Numero 5 - 1992

RATIO MATHEMATICA

Atti del Convegno
Giornate di Geometrie Combinatorie
L'Aquila - Marzo 1991

a cura di

Franco Eugeni e Mario Gionfriddo

Comitato Organizzatore

Indice

PERCHE' SI APPLICA PROPRIO LA MATEMATICA ? ALCUNI PENSIERI CONSIDERANDO LA CRITTOGRAFIA

ALBRECHT BEUTELSPECHER
Math. Institut, Arndtstr. 2 D-6300 Giessen, Germania

1. Introduzione

Le problematiche connesse con la protezione delle cose preziose o delle informazioni sono state sempre presenti e saranno anche un grande problema anzi una sfida nel futuro. Pertanto l'uomo ha sempre provato ad inventare meccanismi per garantire una tale sicurezza. C'e' un grande numero di tali meccanismi e la maggior parte di questi non ha niente a che fare con la crittologia. Consideriamo due di tali meccanismi non-crittografici in dettaglio.

La protezione delle cose preziose oppure di informazioni segrete si ottiene normalmente mediante l'uso di una **cassaforte**. Ogni cosa che e' dentro una cassaforte e' protetta fisicamente. Solo il proprietario puo' aprire la cassaforte mediante una chiave oppure mediante una combinazione di cifre. Se la cassaforte ha piu' di un lucchetto, si puo' anche realizzare il principio dei quattro-occhi: cioe' che almeno due persone autorizzate siano d'accordo prima che la cassaforte si apra.

Un tipo completamente diverso di sicurezza si trova nella **carta moneta**. Qui il problema non e' la segretezza, ma la autenticita': i biglietti di banca non devono essere duplicati e neanche falsificati! Per questo si sono inventate proprieta' fisiche molto sofisticate. L'autenticita' di un biglietto di banca si ottiene (per esempio) mediante una speciale filigrana, mediante lo stampare con precisione, con l'utilizzo di carta speciale, etc. Ma si e' sempre saputo di biglietti di banca falsificati. In particolare, considerando le fotocopiatrici a colori moderne, ci si deve chiedere se la sicurezza offerta dai biglietti di banca sia sufficiente nei prossimi secoli.

I meccanismi tradizionali per ottenere la sicurezza (tra i quali abbiamo parlato della cassaforte e delle proprieta' dei biglietti di banca) hanno le seguenti proprieta' caratteristiche:

1. Sono basati su *proprieta' fisiche invariabili*: non cambia ne'la chiave per una cassaforte, ne' la filigrana di un biglietto di banca. La invariabilita' di tali proprieta' e' (in un certo senso) un fatto positivo e fondamentale per la sicurezza.

2. La maggior parte dei meccanismi tradizionali e' basata su *proprieta'* che sono essenzialmente *note e non segrete*. E' chiaro che la chiave di una cassaforte oppure la combinazione delle cifre deve essere conservata in modo sicuro, ma le proprieta' di sicurezza per i biglietti di banca sono pubbliche e solo quelli che conoscono le proprieta' sono in grado di distinguere un biglietto di banca vero da uno falso.

Ovviamente la sicurezza ottenuta da tali meccanismi puo' essere misurata solo empiricamente. Esprimiamo questo fatto con cattiveria (in pari tempo in modo piu' banale): un sistema viene usato solo fino a quando non viene rotto. La storia delle banche mostra chiaramente che la storia della moneta e' una lotta tra i "buoni" (la gente che inventa i meccanismi per la sicurezza) e i "cattivi" (che trovano il modo di rompere i sistemi di sicurezza). Le banche inventano sempre nuovi meccanismi e ottengono un vantaggio - ma questo vantaggio non e' garantito nel tempo perche' nuovi sviluppi tecnologici (ad esempio l'invenzione della fotocopiatrice a colori) costituiscono un nuovo pericolo.

