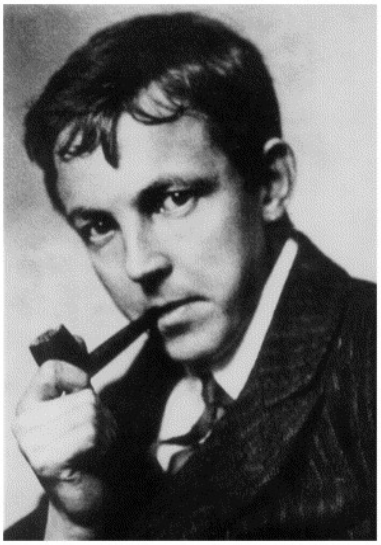
RSA &
Attacco di Wiener

Matteo Giorgi



Godfrey Harold Hardy
(Cranleigh 1877 – Cambridge 1947)

Is mathematics "useful", directly useful, as other sciences such as chemistry and physiology are? This is not an altogether easy or uncontroversial question, and I shall ultimately say No...

...both Gauss and less mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

— G.H. Hardy, A Mathematician's Apology, 1940

Oramai a oltre settant'anni dalla pubblicazione della sua famosa Apologia, mi sono sempre chiesto che cosa direbbe Hardy riguardo l'evoluzione della matematica moderna, la Teoria dei numeri e le applicazioni pratiche che questa ha indotto nell'ultimo mezzo secolo. Proprio la sua Teoria dei numeri, descritta da Gauss come la regina delle matematiche per la sua "suprema inutilità", è stata la base per nuovi settori della matematica applicata come la *Teoria computazionale dei numeri* e la *Crittografia asimmetrica*.

Questo lavoro vuole essere un percorso alla scoperta del crittosistema *RSA* e nello specifico delle conseguenze che il Teorema di Wiener ha portato.

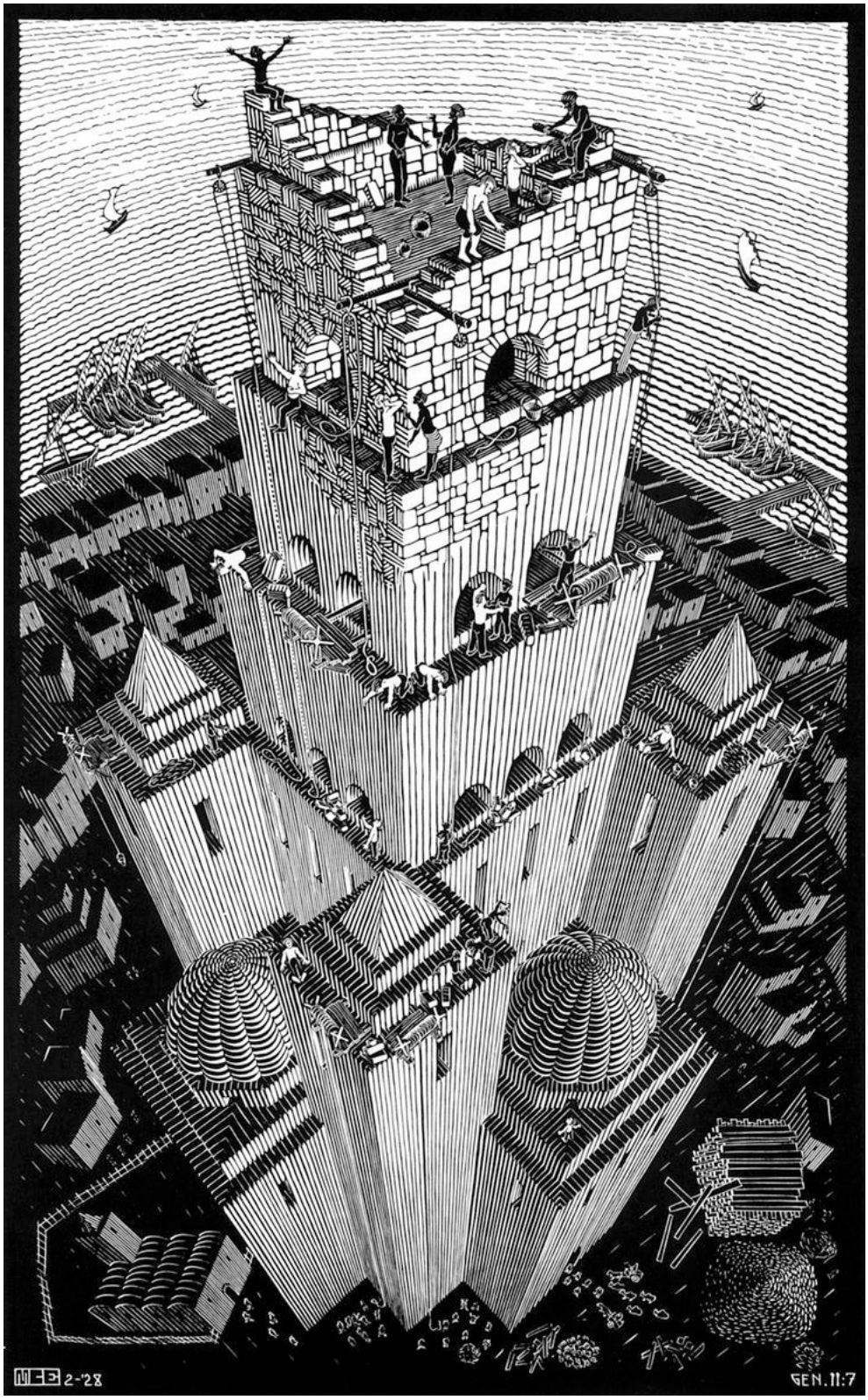
Indice

Nel testo sono usati i nomi che abitualmente si trovano in Letteratura per le comunicazioni cifrate: il mittente *Alice*, il destinatario *Bob* ed il crittoanalista *Oscar* che cerca di carpire il messaggio della conversazione.

Riguardo la notazione, è necessario fornire chiarimenti su quella usata. Il campo finito $\mathbb{Z}/p\mathbb{Z}$ degli interi modulo un primo p, spesso denotato con $\mathbb{F}_p$ o $GF(p)$, è qui indicato con il simbolo $\mathbb{Z}_p$ (in alcuni testi usato invece per gli anelli di interi p-adici), mentre $\mathbb{Z}_p^*$ si riferisce al gruppo delle unità, o gruppo moltiplicativo, di $\mathbb{Z}/p\mathbb{Z}$. Dati $a, b \in \mathbb{Z}_p$, la relazione di uguaglianza è qui denotata dalla congruenza modulo p: $a \equiv b \pmod p$ oppure $a \equiv_p b$. In ultimo, $\mathbb{Z}^+$ indica il sottoinsieme degli interi positivi.

All notation should be as simple as the nature of the operation to which is applied.

— C. Babbage


MCE 2-28
GEN. 11:7

Verso il crittosistema *RSA*

Per comprendere appieno i principi della *crittografia asimmetrica*, è necessario ricapitolare le basi della cifratura simmetrica.

Un sistema simmetrico è tale se un'unica chiave segreta è usata per cifrare/decifrare il testo e le funzioni di cifratura/decifrazione sono simili tra loro. *Alice* dovrà quindi cifrare il messaggio usando una chiave segreta k e spedirlo su un canale insicuro a *Bob* che decifrerà il crittogramma con la medesima chiave.

I moderni algoritmi simmetrici come AES o Triple-DES sono sicuri e largamente utilizzati, tuttavia presentano dei limiti.

- ⊛ Distribuzione delle chiavi: la chiave deve essere stabilita tra *Alice* e *Bob* usando un canale sicuro.
- ⊛ Elevato numero di chiavi: in una rete con n utenti sono necessarie $\mathcal{O}(n^2)$ coppie di chiavi ed ogni utente deve archiviare in modo sicuro $n-1$ chiavi per poter comunicare.
- ⊛ Vulnerabilità alle "truffe": con un'unica chiave privata, la crittografia simmetrica non fornisce sicurezze sull'identità degli utenti.

Questi problemi furono risolti a metà degli anni '70 quando un matematico del MIT Whitfield Diffie ed un ingegnere di Stanford Martin Hellman avanzarono una nuova idea rivoluzionaria basata sul presupposto che il crittogramma potesse essere decifrato unilateralmente: *Bob* rilascia pubblicamente una chiave k_{pub} usata da *Alice* per cifrare il messaggio e spedirlo, sicura del fatto che solamente *Bob* potrà decifrarlo grazie ad una seconda chiave privata k_{priv} in suo possesso. Nasce così la *crittografia asimmetrica* [1].

La base per costruire un tale algoritmo risiede nel cifrare con una funzione *One-Way Trapdoor*: facile da eseguire, ma computazionalmente difficile da invertire a meno di possedere una specifica chiave privata. Questa scelta è sufficiente per proteggersi da *Oscar* che altrimenti potrebbe risalire al messaggio invertendo la funzione di cifratura.

Oggi sono i *protocolli ibridi* come SSL/TLS o IPsec i più utilizzati: un algoritmo asimmetrico per scambiare la chiave segreta k in sicurezza, uno simmetrico per cifrare velocemente il testo da inviare.

Uno dei più importanti algoritmi simmetrici della crittografia moderna è il *Data encryption Standard* o DES, sviluppato negli anni '70 dalla IBM e adottato nel 1977 come *Federal Information Processing Standard* per gli US. Nella sua forma base il DES non è più considerato sicuro per la chiave di soli 56 bit, vulnerabile ad attacchi brute-force. Rimane comunque in grande uso oggi nella sua forma modificata *Triple-DES*.

Michael Wiener, nel 1993 alla conferenza CRYPTO, propose un efficiente key-search con tecniche pipeline, stimando un tempo di ricerca medio di 36 ore ed un costo totale di un milione di dollari.

