema dello zaino, colorabilità di grafi ecc.

Ciò fatto, un po' per tener viva l'attenzione dando ai ragazzi qualcosa di familiare e un po' per usarlo successivamente come chiusura della chiacchierata sull'algoritmo euclideo per la ricerca del massimo comun divisore, proponevo una domanda "fuori luogo":

la retta di equazione 333 x + 156 y = 2 contiene punti a coordinate intere?

Quindi, dopo aver lasciato qualche minuto per rifletterci, invitavo ad accantonare per un po' la questione: ci saremmo tornati. Spiegando che ci sarebbe servito nel seguito, introducevo a questo punto il problema della determinazione del massimo comun divisore di due numeri. Anzitutto lasciavo che fossero loro a proporre un approccio. Dopo aver osservato insieme che l'algoritmo che loro avevano in mente (passando dalla scomposizione in fattori) era uno di quelli "lenti" e "improponibili", introducevo quello di Euclide. In genere premettendo la versione geometrica, passando dalla commensurabilità di segmenti, e poi seguendo con quella algebrica. Ovviamente qui si rendeva necessario introdurre qualche definizione e qualche lemma. Le dimostrazioni dei vari enunciati venivano eseguite dagli alunni, alla lavagna. A ciò seguiva qualche vago cenno al calcolo della complessità dell'algoritmo, scoprendo che è di tipo polinomiale.

Uno dei risultati che ci era servito e che avevamo dimostrato era, chiaramente, il seguente:

se **x** *divide* **a** *e* **x** *divide* **b** *allora* **x** *divide ogni combinazione lineare di* **a** *e* **b**

Con questo risultato, giusto per chiudere i cerchio, tornavamo al problema proposto in precedenza, con la soluzione, negativa.

E se invece avessimo 333 x + 156 y = 3 ? Come potremmo fare a trovare le coordinate (*intere*) *di un punto che appartiene alla retta?*

Mostrato che lo stesso algoritmo fornisce anche questo risultato, chiudevamo l'incontro. Prima, però, lasciavo un piccolo gioco da risolvere:

Scrivete un numero "grande" quanto volete. Sottraete da questo la somma delle sue cifre. Del risultato ottenuto, calcolate la somma di tutte le cifre tranne una*, scelta a caso: ditemi il risultato e vi dirò quale cifra avete trascurato.*

Quindi, dopo aver mostrato qualche volta che la cosa funziona, lasciavo come "compito per casa" quello di scoprire il "trucco" e spiegarmelo la volta successiva.

La curiosità di conoscere il risultato del gioco assegnato veniva soddisfatta come prima cosa. Se nessuno era riuscito a comprenderne il funzionamento, cominciavo dal ricordare il significato della scrittura posizionale:

con la scrittura **abc** (*lavorando in base* 10) *intendo:* $\mathbf{abc} = \mathbf{a}*10^2+\mathbf{b}*10^1+\mathbf{c}*10^0$

benché questa fosse immancabilmente una cosa ovvia per tutti, ben pochi avevano pensato di usarla. Fatto ciò, invitavo qualcuno a completare il lavoro e ben presto ci riducevamo alla seguente fatto:

il risultato della sottrazione è sempre un numero divisibile per 9. Una regola che conosciamo bene ci dice che un numero è divisibile per 9 se e solo se lo è la somma delle sue cifre.

Da qui il gioco era completamente chiarito. Rimaneva però un problema:

perché funziona quella regola di divisibilità?

Ancora si rendeva necessario dimostrare qualcosa e ancora erano invitati a farlo i ragazzi. Una volta che fosse stato chiarito tale perché, procedevo ad una maggior formalizzazione e un allargamento di orizzonti: introducevo prima la notazione e poi, via via, alcuni semplici risultati sull'aritmetica modulare. In particolare dimostravamo insieme ai ragazzi che:

- se $\mathbf{a} \equiv \mathbf{b} \bmod \mathbf{n}$ e $\mathbf{c} \equiv \mathbf{d} \bmod \mathbf{n}$ allora: $\mathbf{a} \pm \mathbf{c} \equiv \mathbf{b} \pm \mathbf{d} \bmod \mathbf{n}$ e $\mathbf{a} * \mathbf{c} \equiv \mathbf{b} * \mathbf{d} \bmod \mathbf{n}$
- esiste $\mathbf{z}$ intero tale che $\mathbf{a} * \mathbf{z} \equiv 1 \bmod n$ se e solo se $(\mathbf{a}, \mathbf{n}) = 1$

Benché descritto in poche righe, questo lavoro toglieva un tempo abbastanza consistente e, arrivati a completare le ultime dimostrazioni, rimaneva in genere poco più di mezz'ora alla fine dell'incontro. Quello che, però, succedeva, era un certo disorientamento generale:

perché stiamo facendo queste cose? Dov'è la crittografia?