A tal punto ci chiediamo: il mondo e' necessariamente cosi'? Non e' possibile fare in modo completamente diverso? E' possibile inventare sistemi di sicurezza nei quali un bandito non ha alcuna possibilita' di fare cose indesiderate - precisamente non solo oggi, ma per sempre ed in eterno? Se avessimo tre desideri liberi, allora potremmo chiedere una sicurezza con le seguenti proprieta':

- Non e' basata esclusivamente su proprieta' fisiche statiche.
- Non e' verificata solo empiricamente, ma si basa su fondamenti teorici.
- E' senza limite.

Nelle fiabe i desideri si avverano sempre - anche nella vita questo puo' talvolta accadere: lo scopo della **crittologia** e' quello di inventare sistemi di sicurezza che offrano sicurezza illimitata, la quale possa essere provata dai matematici in modo

rigoroso!

A questo punto il lettore certamente si chiedera': perche' proprio la crittografia e' in grado di produrre una tale meraviglia e non le altre scienze? La risposta e' semplice: ... perche' la crittografia e' matematica! Ci si chiede ora: perche' la matematica e' buona? La matematica e' adatta perche' i fatti sono accettati solo se sono dimostrati!

E' vero che le dimostrazioni non sono sempre molto gradite agli allievi e studenti, ma sono il vero vantaggio della matematica rispetto ad altre discipline. Immaginiamo ad esempio di avere monete (forse "monete elettroniche") tali che la loro sicurezza sia ottenuta mediante meccanismi crittografici e supponiamo che tale sicurezza sia provata matematicamente. Allora nessuna banca deve avere paura di un futuro sviluppo tecnologico, poiche' la sicurezza non e' basata sulla tecnologia di oggi, ma accertata per sempre!

Esiste un altro vantaggio nelle tecniche crittografiche. Se i cattivi riescono, ad esempio, a falsificare la filigrana, non ha senso mettere due filigrane dentro la carta per aumentare la sicurezza. D'altro canto, se esiste un protocollo crittografico che garantisce una sicurezza di, diciamo, 2^{-64} (cioe' una chiave di 64 bit), spesso e' anche possibile costruire un protocollo dotato di sicurezza doppia (cioe' 2^{-65}). In altre parole usando meccanismi crittografici, si puo' avere un livello di sicurezza arbitrario ("sicurezza senza limite").

Lo scopo di questo lavoro e' quello di dare argomentazioni a favore di queste tesi e di discutere se queste sono utopiche oppure realistiche.

2. Tre Applicazioni crittografiche

2.1 Controllo d'accesso

Consideriamo il problema di come una macchina possa convincersi della identita' di una persona. Un tale problema si presenta in molte situazioni, non solo per l'accesso ad un grande computer, ma ad ogni sportello Bancomat. Il metodo usuale e' che l'utente sia autenticato mediante un segreto (ad esempio il PIN). L'utente

trasmette il suo segreto all'Automa, il quale verifica se il segreto esibito e' proprio quello corrispondente al nome dell'utente.

Questo e' un **metodo statico** (poiche' il PIN non cambia mai) e ha tutti gli svantaggi di un metodo statico. Poiche' il PIN non cambia mai, un nemico deve scoprire solo una volta il PIN e dopo, conoscendo il segreto, puo' giocare il ruolo dell'utente.

Ma questo metodo ha un aspetto positivo: una persona puo' provare la sua identita' ad un computer mostrando di essere in possesso di un certo segreto. L'aspetto negativo e' che il segreto puo' essere scoperto.

Presentiamo ora un protocollo semplice, che costituisce un miglioramento essenziale: il segreto non viene trasmesso, i dati trasmessi sono di carattere random e il nemico non puo' fare nulla. L'idea e' la seguente: il computer pone una certa domanda, l'utente fornisce una risposta che dipende dal suo segreto **k**; infine il computer confronta la risposta dell'utente con il risultato che esso ha computato (cfr. Fig. 1).