Nel 1998 la *Electronic Frontier Foundation*, con un budget di 250,000 dollari, costruì *Deep Crack* capace di una ricerca esaustiva della chiave in 56 ore. Nel 2006 un team di ricercatori delle università di Bochum e Kiel realizzò COPACOBANA, una macchina composta da 120 FPGA, in grado di rompere il DES in 7 giorni con un budget di soli 10,000 dollari. Questo decretò il definitivo pensionamento del DES in favore del nuovo standard *Advanced Encryption Standard* (AES).

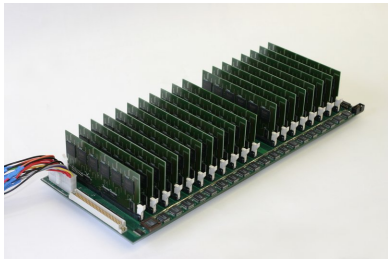


Figura 1: versione aggiornata al 2008 di COPACOBANA con 128 Virtex-4 SX35. Il tempo medio è sceso a 6 giorni, quello al caso pessimo a meno di 13.

⇝ www.copacobana.org

Definizione 1 (ϕ di Eulero).
Dato $n\in\mathbb{Z}^+$, la funzione di Eulero $\phi(n)$ è definita come il numero di classi di resto modulo n coprime con n:

$$\phi(n) \overset{def}{=} \{z\in\mathbb{Z}_n \mid MCD(z,n)=1\}$$

Definizione 2 (μ di Möbius).
Dato $n\in\mathbb{Z}^+$, la funzione di Möbius $\mu(n)$ è definita come:

$$\mu(n) \overset{def}{=} \begin{cases} 1 & se\ n=1 \\ 0 & se\ \exists\ p^2|n,\ p\ primo \\ (-1)^k & se\ n=\prod_{i=1}^{k} p_i \end{cases}$$

Lemma 1 ($\phi \propto \sum\mu$). *Sia $n\in\mathbb{Z}^+$:*

$$\phi(n) = \sum_{d|n} n\frac{\mu(d)}{d} \tag{1}$$

Dimostrazione. Sia $m\in\mathbb{Z}^+$. Allora:

$$\sum_{d|m}\mu(d) = \begin{cases} 1 & \text{se } m=1 \\ \boxed{0} \leftarrow \sum_{i=1}^{k}\binom{k}{i}1^{k-i}(-1)^i & \text{se } m>1 \end{cases}$$

e posso affermare che $\sum_{d|m}\mu(d)=\lfloor 1/m \rfloor$. Ora, usando la Definizione 1 e fissato un $d|n$, posso sommare tutti i $k=qd\in[1,n]$:

$$\phi(n) = \sum_{k=1}^{n}\left\lfloor\frac{1}{(n,k)}\right\rfloor = \sum_{\substack{d|n \\ d|k}}\mu(d) =$$
$$= \sum_{d|n}\sum_{q=1}^{n/d}\mu(d) = \sum_{d|n} n\frac{\mu(d)}{d} \qquad \blacksquare$$

Lemma 2 (Calcolo ϕ). *Sia $n\in\mathbb{Z}^+$:*

$$\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) \tag{2}$$

Dimostrazione. Per $n=1$ la produttoria è vuota perchè non esistono primi divisori di 1, quindi $\phi(1)=1$. Supponendo invece $n>1$, si può esprimere $n=\prod_{i=1}^{k}p_i^{\alpha_i}$ e, per il *Principio di Inclusione-Esclusione*, la produttoria può essere riscritta come:

$$\prod_{p|n}(1-\tfrac{1}{p}) = \prod_{i=1}^{k}(1-\tfrac{1}{p_i}) =$$
$$= 1-\sum\tfrac{1}{p_i}+\sum\tfrac{1}{p_ip_j}+\ldots+\tfrac{(-1)^k}{\prod_{i=1}^{k}p_i}$$

dove ciascun termine è della forma $\pm 1/d$. Il denominatore d è un divisore di n, prodotto di primi distinti; il numeratore ± 1 è esattamente la *Funzione di Möbius* $\mu(d)$. Quindi la produttoria risulta:

$$\prod_{p|n}\left(1-\frac{1}{p}\right) = \sum_{d|n}\frac{\mu(d)}{d}$$

che, per il lemma 1, dimostra la tesi. $\blacksquare$

Il crittosistema *RSA*

La scelta per una funzione *One-Way Trapdoor* deve ricadere su un'idea concettualmente semplice, facile da implementare ma con una forte prova empirica che la decifrazione non sia possibile a meno di conoscere la chiave segreta. La risposta arriva dalla teoria dei numeri: la fattorizzazione di un intero.

Nel 1977 tre informatici del MIT Ronald Rivest, Adi Shamir e Leonard Edleman esposero il *MIT public-key criptosystem*, successivamente *RSA*, incentrato proprio sulla fattorizzazione di interi ed il Teorema di Eulero-Fermat [2].

Teorema 1 (Eulero-Fermat). *Siano a, n interi coprimi. Allora:*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{3}$$

Dimostrazione. Preso $k\in\mathbb{Z}$ coprimo con n e $\{a_1,a_2,\ldots,a_{\phi(n)}\}$ insieme delle classi di resto modulo n coprime con n, $\{ka_1,ka_2,\ldots,ka_{\phi(n)}\}$ è il medesimo insieme perchè:

① scelte due classi distinte a_i, a_j con $i,j\in[1,\phi(n)]$ e $i\neq j$, posso affermare che $a_i\not\equiv_n a_j \Rightarrow ka_i\not\equiv_n ka_j$;

② fissato $a\in\{a_1,a_2,\ldots,a_{\phi(n)}\}$, la congruenza $kx\equiv_n a$ ha soluzione $x_0\in\{a_1,a_2,\ldots,a_{\phi(n)}\}$, quindi $x_0\equiv_n a_i \Rightarrow kx_0\equiv_n ka_i\equiv_n a$.

Pertanto adesso posso scrivere

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$
$$a^{\phi(n)}\prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

e concludere che $a^{\phi(n)}\equiv_n 1$. $\blacksquare$

Funzionamento *RSA*. Analogamente agli altri sistemi asimmetrici, l'*RSA* può essere pensato come composto da tre algoritmi efficientemente calcolabili: un generatore della chiave che definisce lo spazio delle *chiavi* ($\mathcal{K}$), un algoritmo di cifratura e uno di decifrazione che definiscono lo spazio dei *messaggi* ($\mathcal{M}$) e dei *crittogrammi* ($\mathcal{C}$).

Bob sceglie dunque due primi molto grandi p e q che tiene segreti e calcola il modulo dell'*RSA* $N=pq$. Sceglie poi un esponente pubblico $e\in\mathbb{Z}^*_{\phi(N)}$ (unità di $\mathbb{Z}_{\phi(N)}$) e calcola l'esponente privato d tale che $ed\equiv_{\phi(N)}1$. Quindi, per ogni possibile chiave $k=(N,p,q,e,d)\in\mathcal{K}$, le funzioni di cifratura e decifrazione sono definite come:

$$Enc_k : \overset{\mathbb{Z}_N}{\mathcal{M}} \to \overset{\mathbb{Z}_N}{\mathcal{C}} \qquad m \to m^e$$

$$Dec_k : \overset{\mathbb{Z}_N}{\mathcal{C}} \to \overset{\mathbb{Z}_N}{\mathcal{M}} \qquad c \to c^d$$

mentre le chiavi pubblica e privata risultano:

$$k_{pub} = (e, N) \qquad\qquad k_{priv} = (d, p, q)$$

A questo punto è chiaro come la correttezza della funzione di decifrazione Dec_k risieda nel Teorema di Eulero-Fermat, sia nel caso in cui $MCD(m,N)=1$, che altrimenti:

$$m \equiv c^d \equiv (m^e)^d = \boxed{m^{1+k\phi(N)} \equiv m \pmod N}$$

$$\downarrow$$

$$\text{se } MCD(m,N)=1 \Rightarrow m^{\phi(N)} \equiv_N 1 \Rightarrow m^{1+k\phi(N)} \equiv_N m$$

$$\text{altrimenti } \begin{cases} m^{1+r\phi(N)} \equiv_p m \\ m^{1+s\phi(N)} \equiv_q m \end{cases} \overset{\text{Th. Cinese dei Resti}}{\boxed{\Rightarrow}} m^{1+k\phi(N)} \equiv_N m$$

Certamente, messaggi coprimi con il modulo dovrebbero essere evitati perchè il relativo crittogramma c rivelerebbe la fattorizzazione del modulo stesso: in particolare, eseguire $MCD(c,N)$ individuerebbe un multiplo di uno dei primi p e q.

Definire gli esponenti pubblico e privato come inversi modulo $\phi(N)$ fornisce una condizione sufficiente per recuperare il messaggio da qualsiasi crittogramma, mentre la condizione necessaria è che siano inversi modulo $\lambda(N)$, *Funzione di Carmichael*. Quindi, dato il modulo N, $\lambda(N)=mcm(p-1,q-1)$ e:

$$\begin{aligned} \phi(N) &= (p-1)(q-1) \\ &= MCD(p-1,q-1)\ mcm(p-1,q-1) \\ &= MCD(p-1,q-1)\ \lambda(N) \end{aligned}$$

ovvero $\lambda(N)|\phi(N)$, il che ci permette di usare $\phi(N)$ nell'algoritmo generatore della chiave. Nel corrente standard *PKCS #1* i due esponenti pubblico e privato sono definiti come inversi modulo $\lambda(N)$.