La domanda era perfettamente legittima e, benché mi interessasse proporre (e magari dimostrare) il piccolo teorema di Fermat, convenivo con loro che era necessario riagganciarsi al tema principale. Gli elementari strumenti che ci eravamo procurati erano comunque sufficienti ad illustrare il protocollo a chiave pubblica di Merkle-Hellmann, basato sul problema dello zaino. Dunque, il "ritorno" alla crittografia passava dall'illustrare il nuovo tipo di approccio:

Fino a questo momento i sistemi che abbiamo incontrato sono caratterizzati dall'essere "simmetrici": se so cifrare un messaggio allora lo so anche decifrare. Un sistema si dice a chiave pubblica se il fatto di essere capace di cifrare un messaggio non implica, necessariamente, di essere in grado di decifrarlo.

Quindi, con l'uso di qualche disegno e schematizzazione, spiegavo meglio quale fosse l'obiettivo. Ora eravamo pronti a parlare del protocollo summenzionato. Ricordavo quindi, brevemente, in cosa consistesse il problema dello zaino (era uno degli esempi proposti di

problemi per cui non si conosce algoritmo polinomiale) e mostravo come usarlo per ottenere un sistema di cifratura a chiave pubblica.

QUINTO INCONTRO

L'ultimo incontro era dedicato al protocollo di Diffie-Hellmann per lo scambio di chiavi e ad RSA. Dopo aver analizzato, dal punto di vista computazionale, la questione dell'elevamento a potenza, concentravamo l'attenzione sul piccolo teorema di Fermat e quello di Eulero-Fermat. Non vi sono, mi pare, cose particolari da riportare riguardo questo incontro: si trattava di dar ulteriore corpo e sostanza all'idea di cifratura asimmetrica, mostrando e sottolineando come la crittografia moderna "certifichi" la sicurezza di un metodo sulla base della (supposta) intrattabilità computazionale di certi problemi; dunque l'attenzione era rivolta a questi: fattorizzazione per RSA e logaritmo discreto per entrambi.

OSSERVAZIONI

La pianificazione dell'attività è stata completata, essenzialmente, prima del primo incontro dell'anno. Durante lo svolgimento dei vari laboratori mi sono reso conto di alcune mancanze a cui, in corsa, mi è stato e mi è tutt'ora difficile porre rimedio. Ritengo che la difficoltà principale nasca dal tipo di argomento trattato: tolte le prime due lezioni nelle quali è molto facile proporre una vera attività laboratoriale, nelle successive, in cui cercavo di fornir le basi per introdurre alcuni metodi moderni, è stato effettivamente difficile mettere gli studenti nelle stesse condizioni di lavoro iniziali. D'altra parte l'argomento non si presta alla risoluzione di veri e propri esercizi: anzi, gli strumenti usati sono talmente "di base" che l'unico esercizio possibile mi sembrava proprio quello di stimolare a trovare dimostrazioni su certi "perché". Probabilmente un uso più continuativo del computer avrebbe dato l'idea di una maggior dose di partecipazione "costruttiva"; tuttavia, secondo me, avrebbe anche svilito parzialmente la natura "matematica" dell'iniziativa. D'altra parte, in base anche alle schede di valutazione che ho raccolto, vi è stata in genere un'accoglienza benevola dell'attività: qualcuno, forse, si aspettava qualcosa di diverso, immagino, più "applicativo". Su questo, magari, porre rimedio è più semplice: quello che quest'anno ho tralasciato di fare ma che non dimenticherei quando si dovesse ripetere l'esperienza è, semplicemente, un incontro preventivo che sia ad uso "valutativo" per i ragazzi: non più iscrizioni ad un corso a scatola chiusa, con aspettative vaghe, ma partecipazione con cognizione di cosa, grosso modo, verrà fatto.