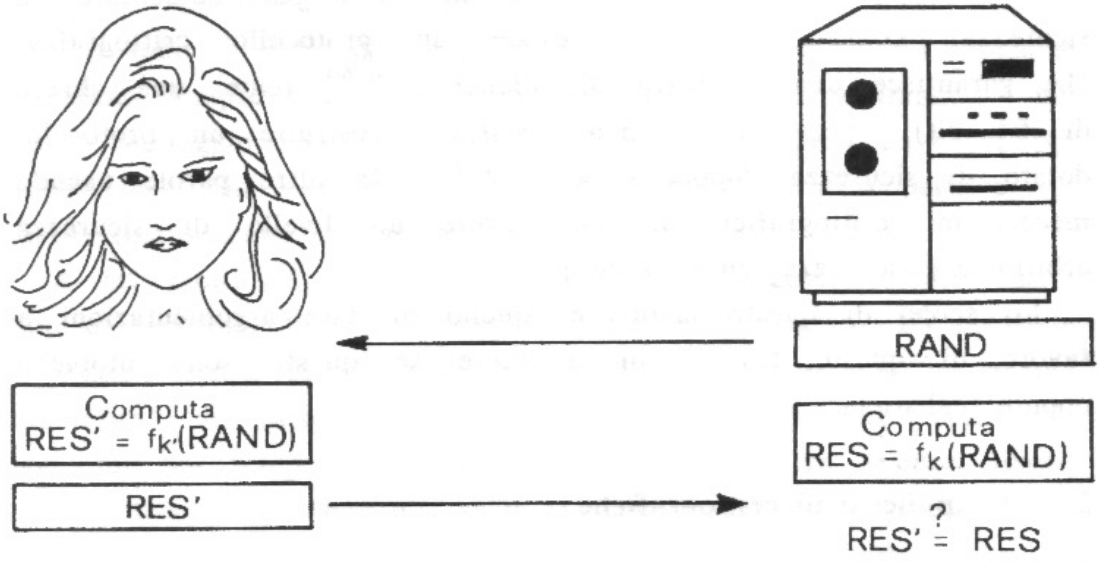

Fig. 1. Un protocollo challenge and response

Chiamiamo questo un protocollo **challenge and response**; il challenge e' un numero random RAND. Notiamo che f e' una funzione crittografica, che ha come input un "testo chiaro" RAND e una chiave k e ha come output una risposta RES := f_k(RAND).

Il nostro scopo qui non e' studiare le proprieta' che una tale

funzione f deve avere per essere adatta ad un protocollo challenge and response. Affermiamo solo che mediante l'uso di un protocollo semplice ed una funzione non complicata abbiamo ottenuto un progresso enorme: l'utente non deve scoprire il suo segreto, il computer si convince in *modo indiretto* che l'utente conosce il segreto k. Principalmente, un nemico non ha nessun vantaggio se ascolta la comunicazione.

Negli ultimi anni, tali protocolli challenge and response sono stati ampiamente sviluppati: i cosidetti protocolli "zero knowledge" hanno ottenuto un grado insuperabile di perfezione.

2.2 Funzioni unidirezionali

Per molte applicazioni crittografiche servono funzioni chiamate **unidirezionali**. Sono applicazioni che soddisfanno le seguenti proprieta' che a prima vista possono sembrare paradossali:

- E' facile computare f(x).
- La funzione f e' invertibile, ma dato un y, e' estremamente difficile trovare un x tale che sia f(x) = y.

Esistono delle funzioni unidirezionali? Nella vita quotidiana incontriamo "ampie carrettate" di tali funzioni: un esempio molto chiaro e significativo e' quello costituito da un elenco telefonico:

E' una cosa facilissima, usando un elenco telefonico, trovare il numero telefonico di una certa persona. Inversamente e' una grande perdita di tempo trovare il nome che corrisponde ad un numero dato. La ragione e' che per trovare un sol nome, si deve di fatto invertire tutta la guida telefonica.

Ci sono funzioni unidirezionali crittografiche? Questa e' una domanda difficilissima, che teoricamente non ha avuto ancora risposta. Nella ricerca si studiano funzioni che sono candidate ad essere funzioni unidirezionali: di conseguenza la matematica tocca livelli piu' elevati. Mediante l'uso di strutture matematiche si costruiscono potenziali funzioni unidirezionali. Gli oggetti piu' importanti per questi scopi sono i numeri primi p, precisamente "gli interi modulo p".

