Problema

State viaggiando in autostrada, e decidete di fermarvi in un autogrill. Chiudete la macchina con il telecomando che aziona la chiusura centralizzata a distanza, andate al bar, tornate. Aprite la macchina con lo stesso telecomando, e scoprite che è stata svuotata. Chiamate la Polizia, e vi spiegano che qualcuno si è appostato nelle vicinanze, e con un apposito ricevitore, ha intercettato il codice “segreto” (pubblicizzato come “dotato di 100000000 di diverse combinazioni”) inviato dal vostro telecomando alla centralina della macchina, e in questo modo l'ha aperta, svuotata e poi richiusa, sempre nello stesso modo.
Come evitare tutto ciò ? Cosa c'entra la crittografia, e a maggior ragione la matematica in tutto questo ?

La crittografia

La crittografia è un'arte antica, risale almeno ai Greci (Tucidide, scitala lacedemonica).

E' sempre stata associata con i segreti, soprattutto diplomatici e militari. La sua funzione fondamentale consiste nell'alterare un messaggio in modo tale che sia leggibile solo da parte di chi possiede una qualche **informazione segreta**, che in gergo viene chiamata "**chiave**".

Giulio Cesare, per proteggere la sua corrispondenza privata, usava sostituire ogni lettera dell'alfabeto con la lettera che si trova tre posizioni più avanti: la **a** con la **d**, la **b** con la **e,** e così via.

Tutti i cifrari di questo genere (monoalfabetici) possono essere forzati facilmente usando una tecnica statistica, basata sul fatto che la sostituzione applicata alle lettere dell'alfabeto conserva le frequenze con cui le lettere occorrono, nella lingua in cui è scritto il messaggio (scoperta dagli Arabi intorno al IX secolo).

Nel Rinascimento (G.B. Alberti) sono stati sviluppati sistemi più raffinati (polialfabetici) fino ad arrivare al cifrario di Vigenère (XVI secolo), che ha resistito per circa tre secoli (Babbage e Kasinski).

Nel secolo scorso la crittografia si è meccanizzata: sono state inventate macchine cifranti in grado di eseguire tutto il lavoro di cifratura e decifrazione.
Ciò ha permesso di introdurre cifrari molto più complessi: Enigma, usato dall'esercito tedesco durante la Seconda Guerra Mondiale, Purple, usato dai giapponesi.

Questi cifrari non potevano essere attaccati con i metodi tradizionali; sono così entrati in scena i matematici.
Alan Turing ha dato un contributo fondamentale alla decifrazione di Enigma da parte degli alleati, il che ha avuto un'influenza decisiva sulle sorti della guerra.
Per arrivare alla decifrazione del codice Lorentz SZ40, un sistema analogo a Enigma, ma più complesso, usato per le comunicazioni tra Hitler e il suo stato maggiore, il matematico inglese Max Newman ha sviluppato il primo progetto di calcolatore elettronico programmabile, basandosi sulle idee di Turing.

La prima vera rivoluzione della crittografia è avvenuta nel 1976.

La crittografia simmetrica (o a chiave privata)

Le due entità che vogliono comunicare in modo riservato su un **canale insicuro** devono condividere una chiave segreta **k**. Alice, che invia il messaggio, applica l'algoritmo di cifratura **E**, che usa la chiave **k**, al messaggio **m**, per produrre il messaggio cifrato **c**, e lo invia a Bob. Questi riceve il messaggio **c**, e applica l'algoritmo di decifrazione **D**, che usa la stessa chiave **k**, per recuperare **m**. Solo il possesso di **k** permette di cifrare e decifrare; in questo modo il messaggio è protetto.