Attacchi elementari

Gli attacchi al crittosistema *RSA* sono generalmente classificabili in diverse famiglie. Gli attacchi *algoritmici diretti* sono quelli di più immediata intuizione e si suddividono in attacchi sulla fattorizzazione intera, logaritmo discreto e attacchi quantistici. Da notare invece che gli attacchi migliori cercano di sfruttare le debolezze matematiche dell'algoritmo o un improprio uso del sistema (un esponente piccolo o il medesimo modulo su più comunicazioni): questi sono gli attacchi *algoritmici indiretti* e saranno l'oggetto del resto di questo lavoro. A titolo informativo è giusto citare anche gli attacchi *side-channel*: essi sfruttano specifici problemi di implementazione dell'hardware, come il consumo energetico o il tempo di cifratura/decifrazione del dispositivo, per recuperare la chiave segreta.

Di seguito alcuni attacchi algoritmici elementari indiretti.

Teorema 2 (Cinese dei resti).
Sia $a,b,m,n \in \mathbb{Z}$ con $MCD(m,n)=1$. Allora $\exists!\ x \in \mathbb{Z}_{mn}$ tale che:

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases} \tag{4}$$

Dimostrazione. Se $\tilde{t} \in \mathbb{Z}$ risolve $a+tm \equiv_n b$ allora $x=a+tm$ è soluzione di (4).
Esistenza: $\exists\ \tilde{t} \in \mathbb{Z}$ soluzione di $a+tm \equiv_n b$ perchè $MCD(m,n)=1$ per ipotesi.
Unicità: se il sistema ammette due soluzioni x, y allora $m,n|b-a$. Segue che $mn|b-a$, ovvero $x \equiv_{mn} y$. ■

Definizione 3 (λ di Carmichael).
Dato $n \in \mathbb{Z}^+$, la funzione di Carmichael $\lambda(n)$ è definita in termini di $\phi(n)$:

$$\lambda(n) \overset{def}{=} \begin{cases} \frac{1}{2}\phi(2^\alpha) & \text{se } n=2^\alpha,\ \alpha>2 \\ \phi(p_1^\alpha) & \text{se } n=p_1^\alpha \\ \underset{i=1\ldots k}{mcm}\left(\lambda(p_i^{\alpha_i})\right) & \text{se } n=\prod_{i=1}^k p_i^{\alpha_i} \end{cases}$$

con $\alpha \in \mathbb{Z}^+$, $p_{i\in\{1\ldots k\}} \in \mathbb{Z}^+$ primi.

Lemma 3. *Siano a, n interi coprimi. Allora:*

$$a^{\lambda(n)} \equiv 1 \pmod n \tag{5}$$

Dimostrazione. In accordo con la Definizione 3:

$$\text{se } n=2^\alpha \Rightarrow \phi(n)=2\lambda(n) \Rightarrow a^{\lambda(n)} \equiv 1 \pmod n$$

$$\text{se } n=p_1^\alpha \Rightarrow \phi(n)=\lambda(n) \Rightarrow a^{\lambda(n)} \equiv 1 \pmod n$$

$$\text{se } n=\prod_{i=1}^k p_i^{\alpha_i} \Rightarrow \lambda(n)=x_j\lambda\left(p_j^{\alpha_j}\right) \text{ per } j\in\{1\ldots k\}$$

$$\Rightarrow \begin{cases} \left(a^{\lambda(p_1^{\alpha_1})}\right)^{x_1} \equiv 1 \pmod{p_1^{\alpha_1}} \\ \left(a^{\lambda(p_2^{\alpha_2})}\right)^{x_2} \equiv 1 \pmod{p_2^{\alpha_2}} \\ \vdots \\ \left(a^{\lambda(p_k^{\alpha_k})}\right)^{x_k} \equiv 1 \pmod{p_k^{\alpha_k}} \end{cases}$$

$$\overset{\text{Th. Cinese dei Resti}}{\boxed{\Rightarrow}} a^{\lambda(n)} \equiv_n 1. \qquad ■$$

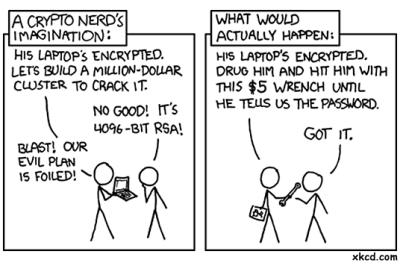


Figura 2: Crypto-Brainstorming.

Quanti bits deve avere il modulo per essere considerato sicuro?

Nel 1999 gli RSA-Laboratories impiegarono sette mesi per fattorizzare un intero di 515b (155 cifre decimali) nel prodotto di due primi da 77b: non male!

Nel 2004, per una chiave che rimanesse sicura fino al 2010, raccomandavano l'utilizzo di moduli da 1024b (fattorizzabili in primi da 154b), mentre per una sicurezza più a lungo termine (2030) sono tuttora necessari almeno 2048b.

⇝ www.rsa.com

Stima $\phi(N)$. Se *Oscar* potesse conoscere il valore di $\phi(N)$, potrebbe facilmente recuperare m in tempo polinomiale: $\phi(N) \overset{\mathcal{P}}{\Rightarrow} \{m\}$.
Sarà dunque necessario mostrare che il calcolo di $\phi(N)$ e l'*Integer Factorization Problem* (*IFP*), ovvero la fattorizzazione del modulo, sono asintoticamente equivalenti.

Teorema 3.

$$\phi(N) \overset{\mathcal{P}}{\Longleftrightarrow} IFP(N) \tag{6}$$

Dimostrazione. Essendo $\phi(N)=(p-1)(q-1)$ noto, si ottiene che

$$\begin{gathered} p^2 - \underbrace{\big(N-\phi(N)+1\big)}_{p+q=A} p + \underbrace{N}_{p\cdot q} = 0 \\ \text{quindi} \quad (p,q) = \tfrac{A\pm\sqrt{A^2-4N}}{2} \end{gathered} \tag{7}$$

Dunque, possedere $\phi(N)$, significa poter fattorizzare N:

$$\begin{cases} p+q = A \\ p-q = \sqrt{A^2-4N} \end{cases} \implies \begin{cases} p = \frac{(p+q)+(p-q)}{2} \\ q = \frac{(p+q)-(p-q)}{2} \end{cases}$$

Mentre l'implicazione inversa è diretta conseguenza del lemma 2. ■

⇛ Del resto, conoscere $\phi(N)$, permette di rompere l'RSA anche senza fattorizzare N: è sufficiente calcolare d come inverso moltiplicativo di e in $\mathbb{Z}^*_{\phi(N)}$.

Radice e-esima. Come mostrato dalla Enc_k, per rompere l'RSA sarebbe sufficiente risolvere il *Root Finding Problem* (*RFP*), ovvero ricavare la radice e-esima del crittogramma: $m \equiv_N \sqrt[e]{c}$. Chiaramente, se la radice e-esima di c è data, m può essere calcolato in tempo polinomiale: $RFP(c) \overset{\mathcal{P}}{\Rightarrow} \{m\}$.

Dal momento che $\mathcal{M}=\mathbb{Z}^*_N$ è un insieme finito numerabile si potrebbe pensare di trovare m per forza bruta, ma nella pratica, con grandi valori di N, questo è impossibile. Tuttavia, se *Oscar* fosse a conoscenza di $\phi(N)$, potrebbe calcolare $\sqrt[e]{c}$ modulo N in tempo polinomiale.

Teorema 4.

$$\phi(N) \overset{\mathcal{P}}{\Longrightarrow} RFP(c) \tag{8}$$

Dimostrazione. Con $\phi(N)$ noto, sapendo che e, d sono inversi in $\mathbb{Z}^*_{\phi(N)}$, dall'equazione diofantea

$$ed - k\phi(N) = 1, \quad k\in\mathbb{Z}$$

posso determinare d e k in tempo polinomiale usando l'*Algoritmo di Euclide esteso*[1] e quindi ricavare il messaggio m:

$$m^e \equiv \big(c^d\big)^e = c^{1+k\phi(N)} \equiv c \pmod N$$

■

[1] L'Algoritmo di Euclide è più che una efficiente tecnica per determinare il massimo comun divisore tra due interi, fornisce un metodo per scrivere l'*Identità di Bezout*: da qui il termine esteso.

L'algoritmo è inoltre intimamente connesso con le frazioni continue (oggetto dell'*Attacco di Wiener*). Dati x,y interi coprimi, per l'Identità di Bezout $ax+by=1$, quindi posso scrivere:

$$\frac{x}{y} = 0 + \cfrac{1}{\beta_1 + \cfrac{1}{\ddots + \cfrac{1}{\beta_{n-1} + \cfrac{1}{\beta_n}}}}$$

dalla quale ricavo $\{0, \frac{1}{\beta_1}, \cdots, \frac{\widetilde{x}}{\widetilde{y}}, \frac{x}{y}\}$ detti *convergenti*, che mi permettono facilmente di calcolare a e b:

$$\begin{aligned} a &= (-1)^{n-1}\widetilde{y} \\ b &= (-1)^{n-1}\widetilde{x} \end{aligned}$$

È interessante osservare che, i calcoli effettuati nello sviluppo in **frazione continua regolare** di x/y, sono identici a quelli necessari all'Algoritmo di Euclide per il calcolo di $MCD(x,y)$.

La serie dei quozienti che occorrono nell'Algoritmo di Euclide coincide con quella dei **denominatori parziali** nell'espansione in frazione continua; questo è molto utile per una efficiente soluzione di equazioni diofantee lineari.

Modulo comune. La quadrupla $(d, p, q, \phi(N))$ rappresenta la funzione *One-Way Trapdoor* dell'RSA: conoscere uno dei componenti, significa svelare anche gli altri e quindi essere in grado di rompere il crittogramma. Un uso improprio dell'RSA, come il molteplice utilizzo del medesimo modulo N in Enc_k, potrebbe però renderlo ugualmente vulnerabile senza la necessità di conoscere $(d, p, q, \phi(N))$.