Nella crittografia il candidato principale a funzione unidirezionale e' la funzione esponenziale discreta. Che cosa e'? Per definirla ci serve (nel caso piu' semplice) un numero primo p (il modulo) e un intero b qualsiasi (la base). Si puo'

immaginare che la **funzione esponenziale discreta** ε_b sulla base b viene computata nei due passi seguenti:

Sia x un numero intero qualsiasi.

1*mo passo*: Computa b^x.

2*do passo*: Dividi b^x per p; il resto non-negativo si denota con $\varepsilon_b(x)$.

In poche parole: $\varepsilon_b(x) := b^x \bmod p$.

Si puo' credere che questa funzione sia molto simile alla funzione esponenziale reale ... e la funzione esponenziale reale e' una delle funzioni piu' studiate; in particolare ogni ingegnere conosce la sua funzione inversa e sa come trattarla. E poi?

Nella realta' - a parte la definizione - non vi e' alcuna somiglianza tra la funzione esponenziale reale continua e la funzione esponenziale discreta. La Fig. 2 mostra la difficolta' insita in una funzione esponenziale discreta.

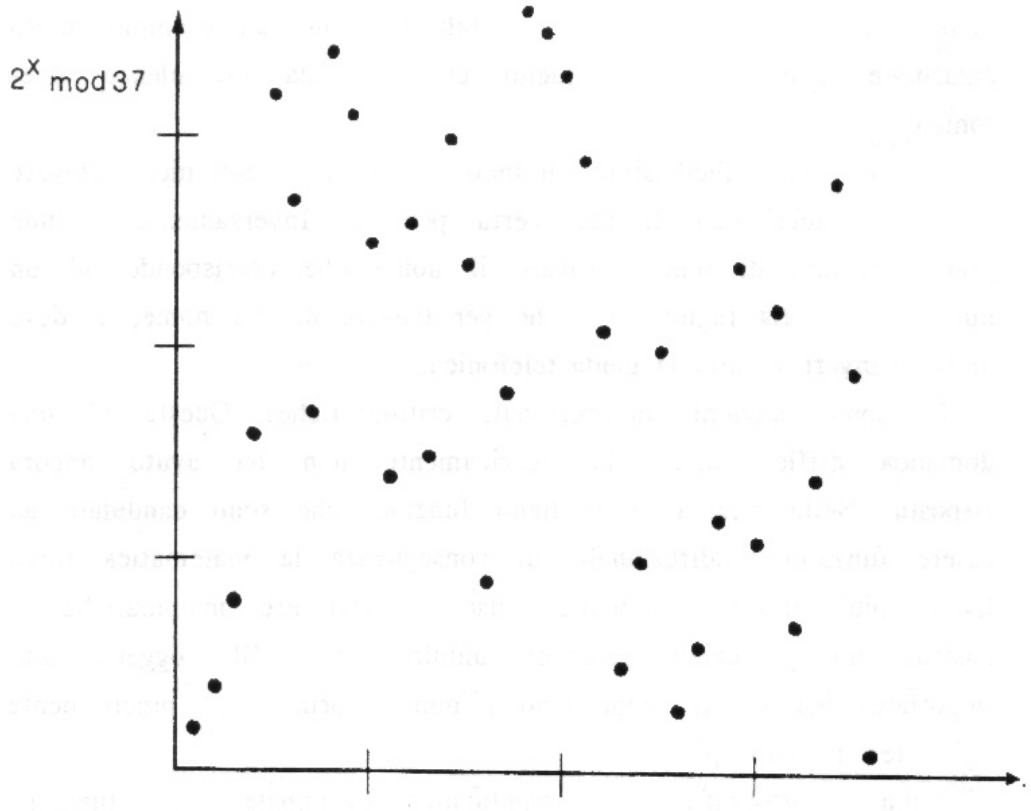

Fig. 2. Il fascino discreto della funzione esponenziale discreta (p = 37)

Chiaramente ci sono algoritmi migliori per computare la funzione esponenziale discreta; servono circa 2log p moltiplicazioni. Ma per invertire l'esponenziale discreto (cioe' per computare un **logaritmo discreto**) con i migliori algoritmi che possediamo servono circa $\sqrt{p}$ moltiplicazioni. Quindi la funzione esponenziale discreta puo' essere considerata come unidirezionale.

