Periodico di Matematiche – Serie VIII – Volume 1- Numero 1 – gennaio-marzo 2001

La crittografia a chiave pubblica per giocare e imparare: il gioco del codice RSA (parte prima)

Franco Eugeni, Raffaele Mascella, Daniela Tondini*

Premessa.

Tra i saperi di interesse per tutte le età scolari gioca un ruolo affascinante quella parte della matematica che si lega con le tecniche di protezione dell'informazione. Accanto alla crittografia classica, che ha forti potenzialità interdisciplinari ed è un'ottima palestra mentale per esercitare e sviluppare le capacità logico-deduttive, è possibile pensare all'insegnamento delle tecniche più recenti: queste, se adeguatamente semplificate, offrono esempi notevoli di applicazioni della matematica. Così, nell'uso del codice RSA, inventato da Rivest, Shamir ed Adleman nel 1977, si fa uso della funzione di Eulero, di numeri primi molto grandi e di aritmetica modulare. E' possibile utilizzare il grande impatto di modernità e popolarità che riscuotono queste problematiche per aiutare gli allievi anche molto giovani ad apprendere queste parti della cultura matematica? Gli autori propongono un gioco che, ben presentato da un insegnante esperto, dovrebbe essere la "chiave" per "decrittare" questi interessanti concetti. Nel gioco, che è da fare adoperando al più una comune calcolatrice, non sono usati primi grandi, al contrario di quanto avviene nella realtà. Sarà la sensibilità dell'insegnante a trovare poi, come sempre, la giusta via. In una fase successiva, quando lo studente sarà in grado di usare un computer, potrà operare con un codice RSA della giusta dimensione computazionale, ma sarà pronto a farlo e ne capirà tutte le esigenze. Per il futuro vorremmo progettare una sperimentazione in vari tipi di classi proponendo una descrizione del gioco adattata ai vari livelli e un software didattico molto elementare che ne faciliti le implementazioni.

La versione che presentiamo ora è preparata per il docente. La versione da presentare in una seconda o terza media non è molto

* Università di Teramo, Dipartimento di Metodi per l'Economia ed il Territorio.

dissimile ma è più lunga avendo sia adattato il linguaggio sia aumentato di molto il numero di esempi ed esercizi.

1. Preparazione del gioco.

Organizziamo gli studenti in tre gruppi, ciascuno dei quali prende il nome dal suo capogruppo. Nel nostro esempio saranno: Anna, Barbara, Carlo. Ogni gruppo sceglie due numeri primi, diciamo di due cifre, e ne calcola il prodotto. Ogni capogruppo scrive alla lavagna, accanto al proprio nome, il valore del prodotto. I due numeri primi, invece, rimangono segreti.
Ogni studente calcola il valore di Eulero del prodotto dei due primi scelti, calcolo che nella fattispecie risulta elementare, essendo:

$$\phi(p \cdot q) = (p - 1) \cdot (q - 1)$$

Così, per la scelta fatta dai tre gruppi, si ottengono:

$\phi_A = \phi(13 \cdot 23) = 264$; $\phi_B = \phi(11 \cdot 41) = 400$; $\phi_C = \phi(17 \cdot 31) = 480$.

Questo primo passo non è difficile presentando solo il calcolo da fare nel suo elementare svolgimento.
Il secondo stadio è decisamente più difficile. Se il gruppo ha fissato come prodotto di primi il naturale n, dovrebbe individuare due numeri naturali d, e che siano l'uno inverso dell'altro rispetto al modulo $\phi(n)$:

$$d \cdot e \equiv 1 \pmod{\phi(n)}$$

Dunque Anna, Barbara e Carlo calcolano d ed e, in modo che siano congruenti ad 1 modulo, rispettivamente, ϕ_A, ϕ_B e ϕ_C. Per far ciò ogni gruppo, ad esempio Anna, deve prendere un multiplo del numero ϕ_A, aumentarlo di uno $(1 + k\phi_A)$ e trovarne due fattori complementari:

Anna:	$\phi_A = 264$,	$1 + \phi_A = 265 = 5 \cdot 53$,	d = 5, e = 53
Barbara:	$\phi_B = 400$,	$1 + 2\phi_B = 801 = 9 \cdot 89$,	d = 9, e = 89
Carlo:	$\phi_C = 480$,	$1 + \phi_C = 481 = 13 \cdot 37$,	d = 13, e = 37