Teorema 5. *Siano $e_1 \neq e_2$ esponenti coprimi, N ed $m_1 = m_2$ modulo e messaggi tali che $\begin{cases} c_1 \equiv_N m_1^{e_1} \\ c_2 \equiv_N m_2^{e_2} \end{cases}$. Allora il messaggio può essere recuperato in tempo polinomiale:*

$$((c_1, e_1, N), (c_2, e_2, N)) \xRightarrow{\mathcal{P}} \{m\} \tag{9}$$

Dimostrazione. Dall'ipotesi $MCD(e_1, e_2) = 1$ ricavo l'equazione diofantea $e_1 x + e_2 y = 1$ che può essere risolta in tempo polinomiale con l'Algoritmo di Euclide esteso (o equivalentemente mediante frazioni continue). Quindi:

$$c_1^x c_2^y \equiv \left(m_1^{e_1}\right)^x \left(m_2^{e_2}\right)^y = m^{e_1 x + e_2 y} \equiv m \pmod N$$

■

Come precedentemente accennato, il nostro obiettivo è mostrare che esistono attacchi al crittosistema che recuperano il messaggio senza la necessità di fattorizzare il modulo. Cionondimeno alcuni interi sono particolarmente facili da fattorizzare; per esempio moduli per cui $p-1$ è prodotto di primi $p_i < B \in \mathbb{N}$, sono fattorizzabili in tempo $t < B^3$.

È necessario dunque conoscere la fattorizzazione di N per calcolare efficientemente la e-esima radice del crittogramma?

Problema aperto 1. *Dato un modulo N, un esponente pubblico e ed una funzione $f_{e,N}$ così definita:*

$$f_{e,N} : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$$
$$c \to \sqrt[e]{c}$$

Esiste un algoritmo tempo-polinomiale che calcola la fattorizzazione di N?

Punto-Fisso. Quest'ultimo attacco elementare, chiamato anche *attacco ciclico* o *superencryption attack*, fu scoperto da Simmons e Norris nel 1977 poco dopo la famosa pubblicazione di Rivest, Shamir e Edleman [3]. L'attacco sul punto-fisso non fa uso della fattorizzazione di N, nè di qualsiasi informazione riguardo la funzione *One-Way Trapdoor*.

Teorema 6. *Sia c punto-fisso ordine k di $RSA(e, N)$. Allora:*

$$c^{(e^{k-1})} \equiv m \pmod N \tag{10}$$

Dimostrazione. Dal momento che Enc_k è una permutazione su $\mathcal{M}$, un intero c che soddisfi (10) esiste:

$$\left(c^{(e^{k-1})}\right)^e = c^{(e^k)} \underset{def4}{\boxed{\equiv}} c \underset{Enc_k}{\boxed{\equiv}} m^e \implies c^{(e^{k-1})} \equiv m \pmod N$$

■

Il Teorema 6 fornisce dunque un diretto attacco all'RSA semplicemente calcolando la successione di interi il cui penultimo elemento è proprio il messaggio cercato:

$$\begin{array}{cccccc} c^e, & c^{(e^2)}, & \ldots, & c^{(e^{k-1})}, & c^{(e^k)} & \pmod N \\ & & & \Uparrow & \Downarrow & \\ & & & m & c & \end{array}$$

Definizione 4 (Punto-Fisso). *Sia $0 \leq x < N$, $x \in \mathcal{C}$. Se $x^{(e^k)} \equiv_N x$ e $k \in \mathbb{Z}^+$, allora x è chiamato punto-fisso ordine k del crittosistema $RSA(e, N)$.*

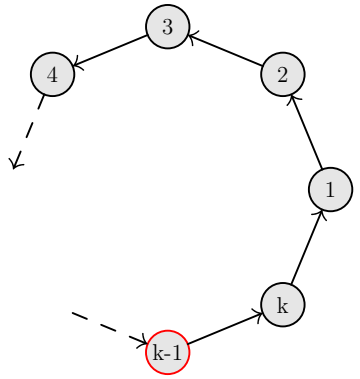


Figura 3: attacco punto-fisso. Il $k-1$ esimo elemento della serie è m.

Attacco di Wiener

Per velocizzare il calcolo della funzione di decifrazione Dec_k, è abitudine usare un esponente privato d piccolo, soprattutto in dispositivi dalle risorse limitate come le smartcards. Sfortunatamente però un attacco suggerito da Michael Wiener nel 1989 [4], basato sulle *frazioni continue*, dimostra che scegliere d piccolo, comporta un sistema altamente insicuro dove tutte le informazioni segrete possono essere recuperate. In particolare:

$$(e, N) \xrightarrow[d \text{ piccolo}]{\mathcal{P}} \{d\}$$

Usando il *Teorema di Legendre* sulle approssimazioni diofantee della forma $|\gamma - \frac{a}{b}| < \frac{1}{2b^2}$, l'Attacco mostra che se $d < \sqrt[4]{N}$, i convergenti dell'espansione in frazione continua di e/N (che ne approssimano il valore), sono della forma k/d.

Quindi è immediato che d possa essere calcolato efficientemente a partire dalla chiave pubblica (e, N).

Il ruolo dei convergenti

I convergenti di una frazione continua regolare sono strettamente correlati al suo valore γ e giocano un ruolo fondamentale nell' Attacco di Wiener. Dunque, come calcolarli?

Teorema 7. *Data la frazione continua regolare*

$$\gamma = \beta_0 + \cfrac{1}{\beta_1 + \cfrac{1}{\ddots + \cfrac{1}{\beta_{n-1} + \cfrac{1}{\beta_n}}}} = [\, \beta_0;\ \beta_1,\ \ldots\ , \beta_{n-1},\ \beta_n \,]$$

e definiti due interi positivi a_i, b_i ($i = -1 \ldots n$) tali che

$$a_i = \begin{cases} 1 & \text{se } i = -1 \\ \beta_0 & \text{se } i = 0 \\ \beta_i a_{i-1} + a_{i-2} & \text{se } 1 \le i \le n \end{cases} \qquad b_i = \begin{cases} 0 & \text{se } i = -1 \\ 1 & \text{se } i = 0 \\ \beta_i b_{i-1} + b_{i-2} & \text{se } 1 \le i \le n \end{cases}$$

Definizione 5 (Frazione Continua)**.** *Una frazione continua finita è una espressione della forma*

$$\gamma = \beta_0 + \cfrac{\alpha_1}{\beta_1 + \cfrac{\alpha_2}{\ddots + \cfrac{\alpha_{n-1}}{\beta_{n-1} + \cfrac{\alpha_n}{\beta_n}}}}$$

con α_i, β_i ($i = 1 \ldots n \in \mathbb{Z}^+$) detti numeratori e denominatori parziali, γ valore.
*La frazione è chiamata **regolare** se $\beta_0 \in \mathbb{Z}$, $\alpha_i = 1$, $\beta_i \in \mathbb{Z}^+$ ($i = 1 \ldots n$). Una frazione regolare sarà dunque esprimibile come sequenza dei propri denominatori parziali:*

$$\gamma = [\, \beta_0;\ \beta_1,\ \beta_2,\ \ldots\ , \beta_n \,]$$

Definizione 6 (Convergente)**.** *Per $0 \le i \le n$, si definisce i-esimo convergente di γ la frazione $c_i = [\beta_0; \beta_1, \beta_2, \ldots, \beta_i]$.*

Si ricordi che, come previsto nel *PKCS* #1, gli esponenti e, d, sono inversi in $\mathbb{Z}^*_{\lambda(N)}$:

$$0 < k = \frac{ed - 1}{\lambda(N)} < \frac{ed}{\lambda(N)} < min\{e, d\}$$

Le specifiche ***PKCS*** (Public Key Cryptography Standards), attualmente prodotte dagli RSA-Laboratories in collaborazione con esperti di sicurezza di tutto il mondo, hanno l'obiettivo di accelerare lo sviluppo della crittografia a chiave pubblica.

Pubblicate nel 1991 ad un incontro dei primi utilizzatori delle tecnologie a chiave pubblica, sono divenute un importante ed aggiornato riferimento per chiunque. Tra i moderni standard che fanno uso delle *PKCS* si ricordano *SSL/TLS* e *WAP/WTLS*.

Nello specifico, la famiglia delle *PKCS* #1 fornisce definizioni di base e accorgimenti di sicurezza per l'implementazione del crittosistema *RSA*. [10]

Lemma 4. *Sia $k\in\mathbb{Z}^+$. La successione dei convergenti pari $\{c_i\}_{i=2k}$ è monotona strettamente crescente, mentre la $\{c_i\}_{i=2k+1}$ dei dispari è monotona strettamente decrescente.*

Dimostrazione. Partendo da (13) e usando a_i, b_i definiti in (12), posso ottenere la seguente uguaglianza:

$$a_ib_{i-2}-a_{i-2}b_i=(-1)^i\beta_i \quad \xrightarrow[\text{per } b_ib_{i-2}]{\text{e se divido}} \quad c_i-c_{i-2}=(-1)^i\tfrac{\beta_i}{b_ib_{i-2}}$$

Quindi la differenza tra due convergenti dispari (pari) consecutivi avrà sempre segno negativo (positivo). ■

Lemma 5. *Ogni convergente $c\in\{c_i\}_{i=2k+1}$ è maggiorante di $\{c_i\}_{i=2k}$.*

Dimostrazione. Analogamente alla precedente, dividendo per $-b_ib_{i-1}$ entrambi i membri di (13), si ottiene:

$$c_i-c_{i-1}=\tfrac{(-1)^{i-1}}{b_ib_{i-1}}$$

Segue che la differenza tra due convergenti consecutivi c_i e c_{i-1} avrà sempre segno $(-1)^{i-1}$. Quindi, per $\mu\in\mathbb{Z}^+$:

$$c_{2\mu+1}>c_{2\mu} \tag{11}$$

Se, per assurdo, la tesi fosse falsa, dati $\mu,\eta\in\mathbb{Z}^+$, risulterebbe:

$$c_{2\mu+1}\le c_{2\eta}\Rightarrow\begin{cases}c_{2\mu+1}<c_{2\mu} & \text{se } \eta<\mu\\ c_{2\eta+1}<c_{2\eta} & \text{se } \eta>\mu\end{cases}$$

in contraddizione con (11). ■

Lemma 6. *γ è maggiorante di $\{c_i\}_{i=2k}$ e minorante di $\{c_i\}_{i=2k+1}$.*