2.3 Segreti distributivi

In molte situazioni una informazione segreta deve essere distribuita tra molte persone cosi' da condividere anche la responsabilita' del segreto stesso. Presentiamo due esempi:

- Molte casseforti moderne utilizzano il "principio dei quattro occhi": solo se due persone autorizzate sono d'accordo ad aprire una cassaforte (con la chiave oppure con una combinazione di cifre), la cassaforte si apre.

Possiamo generalizzare il principio dei "quattrocchi" senza difficolta': desideriamo che un procedimento possa essere iniziato solo se due persone tra un numero totale di n autorizzate sono d'accordo. Questo metodo e' molto piu' flessibile del classico principio dei quattrocchi, poiche' basta che siano d'accordo due persone qualsiasi nell'insieme di tutti gli autorizzati.

- Nei sistemi crittografici spesso una chiave gioca un ruolo straordinario; usualmente una tale chiave si chiama **masterkey**. E' ovvio che la masterkey e' il tallone d'Achille del sistema, e dunque deve essere protetta meglio possibile. Ci sono due cose da osservare: una e' che il nemico non deve mai poter conoscere tutto il segreto, l'altra e' che gli impiegati leali devono essere protetti da falsi sospetti; quindi neanche un impiegato deve conoscere tutta la chiave - e questo deve poter essere dimostrato!

Per realizzare tutti questi scopi sono stati introdotti i **threshold schemes** come caso speciale degli **shared secret schemes**. In questo contesto il livello delle applicazioni della matematica e' altissimo: i threshold schemes offrono una sicurezza che puo' essere dimostrata in modo rigoroso!

In un **t-threshold scheme** il segreto viene diviso in molte parti (chiamati **segreti parziali**) tali che valgano le seguenti

proprieta':

- dato un sottoinsieme di t segreti parziali qualsiasi, il segreto puo' essere ricostruito facilmente;
- se sono noti t-1 segreti parziali o meno, il segreto non puo' essere ricostruito.

(E' chiaro che in un certo senso ogni segreto puo' essere ricostruito, per esempio, se il numero totale dei segreti possibili e' k, allora il segreto puo' essere "ricostruito" con una probabilita' di 1/k.)

Come esempio presentiamo il caso t = 2. Scegliamo una retta r in un piano (per gli esperti: in un piano proiettivo d'ordine q). Il segreto sia un punto K di r, scelto a caso. Per dividere il segreto K scegliamo una retta s diversa da r per il punto K. Infine scegliamo molti punti di s. Ognuno di questi punti e' un segreto parziale (cfr.Fig.3).