Le coppie (d, n) ed (e, n) vengono denominate rispettivamente *chiave pubblica* e *chiave privata*. I numeri d_A, d_B, d_C si riportano alla lavagna accanto ai valori-prodotto, mentre i numeri e_A, e_B, e_C, rimangono segreti. Il codice di trasmissione è a questo punto definito.
Sul canale pubblico/lavagna e nella parte segreta vi saranno così i seguenti dati:

Lavagna

Gruppo	*Prodotto*	*Chiave d*
Anna	299	5
Barbara	451	9
Carlo	527	13

Parte segreta

Gruppo	*Nr di Eulero*	*1° fattore*	*2° fattore*	*Chiave e*
Anna	264	13	23	53
Barbara	400	11	41	89
Carlo	480	17	31	27

2. Come effettuare firma, cifratura e decifratura.

2.1. Trasformazione del messaggio da letterale a numerico.

Ogni gruppo, in segreto, sceglie una parola che va a codificare con una semplice sostituzione numerica. Ad ogni lettera dell'alfabeto si associa un numero di tre cifre dato dalla tabella seguente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
001	002	003	004	005	006	007	008	009	010	011	012	013	014

O	P	Q	R	S	T	U	V	W	X	Y	Z	spazio
015	016	017	018	019	020	021	022	023	024	025	026	027

Ad esempio Anna sceglie la parola "ROBIN". Questa diventa: "018 015 002 009 014".

Le parole sono così pronte per essere "trattate" numericamente.

2.2. Firma numerica del messaggio.

Anna prende il suo messaggio "018015002009014", e lo divide in gruppi di tre cifre[1], in pratica i gruppi corrispondenti ad ogni lettera, poi effettua di ciascuno di questi un elevamento a potenza con esponente la sua chiave privata, che è il numero 53, calcolandone il modulo rispetto al numero-prodotto riportato alla lavagna, cioè 299. Le operazioni di elevamento a potenza vanno cioè fatte tenendo conto che si lavora in aritmetica modulare.

Anna per firmare "018" con la sua chiave privata 53 deve calcolare 18^{53} a meno di multipli di 299, ma poichè $18^2 = 324 = 299 + 25$ il trucco consiste nel mettere 25 al posto di 18^2:

$$18^{53} \equiv 18 \cdot 18^{52} \equiv 18 \cdot (18^2)^{26} \equiv 18 \cdot (25)^{26}$$

[1] La contemporanea sostituzione numerica e divisione del messaggio in gruppi di tre cifre non è crittograficamente adeguata ma inizialmente è molto semplificativa.

Così anche $25^2 = 625 = 2 \cdot 299 + 27$ per cui

$$18 \cdot 25^{26} \equiv 18 \cdot (25^2)^{13} \equiv 18 \cdot 27^{13}$$

e procedendo in modo analogo si ottengono in sequenza:

$$18 \cdot 27^{13} \equiv (18 \cdot 27) \cdot (27^2)^6 \equiv 187 \cdot 131^6 \equiv 187 \cdot (131^2)^3 \equiv$$
$$\equiv 187 \cdot 118^3 \equiv (187 \cdot 118) \cdot 118^2 \equiv 239 \cdot 170 \equiv 265.$$

Dunque il termine "018" si firma trasformandolo in "265".
Così per firmare "015" con la sua chiave privata 53 occorre calcolare 15^{53} a meno di multipli di 299:

$$15^{53} \equiv 15 \cdot 15^{52} \equiv 15 \cdot (15^2)^{26} \equiv 15 \cdot 225^{26} \equiv 15 \cdot (50625)^{13} \equiv 15 \cdot 94^{13} \equiv$$
$$\equiv 15 \cdot 94^{13} \equiv (15 \cdot 94) \cdot (94^2)^6 \equiv 214 \cdot 165^6 \equiv 214 \cdot (27225)^3 \equiv$$
$$\equiv 214 \cdot 16^3 \equiv (214 \cdot 16) \cdot (16^2) \equiv 135 \cdot 256 \equiv 34560 \equiv 175$$

Dunque la firma del termine "015" avviene attraverso "175".
Proseguendo nei calcoli:

"002" $\rightarrow 2^{53} \equiv 2 \cdot 2^{52} \equiv \ldots \ldots \ldots \equiv 6 \rightarrow$ "006"
"009" $\rightarrow 9^{53} \equiv 9 \cdot 9^{52} \equiv \ldots \ldots \ldots \equiv 94 \rightarrow$ "094"
"014" $\rightarrow 14^{53} \equiv 14 \cdot 14^{52} \equiv \ldots \ldots \ldots \equiv 274 \rightarrow$ "274"

In definitiva il messaggio di Anna, "ROBIN", viene tradotto e firmato nel messaggio numerico "265175006094274".

2.3. Verifica della firma.

Sia Barbara che Carlo possono verificare che il messaggio numerico è stato scritto da Anna e capire cosa significa. Per questo divideranno "265175006094274" in gruppi di tre cifre e calcoleranno le potenze prendendo come esponente la chiave pubblica di Anna, ovvero 5. Poi utilizzeranno la tabella di conversione numeri-lettere a ritroso, cioè sostituendo ai numeri le lettere ad essi corrispondenti. Nel dettaglio:

"265" $\rightarrow 265^5 \equiv 265 \cdot 265^4 \equiv \ldots \ldots \ldots \equiv 18 \rightarrow$ "018" $\rightarrow$ "R"
"175" $\rightarrow 175^5 \equiv 175 \cdot 175^4 \equiv \ldots \ldots \ldots \equiv 15 \rightarrow$ "015" $\rightarrow$ "O"
"006" $\rightarrow 6^5 \equiv 6 \cdot 6^4 \equiv 6 \cdot (6^2)^2 \equiv \ldots \ldots \ldots \equiv 2 \rightarrow$ "002" $\rightarrow$ "B"
"094" $\rightarrow 94^5 \equiv 94 \cdot 94^4 \equiv \ldots \ldots \ldots \equiv 9 \rightarrow$ "009" $\rightarrow$ "I"
"274" $\rightarrow 274^5 \equiv 274 \cdot 274^4 \equiv \ldots \ldots \ldots \equiv 14 \rightarrow$ "014" $\rightarrow$ "N"

Il messaggio "265175006094274" che Anna aveva mandato nel canale pubblico-lavagna viene così ricondotto alla parola di senso compiuto iniziale "ROBIN". Questa parola, attenzione, può essere stata codificata, cioè firmata numericamente, solo da Anna con la sua chiave segreta! Chiunque potrà leggerla e identificarne la provenienza.

2.4. Copertura del messaggio.

Se Anna vuole inviare un messaggio a Carlo nascondendo il contenuto a Barbara, procede così:

- Traduce "ROBIN" con la tabella ottenendo: "018015002009014"
- Divide il messaggio in gruppi di tre cifre e calcola le potenze dei numeri ottenuti 18, 15, 2, 9, 14 con esponente il numero pubblico $d = 13$ di Carlo, facendone il modulo secondo il prodotto pubblico di Carlo, che è 527.

Il messaggio ottenuto "392461287297090" viene inviato a Carlo attraverso un canale cui tutti possono accedere, e non c'è da temere che Barbara lo legga. Infatti per scoprire cosa c'è sotto bisogna conoscere la chiave segreta di cui solo Carlo è in possesso!

2.5. Decifratura del messaggio.

Quando Carlo riceve il messaggio a lui destinato, cifrato in modo da tenerlo segreto a tutti gli altri, procede nel modo seguente:

- Per ogni gruppo di tre cifre Carlo effettua la decifratura utilizzando come esponente il suo numero privato $e = 27$, e facendone il modulo secondo il suo prodotto 527.
- Ottenuta la sequenza numerica del messaggio, che a questo stadio corrisponderà a "018015002009014", utilizza la tabella di conversione per ottenere il messaggio nella forma originale "ROBIN".

3. Funzionamento del gioco.

3.1. Gioco de "Il messaggio segreto".

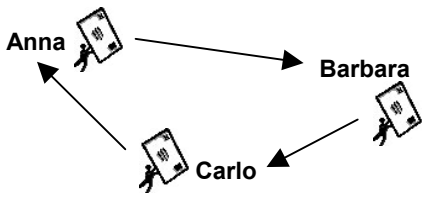
Ruoli: nella prima fase Anna, Barbara e Carlo sono tutti *mittenti*;
nella seconda fase Anna, Barbara e Carlo sono tutti *riceventi*.