La crittografia simmetrica ha un grosso **problema**: la distribuzione delle chiavi.
Ricordate che A e B devono condividere la stessa chiave segreta, devono quindi o avere a disposizione un canale sicuro per scambiarsela (difficile e costoso), oppure incontrarsi e scambiarsela di persona.
Immaginate che, prima di comprare qualcosa su Internet usando una carta di credito, il cui numero deve rimanere un segreto tra voi e il venditore, dobbiate incontrarlo personalmente (magari si trova negli USA ...) e scambiare con lui una chiave segreta. Il commercio su Internet non avrebbe un gran futuro ...

La crittografia a chiave pubblica

Nel 1976 due americani, W.Diffie e M.Hellmann, ebbero un'idea veramente rivoluzionaria: i sistemi a chiave pubblica.

L’idea è questa: ogni utente di un sistema di crittografia a chiave pubblica ha **due** chiavi, una usata solo per cifrare, l’altra solo per decifrare.

La chiave di decifrazione deve essere tenuta segreta, e non va quindi rivelata a nessuno.

La chiave di cifratura può essere resa pubblica, in una specie di elenco telefonico on-line, dato che serve solo a cifrare i messaggi, e la sua conoscenza non è di nessun aiuto per la decifrazione.

Supponiamo ad esempio che Alice voglia mandare un messaggio riservato a Bob. Si procura la chiave pubblica di Bob, chiamiamola e_B , e la usa per cifrare il messaggio:

$$c = E_{e_B}(m)$$

Quando Bob riceve il messaggio, usa la sua chiave privata d_B per decifrarlo:

$$m = D_{d_B}(c)$$

Il problema dello scambio delle chiavi è risolto nel modo più brillante: eliminando lo scambio delle chiavi.

L'idea è molto elegante, ma come realizzarla ? Diffie ed Hellmann non ci riuscirono.

L'anno dopo (1977) Rivest, Shamir ed Adleman realizzarono il sistema RSA (dalle iniziali dei loro nomi), che è tuttora il sistema a chiave pubblica più usato (ad esempio nel protocollo SSL).

La teoria dei numeri

Qui entra in gioco la **teoria dei numeri**. Questa è una branca molto antica della matematica (risale almeno ad Euclide), che tradizionalmente è stata sempre considerata "pura", ossia priva di applicazioni pratiche.

Un famoso matematico inglese, G.H.Hardy, è arrivato al punto di celebrare questa "inutilità" della teoria dei numeri come una delle sue virtù.

Rivest, Shamir ed Adleman hanno utilizzato, nel loro sistema RSA, alcuni strumenti della teoria elementare dei numeri (che risalgono almeno a Gauss, all'inizio dell'800).

Perché la teoria dei numeri ?

La ragione è che la teoria dei numeri fornisce **problemi difficili**, per la cui soluzione non esistono, a tutt'oggi, procedimenti efficienti.

Il problema difficile usato in RSA è quello della **fattorizzazione in primi** di un numero naturale.

Un numero naturale è **primo** se è divisibile (con resto 0) solo per se stesso e per 1. Ad esempio, sono primi 2, 3, 5, 7, 11 etc.

Esistono infiniti numeri primi, e ogni numero naturale si rappresenta, in modo unico (a meno dell'ordine con cui vengono scritti i fattori), come prodotto di numeri primi (teorema fondamentale dell'aritmetica).

Ad esempio:

$$10 = 2 \times 5$$

$$40 = 2^3 \times 5$$

Tutto questo è noto fin dal tempo dei Greci: un metodo per generare numeri primi è il Crivello di Eratostene (III secolo a.c.).

Per trovare la fattorizzazione in primi di un numero **n** dato basta provare a dividere **n** per tutti i numeri che lo precedono.
In questo modo si stabilisce anche se n è primo.

Dove sta allora la difficoltà ?

Problemi facili e difficili

ra i due problemi:

) Stabilire se un numero n è primo

) Trovare la fattorizzazione in primi di un numero n

’è una differenza fondamentale:

ur essendo entrambi banali, in linea di principio, esistono procedimenti (algoritmi) molto fficienti per risolvere il primo, mentre, a tutt’oggi, non esistono algoritmi efficienti per il econdo.