Dimostrazione. $\gamma=c_n$, per qualsiasi valore di n, risulterà il maggiore dei convergenti pari, o il minore di quelli dispari: la tesi sarà vera in entrambi i casi. ■

I Lemmi 4, 5, 6 mostrano che γ di una frazione continua finita regolare è equivalente ad un numero razionale ed i suoi convergenti ne sono un'approssimazione. Ai fini dell'Attacco però è utile sapere il viceversa: ***un numero razionale x/y è esprimibile come una frazione continua finita regolare.***

La dimostrazione è piuttosto semplice e, come accennato, ruota attorno all'Algoritmo di Euclide esteso: trovato $MCD(x,y)$, si divide ciascuna equazione dell'algorirmo per il resto al passo precedente, così da individuare razionali espressi come somma di un intero e un razionale; fatto ciò, tramite eliminazioni successive, è immediato ottenere x/y nella forma desiderata.

l'i-esimo convergente c_i può essere calcolato ricorsivamente:

$$c_i=\frac{a_i}{b_i}=\frac{\beta_ia_{i-1}+a_{i-2}}{\beta_ib_{i-1}+b_{i-2}} \tag{12}$$

Dimostrazione. Procedendo per induzione, il passo base (i=1) risulta:

$$c_1=\frac{a_1}{b_1}=\beta_0+\frac{1}{\beta_1}=\frac{\beta_0\beta_1+1}{\beta_1}=\frac{\beta_1a_0+a_{-1}}{\beta_1b_0+b_{-1}}$$

mentre il passo induttivo ($i\Rightarrow i+1$) è verificabile osservando che il convergente c_{i+1} può essere costruito da c_i sostituendo β_i con $\beta_i+\frac{1}{\beta_{i+1}}$:

$$c_{i+1}=\frac{a_{i+1}}{b_{i+1}}=\frac{(\beta_i+\frac{1}{\beta_{i+1}})a_{i-1}+a_{i-2}}{(\beta_i+\frac{1}{\beta_{i+1}})b_{i-1}+b_{i-2}}=\frac{\overbrace{\beta_ia_{i-1}+a_{i-2}}^{a_i}+\frac{a_{i-1}}{\beta_{i+1}}}{\underbrace{\beta_ib_{i-1}+b_{i-2}}_{b_i}+\frac{b_{i-1}}{\beta_{i+1}}}=$$

$$=\frac{a_i+\frac{a_{i-1}}{\beta_{i+1}}}{b_i+\frac{b_{i-1}}{\beta_{i+1}}}=\frac{\beta_{i+1}a_i+a_{i-1}}{\beta_{i+1}b_i+b_{i-1}}$$

■

Il Teorema 7 suggerisce dunque come approssimare una frazione continua regolare con un numero razionale e fornisce un semplice algoritmo per calcolarne i convergenti; chi ci assicura però che questi siano già ridotti ai minimi termini?

Lemma 7. *Gli interi a_i, b_i definiti nel Teorema 7 soddisfano*

$$a_{i-1}b_i-a_ib_{i-1}=(-1)^i \tag{13}$$

Dimostrazione.

$$(i=0)\quad a_{-1}b_0-a_0b_{-1}=(-1)^0$$
$$(i\Rightarrow i+1)\quad a_ib_{i+1}-a_{i+1}b_i=a_i(b_i\beta_{i+1}+b_{i-1})-(a_i\beta_{i+1}+a_{i-1})b_i=$$
$$=-(a_{i-1}b_i-a_ib_{i-1})=(-1)^{i+1}$$

■

Dal Lemma 7 segue quindi che tutti i convergenti c_i (i=0...n) sono ridotti ai minimi termini perchè $MCD(a_i,b_i)>1$ appare sicuramente come divisore di $a_{i-1}b_i-a_ib_{i-1}$.

Approssimare γ. Nella teoria generale, uno dei motivi d'importanza della rappresentazione dei numeri mediante frazioni continue risiede nel fatto che i relativi convergenti forniscono la migliore approssimazione possibile di un irrazionale mediante razionali. Benchè interessante, per i nostri scopi la rappresentazione di irrazionali non è rilevante ma i risultati generali possono essere usati anche per lo sviluppo in frazioni continue di razionali.

Teorema 8. *Sia $a,b\in\mathbb{Z}^+$, $\gamma=[\beta_0;\beta_1,\dots,\beta_n,\beta_{n+1},\dots]$ frazione continua regolare[2] e $\{c_i\}_{i\in\mathbb{N}}$ l'insieme dei convergenti di γ. Se*

$$|\gamma b-a| < |\gamma b_n-a_n| \tag{14}$$

allora $b\geq b_{n+1}$. Inoltre, se

$$\left|\gamma-\frac{a}{b}\right| < |\gamma-c_n| \tag{15}$$

allora $b>b_n$. In altri termini ogni convergente $c_n=a_n/b_n$ approssima γ meglio di qualunque frazione il cui denominatore non superi b_n.

Dimostrazione. Data l'ipotesi (14), supponendo per assurdo $b<b_{n+1}$, si consideri la seguente implicazione per qualche $x,y\in\mathbb{Z}$:

$$\begin{cases} a_n x+a_{n+1}y = a \\ b_n x+b_{n+1}y = b \end{cases} \xRightarrow[(13)]{} \begin{cases} x = (-1)^n(a_{n+1}b-ab_{n+1}) \\ y = (-1)^n(ab_n-a_n b) \end{cases}$$

con x,y tali che

$$x\neq 0 \xrightarrow{\textit{altrimenti}} b=b_{n+1}y\geq b_{n+1}$$
$$y\neq 0 \xrightarrow{\textit{altrimenti}} \begin{cases} a=a_n x \\ b=b_n x \end{cases} \Rightarrow |\gamma b-a|=|x||\gamma b_n-a_n|\geq|\gamma b_n-a_n|$$

Inoltre è utile dimostrare che x e y hanno effettivamente segni opposti:

$$\text{se } y<0 \implies b_n x=b-b_{n+1}y>0 \overset{b_n>0}{\Rightarrow} x>0$$
$$\text{se } y>0 \implies b_n x=b-b_{n+1}y<0 \overset{b_{n+1}y\geq b_{n+1}>b}{\Rightarrow} x<0$$

Adesso, dall'andamento oscillante dei convergenti mostrato nei Lemmi 4, 5 segue subito che γb_n-a_n e $\gamma b_{n+1}-a_{n+1}$ hanno segni opposti; pertanto $x(\gamma b_n-a_n)$ e $y(\gamma b_{n+1}-a_{n+1})$ hanno lo stesso segno. Quindi si può concludere:

$$\begin{aligned} |\gamma b-a| &= |\gamma(b_n x+b_{n+1}y)-(a_n x+a_{n+1}y)| \\ &= |x||\gamma b_n-a_n|+|y||\gamma b_{n+1}-a_{n+1}| \\ &\geq |\gamma b_n-a_n| \end{aligned}$$

che però nega l'ipotesi (14). Questo dimostra la prima tesi del teorema. Presa ora in considerazione l'ipotesi (15) e supposto per assurdo $b\leq b_n$, troviamo nuovamente l'ipotesi (14):

$$b\left|\gamma-\frac{a}{b}\right| < b_n|\gamma-c_n|$$

Questo suggerisce $b_n\geq b\geq b_{n+1}$ che però contraddice (12). ■

Teorema 9 (Legendre). *Sia $a,b\in\mathbb{Z}^+$, $\gamma=[\beta_0;\beta_1,\dots,\beta_n,\beta_{n+1},\dots]$ frazione continua regolare[2] e $\{c_i\}_{i\in\mathbb{N}}$ l'insieme dei convergenti di γ. Se*

$$\left|\gamma-\frac{a}{b}\right| < \frac{1}{2b^2} \tag{16}$$

allora $\frac{a}{b}\in\{c_i\}_{i\in\mathbb{N}}$.

[2] Sono usate **frazioni continue infinite**. Queste hanno stessa struttura delle finite ma un numero infinito di denominatori parziali e sono molto utili per l'approssimazione di irrazionali.

Nel calcolo di $\sqrt{2}$ mediante convergenti, qual'è l'errore commesso?

Dall'espansione in frazione continua regolare si ottiene che $\sqrt{2}=[1;\overline{2}]$; quindi l'insieme dei convergenti risulterà:

$$\{c_i\}_{i\in\mathbb{N}} = \left\{1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \dots\right\}$$

Scelto di approssimare $\sqrt{2}$ con $c_2=7/5$, l'errore $\mathcal{E}$ che si commette è pari a $|\sqrt{2}-c_2|<|c_3-c_2|=0.01\overline{6}$. Adesso, usando la tesi del Teorema 8, è possibile mostrare che ogni frazione con denominatore minore di 5 commette un errore maggiore di $\mathcal{E}$.

Considerato $1<\sqrt{2}<2$, l'insieme dei possibili razionali sarà $\{\frac{5}{4}, \frac{7}{4}, \frac{4}{3}, \frac{5}{3}, \frac{3}{2}\}$, dal quale sono subito eliminabili $5/4$ e $4/3$ perchè minori di c_2, sottostima di $\sqrt{2}$. Successivamente è sufficiente mostrare che per il minore dei rimanenti ($3/2$), vale la seguente disuguaglianza:

$$\left|\sqrt{2}-\frac{3}{2}\right| > \left|\frac{3}{2}-c_2\right| = 0.18\overline{3} > \mathcal{E}$$

Quindi $7/5$ è effettivamente la miglior approssimazione razionale di $\sqrt{2}$ con denominatore minore o uguale a 5.