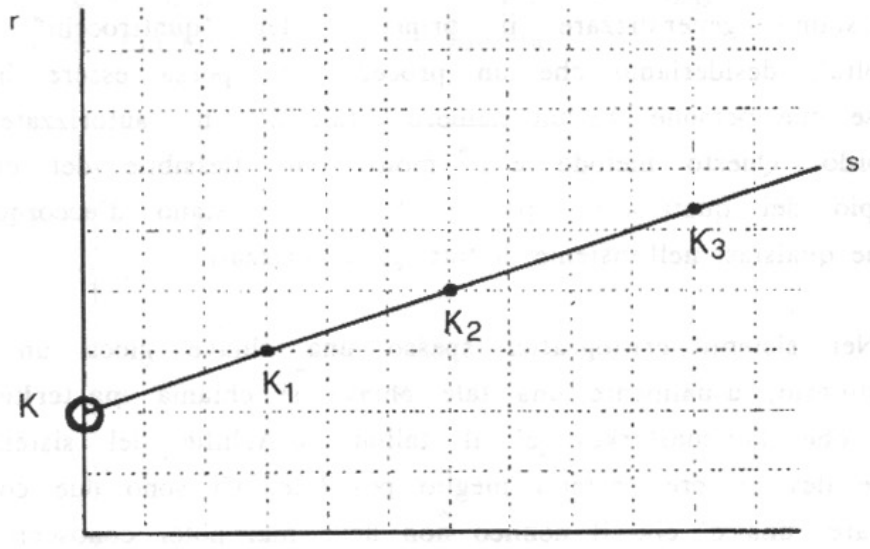

Fig. 3. Un threshold scheme con t = 2

Quando si vuole ricostruire il segreto, il sistema riceve alcuni punti; computa la retta s' per questi punti e computa l'intersezione di r ed s'. Questo punto K' e' il segreto ricostruito. Si confronti K' con K. Se sono uguali, la ricostruzione e' fatta.

Ora analizziamo la sicurezza di un tale 2-threshold scheme. Se la retta r ha almeno q+1 punti, la probabilita' di indovinare il segreto e' al piu' 1/(q+1). E' importante che questa probabilita' non aumenti per gli insider, cioe' per quelli che

conoscono qualche segreto parziale.

E' ben noto che per ogni potenza di un primo q esistono piani con la proprieta' che ogni retta ha precisamente $q+1$ punti (sono i piani di Galois costruiti mediante il campo di Galois con q elementi). Questo significa che e' possibile costruire t-threshold schemes per ogni livello di sicurezza desiderato.

Concludendo, questi sistemi offrono una sicurezza calcolabile; il fruitore sceglie numericamente la probabilita' che desidera e la matematica offre il sistema corrispondente! Inoltre, per avere una sicurezza abbastanza alta (ad esempio una probabilita' di 10^{-9}) servono solo "campi piccoli" (ordine di grandezza 2^{30}). Cio' significa che la implementazione non presenta nessuna difficolta'.

3. Conclusioni

Abbiamo cosi' mostrato che gli strumenti crittografici (cioe' matematici) raggiungono lo scopo desiderato che era appunto quello di avere una sicurezza misurabile, controllabile e dimostrabile. Distinguiamo i seguenti livelli

- sicurezza che puo' essere **analizzata in modo informale** (esempio: protocollo challenge and response);
- sicurezza che puo' essere **analizzata matematicamente** (esempio: la funzione esponenziale discreta);
- sicurezza che puo' essere **dimostrata matematicamente** (esempio: threshold schemes).

Dobbiamo ammettere che meccanismi la cui sicurezza e' dimostrabile, e contemporaneamente adatti per l'uso pratico sono per ora molto rari. Certamente lo scopo principale della crittografia per i prossimi anni sara' quello di sviluppare algoritmi e meccanismi che soddisfino entrambe le proprieta'.

Ma ripetiamo un'altra volta il messaggio di questo lavoro, come i Romani avrebbero detto: *In dubio pro matematica.*

Bibliografia

L. Berardi: Some remarks about an electronic signature derived from a generalized RSA-code. J. of Info. & Opti. Sci. 11 (1990), 189-194.

A. Beutelspacher, F. Eugeni: Geometrie finite e crittosistemi. Atti del II simposio nazionale so "stato e perspettive della ricerca crittografica in Italia". Roma, Novembre 1989.

B.K. Dass, F. Eugeni: How to share secrets: the idea of geometric threshold schemes. J. of Info. & Opti. Sci. 12 (1991), 3-11.

ISO Security Addendum ISO IS 7498/2: Open Systems Interconnection Reference Model - Part 2: Security Architecture

D. Chaum: Security without Identification: Transaction systems to Make Big Brother Obsolete. Comm. ACM 28 (1985), 1030-1044

D.W. Davies, W.L. Price: Security for Computer Networks. John Wiley & Sons, Chichester, 2nd edition 1989

A. Sgarro: Crittografia. Muzzio Editore, 1986.

G. Simmons: How to (really) share a secret. Advances of Cryptology - CRYPTO 88, Lecture Notes in Computer Science 403 (1989), 390-448.

G. Simmons: Authentication Theory / Coding Theory. Advances in Cryptology - CRYPTO 84, Lecture Notes in Computer Science 196 (1985), 411-432.

A. Shamir: How to share a secret. Comm. ACM 22 (1979), 612-613.