RSA

RSA sfrutta questa differenza di difficoltà per implementare l'idea della crittografia a chiave pubblica.

Vengono generati due primi molto grandi **p** e **q**, che vengono tenuti **segreti**, e ne viene calcolato il prodotto **n = pq,** che invece viene reso **pubblico.**

Per trovare la chiave segreta occorrere conoscere **p** e **q**, perciò la sicurezza del sistema riposa proprio sulla difficoltà della fattorizzazione di **n**.

In RSA hanno un ruolo essenziale anche altri strumenti classici della teoria elementare dei numeri: l'algoritmo di Euclide per il calcolo del Massimo Comun Divisore e il Teorema Cinese dei Resti.

Soluzione del problema

Si tratta di un **problema di identificazione**: la centralina, prima di aprire le portiere, deve essere certa dell'"identità" di chi ha inviato la richiesta.

L'attacco descritto è di tipo "replay", ed è analogo alla situazione in cui qualcuno, alle vostre spalle, legge la password che usate per accedere al vostro computer mentre la digitate, e la usa poi per accedere con il vostro nome.

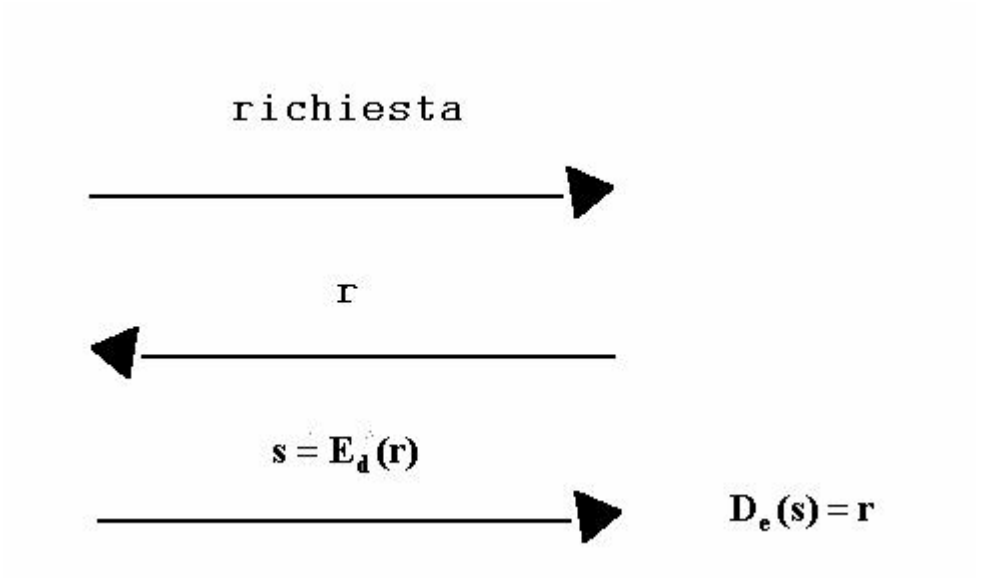
Una soluzione molto elegante e sicura si ottiene applicando una tecnica chiamata "**protocollo di sfida-risposta**", che usa, a sua volta, un sistema di crittografia a chiave pubblica.

Come nell'esempio della password, l'identità viene provata dimostrando di essere a conoscenza di un **segreto**, solo che, in questo caso, il segreto non viene comunicato esplicitamente.

Nel caso si usi il sistema RSA, il segreto consiste proprio nei due primi $\boldsymbol{p}$ e $\boldsymbol{q}$, e non è neppure necessario che chi verifica l'identità (la centralina) li conosca.

Riassumiamo: *A dimostra a B di essere veramente A provando a B di essere a conoscenza di un segreto, che B neppure conosce !*

Sembra impossibile, ma non lo è.


richiesta
r
s = E_d(r)
D_e(s) = r