Prima fase.

- Anna, Barbara e Carlo scelgono una parola di lunghezza fissata.
- Anna cifra la sua parola con la chiave pubblica di Barbara; Barbara cifra la sua parola con la chiave pubblica di Carlo; Carlo cifra la sua parola con la chiave pubblica di Anna.

Seconda fase.

- Anna da il suo messaggio cifrato a Barbara, così Barbara dà il suo messaggio a Carlo e Carlo il suo messaggio ad Anna.



- Anna decifra il messaggio di Carlo con la propria chiave privata, chiave che nessun altro conosce. Barbara decifra il messaggio di Anna con la propria chiave privata; Carlo decifra il messaggio di Barbara con la propria chiave privata.
- Anna, Barbara e Carlo capiscono cosa contiene il messaggio indirizzato a ciascuno di loro; le parole ottenute si possono scrivere alla lavagna così da confrontare se i messaggi corrispondono (anche per valutare eventuali errori).
- Vince il gioco chi per primo (senza commettere errori) indovina il contenuto del messaggio che ha ricevuto.

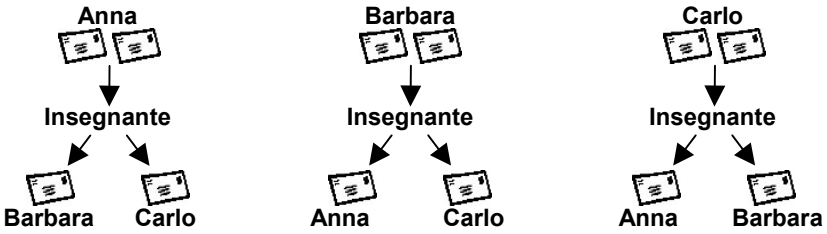
OSSERVAZIONI. *Una ulteriore fase del gioco può avvenire invertendo la consegna dei messaggi fra i tre gruppi. Cioè Anna può cifrare il messaggio con la chiave pubblica di Barbara ma consegnare il messaggio a Carlo, e così via. In fase di decifratura Anna, Barbara e Carlo non ottengono i messaggi originali capendo, così, che il messaggio indirizzato ad un gruppo non può essere letto da altri.*

3.3. Gioco del "Chi è l'autore?".

Ruoli: nella prima fase Anna, Barbara e Carlo sono tutti *mittenti*;
nella seconda fase Anna, Barbara e Carlo sono tutti *riceventi*.

- Anna, Barbara e Carlo scelgono una parola di lunghezza fissata.
- Anna cifra la sua parola con la propria chiave privata. Così scrive su un biglietto sia la parola scelta che la cifratura numerica ottenuta. Quindi fa una copia del biglietto.
- Barbara e Carlo eseguono le stesse operazioni, ciascuno con la propria chiave privata, facendo due copie di ciascun biglietto.
- I messaggi vengono consegnati all'insegnante che provvede a distribuirli ai gruppi nel seguente modo: ad Anna vanno un messaggio di Barbara ed uno di Carlo, a Barbara vanno un messaggio di Anna ed uno di Carlo, così a Carlo vanno un

messaggio di Anna ed uno di Barbara.



- Anna ora deve capire qual è il messaggio di Barbara e quale è di Carlo. Perciò deve decifrare i messaggi che ha ottenuto dagli altri due gruppi provando in entrambi i casi con entrambe le chiavi pubbliche di Barbara e Carlo, che sono scritte alla lavagna.
- Così Barbara e Carlo devono capire chi sono i rispettivi autori dei messaggi ricevuti. Quindi decifrano i messaggi facendo i dovuti calcoli su entrambi, usando entrambe le chiavi pubbliche degli altri gruppi, che sono scritte alla lavagna.
- Vince il gioco chi, non avendo commesso errori, ha impiegato meno tempo nel determinare chi sono gli autori dei messaggi ricevuti.