Dimostrazione. Supponiamo per assurdo che $\frac{a}{b} \notin \{c_i\}_{i\in\mathbb{N}}$, sarà sempre possibile trovare due convergenti c_n, c_{n+1} tali che $b_n \leq b < b_{n+1}$[3]. Quindi, per il Teorema 8:

$$|\gamma b_n - a_n| \leq |\gamma b - a| = b\left|\gamma - \tfrac{a}{b}\right| < \tfrac{1}{2b} \quad \Rightarrow$$
$$\Rightarrow \quad |\gamma - c_n| < \tfrac{1}{2bb_n}$$

Poichè la tesi è negata per assurdo, $|a_n b - a b_n| \geq 1$. Dunque:

$$\tfrac{1}{bb_n} \leq \tfrac{|a_n b - a b_n|}{bb_n} = \left|c_n - \tfrac{a}{b}\right| \leq |\gamma - c_n| + \left|\gamma - \tfrac{a}{b}\right| < \tfrac{1}{2bb_n} + \tfrac{1}{2b^2} \quad \Rightarrow$$
$$\Rightarrow \quad \tfrac{1}{2bb_n} < \tfrac{1}{2b^2}$$

che implica $b_n > b$ contrario all'ipotesi. ■

[3] La proposizione è facilmente verificabile: se per assurdo fosse falsa, tutti i convergenti avrebbero lo stesso denominatore ma questo è impossibile perchè contraddirebbe il Teorema 7.

Adesso che anche il Teorema di Legendre è stato definito, è finalmente possibile esporre il classico attacco alla chiave privata ideato da Wiener nel 1989; vedremo come la disuguaglianza (16) sia un fondamentale tassello nella dimostrazione dell'Attacco.

Attacco classico

Figura 4: Un classico attacco.

Come già introdotto all'inizio del capitolo, data semplicemente la chiave pubblica (e, N), Wiener fattorizza il modulo N usando le informazioni ottenute da uno dei convergenti nell'espansione di e/N. Il miglior modo per procedere è dunque esprimere l'Attacco, nella sua forma più generale, con il seguente teorema.

Teorema 10 (Wiener). *Sia $N=pq$ un modulo RSA e siano $e, d \in \mathbb{Z}^*_{\lambda(N)}$ i relativi esponenti pubblico e privato. Se d soddisfa la seguente ipotesi:*

$$d < \frac{pq}{2(p+q-1)k_0 g_0} = \frac{N}{2\big(N-\phi(N)\big)k_0 g_0} \tag{17}$$

$$\text{con} \quad \begin{aligned} k &= k_0\, MCD(k,g) = {}^{(ed-1)}/_{\lambda(N)} && \in \mathbb{Z}^+ \\ g &= g_0\, MCD(k,g) = MCD(p-1, q-1) && \in \mathbb{Z}^+ \end{aligned}$$

allora N può essere fattorizzato in tempo polinomiale in $\mathcal{O}\big(log_2(N)\big)$.

Dimostrazione. Usando una proprietà del massimo comun divisore[4] è possibile riscrivere il prodotto dei due esponenti ed come:

$$\begin{cases} \phi(N) = g\lambda(N) \\ ed = 1 + k\lambda(N) \end{cases} \quad \Rightarrow \quad ed = 1 + \frac{k}{g}\phi(N) \tag{18}$$

Adesso sarà sufficiente dividere entrambi i lati per dN e usare l'ipotesi (17) per ottenere la seguente disuguaglianza:

$$\left|\frac{e}{N} - \frac{k_0}{dg_0}\right| = \left|\frac{1}{dN} - \frac{k_0}{dg_0}\,\frac{N-\phi(N)}{N}\right| < \frac{k_0}{dg_0}\,\frac{N-\phi(N)}{N} < \frac{1}{2(dg_0)^2}$$

[4] Il prodotto di due interi x, y è pari al prodotto del loro massimo comun divisore e minimo comune multiplo:

$$xy = MCD(x,y)\, mcm(x,y)$$

nel nostro caso $x=p-1$, $y=q-1$ e $\lambda(N)$ è il loro minimo comune multiplo.

Come preannunciato, si noti l'assonanza tra l'ipotesi (16) del Teorema di Legendre e la disuguaglianza appena ricavata:

$$\left|\gamma-\frac{a}{b}\right|<\frac{1}{2b^2} \quad \rightsquigarrow \quad \left|\frac{e}{N}-\frac{k_0}{dg_0}\right|<\frac{1}{2(dg_0)^2} \tag{19}$$

Pertanto, per il Teorema 9, **$c=\frac{k_0}{dg_0}$ sarà uno degli n convergenti dell'espansione in frazione continua di e/N**. Usando (18), non rimane che calcolare $\phi(N)$ necessario per la fattorizzazione del modulo:

$$\phi(N)=e\underbrace{\frac{dg_0}{k_0}}_{b/a}-\frac{g_0}{k_0}=\left\lfloor\frac{e}{c}\right\rfloor-\left\lfloor\frac{g_0}{k_0}\right\rfloor$$

Questo garantisce la possibilità di calcolare $\phi(N)$ conoscendo il corretto convergente c, ovvero ricavare in tempo polinomiale $IFP(N)$ come mostrato nel Teorema 3. I possibili candidati risulteranno dunque della forma $\lfloor e/c\rfloor-m$. Fissato un intero m, sarà sufficiente iterare sulla lista dei convergenti e per ciascun candidato provare a fattorizzare il modulo N; se la ricerca fallisse, il processo verrà ripetuto con $m+1$.

Dal momento che la cardinalità di $\{c_i\}_{i\leq n}$ è polinomiale in $log_2(N)$ e il valore di m non può superare $\lfloor g/k\rfloor$, il costo totale della ricerca avrà al più ordine $\Theta\big(log_2(N)\big)$. ■

Input: insieme $\{c_i\}_{i\leq n}$ dei convergenti dell'espansione di e/N.

```
    m←0
LOOPm:
    i←0
LOOPi:
    if (e/ci−m) ⇒IPF(n) then
        return ci
    if i≤n then
        i←i+1
        goto LOOPi
    if m≤⌊g/k⌋ then
        m←m+1
        goto LOOPm
```

Output: i-esimo convergente c_i, utile alla fattorizzazione di N.

Figura 5: Frammento di pseudocodice per la ricerca del corretto convergente.

Analisi di efficienza. Riguardo l'algoritmo descritto, benchè questo rispetti la tesi del Teorema 10, in certi casi è possibile ottimizzarne la resa riducendo la cardinalità dell'insieme $\{c_i\}_{i\leq n}$ in input.

Nello specifico, tutti i convergenti c_i per cui $|e/N-c_i|$ non rispetta (19), possono essere scartati a priori. Inoltre, se p,q sono primi bilanciati scelti casualmente, la probabilità che g sia piccolo è alta.

	Lunghezza binaria p,q						
g	**128**	**256**	**384**	**512**	**1024**	**Media**	**Percentile**
2	49.5	49.7	49.8	49.5	49.5	49.6	49.6
4	12.4	12.4	12.4	12.3	12.4	12.4	62.0
6	14.7	14.6	14.6	14.7	14.8	14.7	76.7
8	3.1	3.1	3.0	3.2	3.2	3.1	79.8
10	3.1	3.2	3.1	3.2	3.1	3.2	83.0
12	3.8	3.5	3.6	3.5	3.6	3.6	86.6
14	1.4	1.3	1.4	1.3	1.4	1.4	88.0
16	0.7	0.7	0.8	0.8	0.8	0.8	88.8
18	1.6	1.6	1.6	1.7	1.6	1.6	90.4
20	0.7	0.7	0.8	0.8	0.8	0.8	91.2

Distribuzione di probabilità di $g=MCD(p-1,q-1)$ per primi p,q casuali, della stessa lunghezza. I risultati sono dati in percentuale e comprendono i percentili totali.

Definizione 7 (Primi Bilanciati). *Con primi bilanciati si intendono due primi p,q circa della stessa lunghezza binaria. In particolare, per un modulo RSA $N=pq$ si assumerà che:*

$$4<\frac{1}{2}\sqrt{N}<p<\sqrt{N}<q<2\sqrt{N}$$

o equivalentemente che $p<q<2p$ come da Postulato di Bertrand.

Dalla Definizione 7 si può dunque inferire che, quando p,q sono bilanciati, la funzione toziente di Eulero $\phi(N)$ soddisfi:

$$\begin{aligned}|N-\phi(N)| &= |N-(p-1)(q-1)|\\ &= |p+q-1|\\ &< 3\sqrt{N}\end{aligned}$$

Quindi N e $\phi(N)$ avranno circa metà dei loro bit più significativi in comune.

Una diretta conseguenza di quanto affermato è nuovamente la tesi del Postulato di Bertrand, ovvero $\phi(N)<N<2\phi(N)$.

Per esempio $\text{Prob}[g{\leq}6]\simeq 0.77$ e addirittura $\text{Prob}[g{\leq}20]\simeq 0.91$; pertanto è plausibile supporre $\lfloor g/k\rfloor{=}0$ e, di conseguenza, la necessità di una sola iterazione per la ricerca del convergente corretto.