4. Prerequisiti e obiettivi.

I prerequisiti per poter effettuare il gioco sono legati alle abilità di calcolo aritmetico. Sono indispensabili: il concetto di numero primo; algoritmi e test di primalità, (ad es. il crivello di Eratostene); conoscenza di procedure di fattorizzazione; algoritmo euclideo della divisione (divisione con resto); cenni di aritmetica modulare (esempio dell'orologio; ecc.); cenni sugli esponenziali (le proprietà principali $x^{a+b}=x^a \cdot x^b = x^b \cdot x^a$ e $x^{a \cdot b}=(x^a)^b=(x^b)^a$).

Gli obiettivi del gioco sono invece la comprensione delle problematiche e delle operazioni per la protezione dei dati. In sintesi:

(a) conoscere un metodo matematico che si usa nella realtà;
(b) rafforzare le abilità aritmetiche;
(c) rafforzare le capacità logiche in modo ludico.

Oltre a calcolatrici (i pc sono facoltativi), è di grossa utilità avere a disposizione tabelle, tipo quella allegata, per semplificare alcuni

calcoli. Se si lascia ai ragazzi anche la costruzione delle chiavi allora può risultare utile un buon elenco di numeri primi (non molto grandi) per prepararsi da soli il protocollo di base, e utilizzare il lavoro di gruppo come metodo per confrontare idee ed opinioni.

Tabella 1. Elenco delle possibili scelte per $n < 400$.

$n = pq$	p	q	alcune coppie d, e		
121	11	11	3, 67	7, 43	9, 89
143	11	13	7, 103	13, 37	23, 47
169	13	13	5, 29	5, 173	7, 103
187	11	17	3, 107	7, 23	13, 37
209	11	19	7, 103	17, 53	23, 47
221	13	17	5, 77	7, 55	11, 35
247	13	19	5, 173	7, 31	11, 59
253	11	23	13, 17	23, 67	31, 71

$n = pq$	p	q	alcune coppie d, e		
289	17	17	5, 205	7, 183	21, 61
299	13	23	5, 53	7, 151	13, 61
319	11	29	23, 47	27, 83	31, 71
323	17	19	5, 173	11, 131	43, 67
341	11	31	7, 43	17, 53	19, 79
361	19	19	5, 65	11, 59	13, 25
377	13	29	5, 269	13, 181	17, 257
391	17	23	3, 235	5, 141	7, 151

Bibliografia.

[1] L.BERARDI-A.BEUTELSPACHER, Crittografia, Ed. Franco Angeli, 1994.
[2] E.AMBRISI-F.EUGENI, Cenni storici e metodi statistici per la decrittazione di sistemi di cifrature classici, Ratio Math. 1 (1990), 15-37.
[3] F.EUGENI, La funzione di Eulero ieri, oggi, domani, Atti del Convegno Nazionale della Mathesis, Cattolica 1994.
[4] F.EUGENI, La Matematica Discreta per problemi, Atti del Convegno Nazionale della Mathesis dedicato al Centenario della Fondazione, Roma, 1996.
[5] L.BERARDI-F.EUGENI, Strutture geometriche, crittografia e sistemi di sicurezza richiedenti un quorum, Atti del I Simposio su "Stato e prospettive della ricerca crittografica in Italia" - Roma, Ottobre 1987, Fondazione Bordoni.
[6] A.BEUTELSPACHER-F.EUGENI, Geometrie finite e crittosistemi: stato dell'arte e problematiche, Atti del II Simposio su "Stato e prospettive della ricerca crittografica in Italia"-Roma, Ottobre 1989, Fondazione Bordoni.
[7] M.CERASOLI-F.EUGENI-M.PROTASI, Elementi di Matematica Discreta, Zanichelli, Bologna, 1988.
[8] B.K.DASS-F.EUGENI, How to share secrets: the idea of Geometric threshold Games, Journal of Info. & Opti. Sci. 3 (1991), 451-458.
[9] F.EUGENI, Combinatorics and Cryptography, Proceedings of "Combinatorics 90", Gaeta, Annals of Discrete Math. (1992), 159-174.
[10] A. SGARRO, Crittografia, Mondadori giochi, 1990.
[11] A. SGARRO, Elementi di Crittografia, Ed. Muzzio, 1989.
[12] F.EUGENI-R.MASCELLA-D.TONDINI, L'autenticazione dei Messaggi: il software. Quaderno e CD a cura del Dipartimento M.E.T., Università di Teramo.