Data la chiave pubblica di una istanza di *RSA* con esponente privato piccolo:

$$(e,N) = (58549809, 2447482909)$$

l'espansione di e/N ed il relativo insieme di convergenti risulteranno:

$$\frac{e}{N} = [\,0;\,41,\,1,\,4,\,23,\,\dots\,]$$

$$\{c_i\}_{i\leq 15} = \left\{0,\ \frac{1}{41},\ \frac{1}{42},\ \frac{5}{209},\ \frac{116}{4849},\ \dots\right\}$$

Testando i convergenti con l'algoritmo di ricerca del Teorema di Wiener (per $m{=}0$), il quarto convergente $c_3{=}5/209$ fornisce il giusto candidato $\widetilde{\phi}$ per $\phi(N)$:

$$\left\lfloor \frac{e}{c_3} \right\rfloor = \left\lfloor \frac{58549809}{5/209} \right\rfloor = 2447382016$$

$\widetilde{\phi}$ permette così di risolvere (7) e ottenere $p{=}60317$, $q{=}40577$ fattori primi di N. La condizione di sufficienza (17) dell'Attacco di Wiener è soddisfatta:

$$d = 209 < \frac{N}{2(N-\phi(N))g_0k_0} \approx 2426$$

Contromisure. La condizione di sufficienza (17) del Teorema 10 non è l'ipotesi che spesso in Letteratura è associata all'Attacco di Wiener; più semplicemente, dato $\omega{>}1$, è detto *Limite di Wiener* il valore:

$$d < \frac{1}{\omega}\sqrt[4]{N} \tag{20}$$

Esso è ottenuto assumendo l'esponente pubblico della stessa lunghezza binaria del modulo, primi bilanciati e g_0 piccolo.

Usando quindi moduli da 2048b, d dovrà avere almeno 512b per scongiurare l'Attacco. Questo potrebbe essere complicato da realizzare in dispositivi a bassa potenza dove sono preferibili esponenti privati piccoli per una veloce decifrazione. Alcuni accorgimenti riescono tuttavia a coprire questo inconveniente, decrementando il Limite di Wiener indebolendo così l'Attacco:

① utilizzo di primi non bilanciati per incrementare il valore $N{-}\phi(N)$;
② scelta dei primi p,q tali da ottenere g grande (tipico della variante *Common Prime RSA*);
③ scelta di $e{>}N$ tale che $k{\approx}ed/N$: un tale esponente è facilmente ricavabile sommandone uno preesistente con un multiplo di $\lambda(N)$ (difatti, se $e{>}N^{3/2}$ l'Attacco non fornisce garanzie).

Pertanto, dal punto ③ è possibile concludere che **esponenti pubblici grandi indeboliscono l'Attacco** mentre quelli piccoli lo rafforzano.

Una ulteriore tecnica per inibire l'Attacco mantenendo una veloce decifrazione è usare il *Teorema Cinese dei Resti* per spezzare la congruenza modulo $\phi(n)$:

$$\begin{array}{l}\text{scegliere } d \text{ tale che}\\ \exists\, d_p, d_q \text{ piccoli: nel}\\ \text{nostro caso } {\approx}256\text{b}\end{array} \begin{cases} d_p \equiv_{p-1} d \\ d_q \equiv_{q-1} d \end{cases} \xrightarrow{\begin{array}{c}\text{che comporta la}\\ \text{seguente } Dec_k\end{array}} \begin{cases} m \equiv_p m_p \equiv_p c^{d_p} \\ m \equiv_q m_q \equiv_q c^{d_q} \end{cases}$$

ottenendo $m{\equiv_N}c^d$ come nella Dec_k classica. Dunque, sebbene d_p, d_q siano piccoli, N rimarrà ugualmente dell'ordine di $\mathcal{O}(\phi(N))$.

A conclusione, si consideri ora un *RSA* con p,q bilanciati, g_0 piccolo, $d{=}N^\delta$, $e{=}N^\sigma$ (con $0{<}\delta{<}1/2$ e $1/2{<}\sigma{<}1$). Usando (18) è facile ottenere $k{\approx}N^{\sigma+\delta-1}$ che, sostituito in (17) e dato $\nu{>}0$ causa approssimazioni, darà luogo a:

$$N^\delta < N^{1/2-(\sigma+\delta-1)-\nu}$$
$$\text{ovvero} \quad \delta < \tfrac{3}{4}-\tfrac{\sigma}{2}-\nu$$

Quindi, se $e{\approx}N$ allora $\sigma{\approx}1$ e $\delta{<}1/4$, proprio come previsto in (20); con e piccolo il limite incrementa fino ad un massimo di $\delta{=}1/2$ quando $\sigma{=}1/2$. Se invece $e{>}N$, il limite su δ decresce fino a svanire completamente quando $\sigma{=}3/2$, rendendo l'Attacco inefficiente.

Il Teorema di Wiener è stato migliorato nel 1998 da Boneh e Durfee ottimizzando il limite da imporre all'esponente privato [9]. I due matematici dimostrarono che la sicurezza di sfuggire ad un Attacco è garantita quando $d{<}N^{0.292}$.

Questo risultato mostra dunque che il Limite di Wiener non è stretto. È plausibile che quello corretto sia $\sqrt{N}$.

Problema aperto 2. *Sia $N{=}pq$, $d{<}\sqrt{N}$. Conoscendo la chiave pubblica (e,N), con $e{<}\phi(N)$, è possibile recuperare la chiave privata d in tempo polinomiale?*

Attacco esteso

Come argomentato, l'esito dell'Attacco classico dipende dal Limite di Wiener: se infatti capitasse $d{=}N^{0.25+\tau}$ ($\tau{>}0$), la probabilità di successo sarebbe pressochè insignificante. Tuttavia, uno scrupoloso crittoanalista potrebbe chiedersi se un esponente privato di lunghezza binaria maggiore di quella del Limite, possa essere sufficiente per eliminare qualsiasi informazione utile alla fattorizzazione del modulo. Nel 1997 Verheul e van Tilborg proposero una tecnica che risponde a questa domanda eseguendo una ricerca esaustiva su $2r{+}8$ bits, con r differenza tra le lunghezze dei due numeri ($r{=}log_2(d){-}log_2(\sqrt[4]{N})$) [7].

Figura 6: Niente da fare ...

L'osservazione principale risiede nel modo di rappresentare il convergente $c{=}{}^{k_0}/_{dg_0}$ di (19):

$$\frac{k_0}{dg_0} = \frac{Ua_{t+1} + (U\Delta{+}V)a_t}{Ub_{t+1} + (U\Delta{+}V)b_t} \tag{21}$$

$$\text{dove} \quad \begin{matrix} c_t = {}^{a_t}/_{b_t} \\ c_{t+1} = {}^{a_{t+1}}/_{b_{t+1}} \end{matrix} \quad \text{e} \quad \begin{matrix} log_2(U) \leq r{+}4 \\ log_2(V) \leq r{+}4 \end{matrix}$$

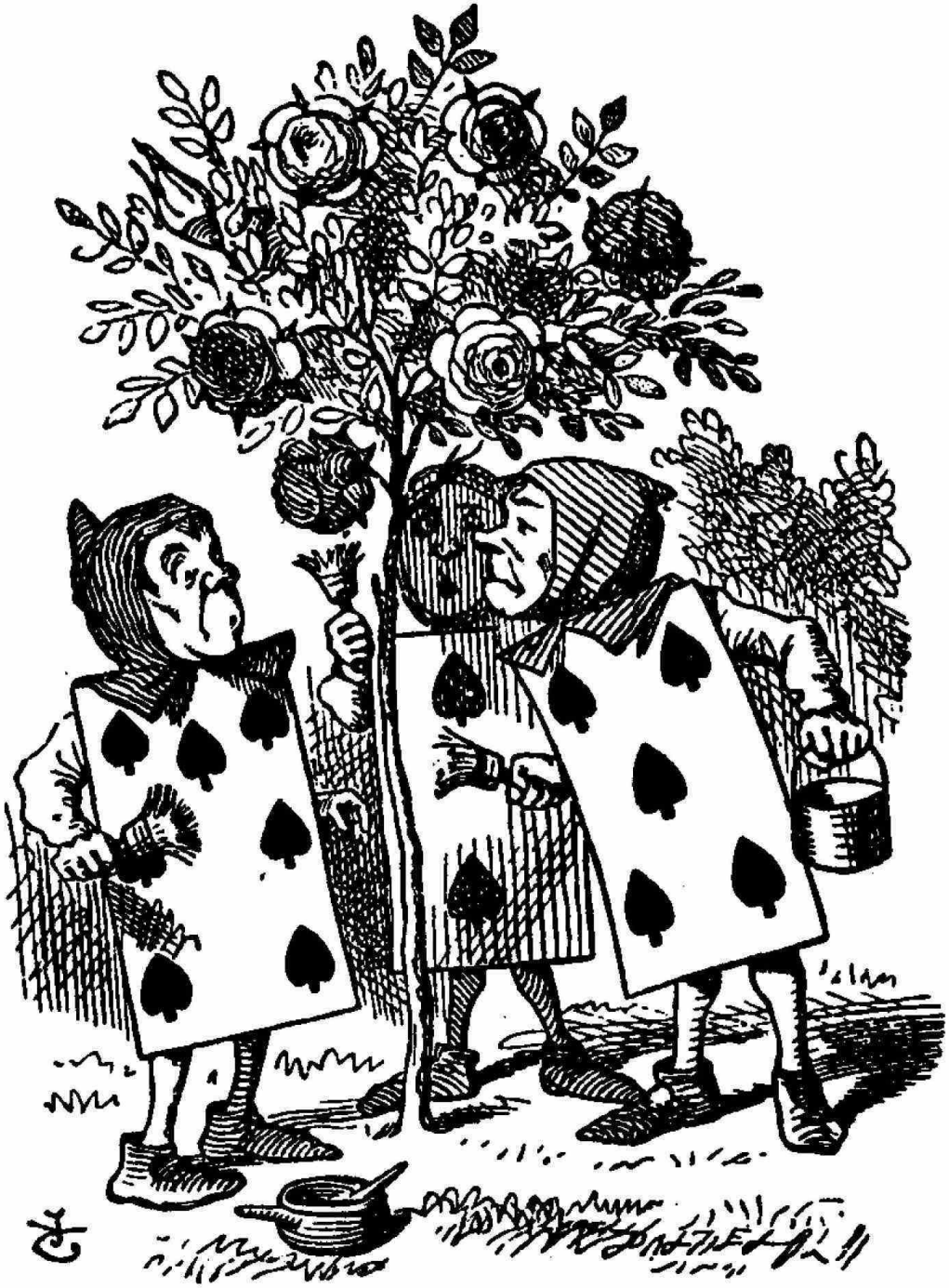
c_t, c_{t+1} rappresentano una specifica coppia di convergenti contigui dell'espansione in frazione continua di ${}^{e}/_{N}$, Δ una costante intera di dimensione trascurabile e U, V due variabili intere di lunghezza limitata. La parte incognita di (21) conterà pertanto un massimo di $2r{+}8$ bits. L'idea di Verheul e van Tilborg è **cercare, per ciascuna delle $n{-}1$ coppie di convergenti contigui, i corretti U, V fra le 2^{2r+8} possibilità** e calcolare così il relativo candidato di $\phi(N)$:

$$\widetilde{\phi} = \left\lfloor e\,\frac{dg_0}{k_0} \right\rfloor - m \qquad \begin{matrix} \text{con } m \text{ intero positivo analogo a} \\ \text{quello usato nell'Attaco classico} \end{matrix}$$

A fini pratici, poniamo adesso un limite alla nostra potenza di calcolo: si assuma una capacità computazionale tale da permettere una ricerca esaustiva su 64b. Per l'Estensione proposta $2r{+}8{=}64$, quindi il Limite di Wiener può essere esteso di 28b. Questo implica che una istanza dell'RSA con esponente privato piccolo $d{<}2^{28}\sqrt[4]{N}$ sia violabile con Brute-Force su 64b in aggiunta all'Attacco classico proposto da Wiener.

Nel 2004 Andrej Dujella ha migliorato ulteriormente l'Attacco esteso restringendo la ricerca dei corretti convergenti solamente a tre coppie [8].

Figura 7: Chiaramente, in alcuni casi l'Attacco di Wiener è pleonastico.



Appendice

Implementazione Attacco Classico in *Mathematica*®

```
e = 7502876735617; n = 28562942440499; (*esempio di chiave pubblica attaccabile*)
fc = ContinuedFraction[e/n];
cList = Convergents[fc];
phiList = Floor[e/Rest[cList]];
```

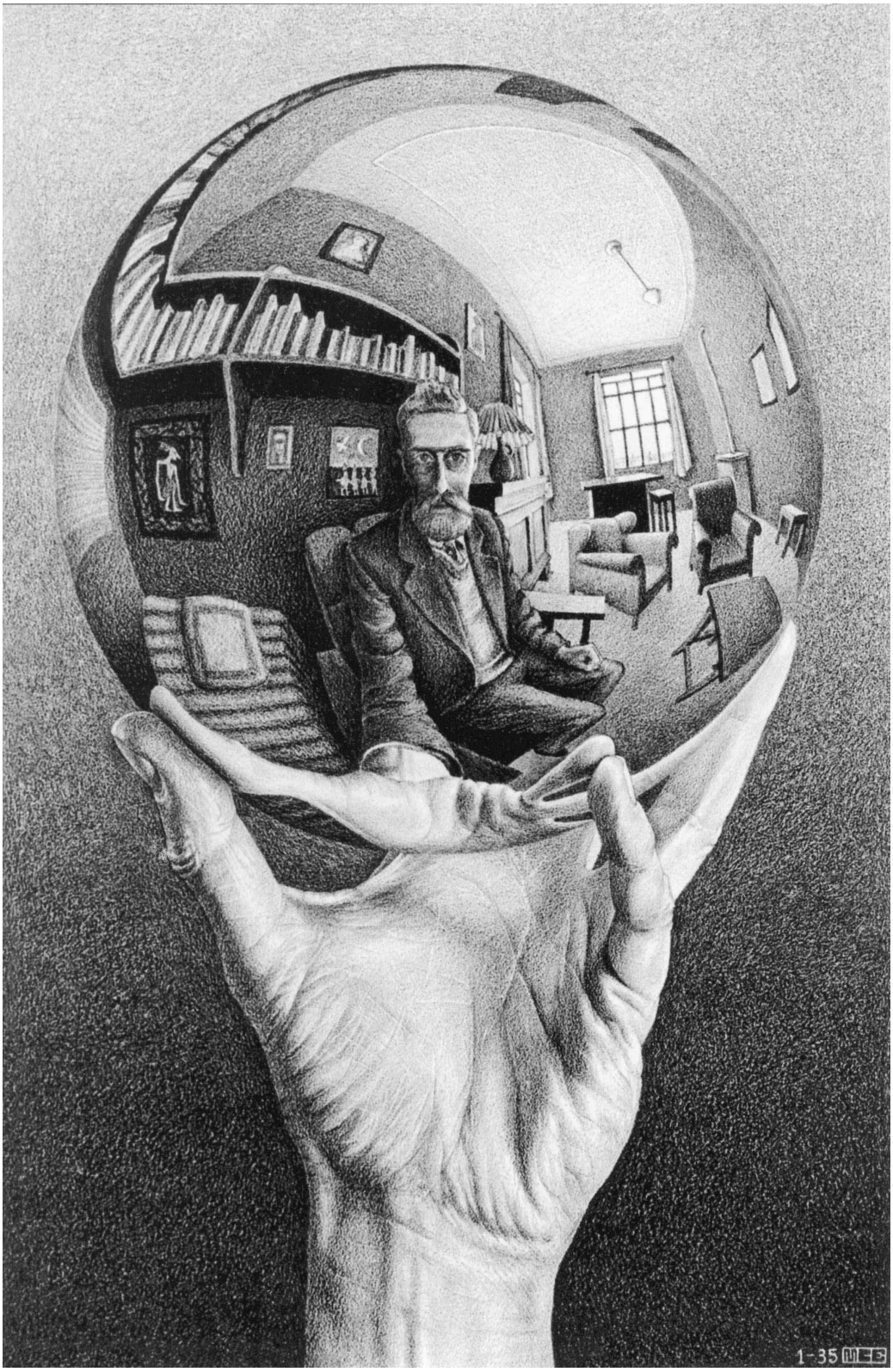
```
check[phi_] := (x/.p) /; (Mod[n,x] /. (p=Solve[x^2-(n-phi+1)x+n==0,x])) == {0, 0};
checkL[phi_List] := Flatten[Cases[check /@ phi,_List]];
```

```
primes = Flatten[checkL /@ (phiList-m /. {m->#}& /@ Range[0,9])];
```

Implementazione Attacco Esteso in *Mathematica*®

```
r = 4; Dl = 2; (*da regolare in base alle esigenze del caso*)
CClist = Partition[Rest[cList],2,1];
UVlist = Tuples[Range[2^r],2];
T = Tuples[{CClist,UVlist}];
phiList = Floor[
  e(T[[2,1]]Denominator[T[[1,2]]]+(T[[2,1]]Dl+T[[2,2]])Denominator[T[[1,1]]])/
   (T[[2,1]] Numerator[T[[1,2]]]+(T[[2,1]]Dl+T[[2,2]])Numerator[T[[1,1]]])];
```

```
primes = Flatten[checkL /@ (phiList-m /. {m->#}& /@ Range[0,9])];
```


1-35 MCE

Bibliografia

[1] W. Diffie, M. Hellman. *New Directions in Cryptography*. *IEEE Transactions on Information Theory, 1976*.

[2] R.L. Rivest, A. Shamir, L. Edleman. *A Method for Obtaining Digital Signature and Public-Key Cryptosystems*. *Commun. ACM, 1978*.

[3] G.J. Simmons, M.J. Norris. *Preliminary comments on the MIT public-key cryptosystem*. *Cryptologia, 1977*.

[4] M.J. Wiener. *Cryptanalysis of Short RSA Secret Exponents*. *IEEE Transactions on Information Theory, 1990*.

[5] D. Boneh. *Twenty years of attacks on the RSA cryptosystem*. *Notices of the American Mathematical Society, 1999*.

[6] M. Wu, C. Chen, Y. Lin, H. Sun. *On the Improvement of Wiener Attack on RSA with Small Private Exponent*. *Scientific World Journal, 2014*.

[7] E.R. Verheul, H.C.A. van Tilborg. *Cryptanalysis of 'less short' RSA secret exponent*. *Applicable Algebra in Engineering, Communications and Computing, 1997*.

[8] A. Dujella. *Continued fractions and RSA with small secret exponent*. *Tatra Mountains Mathematical Publications, 2004*.

[9] D. Boneh, G.Durfee. *Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$*. *Preprint, 1998*.

[10] *PKCS #1: RSA Cryptography Specifications Version 2.2*. *Internet Engineering Task Force, 2012*.

[11] G.H. Hardy. *A Mathematician's Apology*. *Cambridge University Press, 1940*.

[12] G.H. Hardy, E.M. Wright, J.H. Silverman. *An Introduction to the Theory of Numbers*. *Oxford University Press, 6th edition, 2008*.

[13] R.D. Carmichael. *The Theory of Numbers*. *New York: John Wiley & Sons, 1914*.

[14] W.M. Baldoni, C. Ciliberto, G.M. Piacentini Catteneo. *Aritmetica, crittografia e codici*. *Springer, 2006*.

[15] T.M. Apostol. *Introduction to Analytic Number Theory*. *Springer, Undergraduate Text in Mathematics, 5th edition, 1998*.

[16] H. Riesel. *Prime Numbers and Computer Methods for Factorization*. *Birkhäuser, Progress in Mathematics, 1985*.

[17] M.J. Hinek. *Cryptanalysis of RSA and its variants*. *Chapman & Hall/CRC, Cryptography and Network Security, 2010*.

[18] S.Y. Yan. *Cryptanalytic Attacks on RSA*. *Springer, 2008*.