

Teoria dei numeri e Crittografia

Christian Ferrari

La sicurezza di RSA

Lo scopo di questa attività, supportata dai software Maple ed Excel, è di analizzare il problema della sicurezza del protocollo di crittografia RSA.

Preparazione Procedere con i comandi Maple indicati per ottenere quanto menzionato.

- Per generare dei numeri aleatori
`z:=lunghezza numero;`
`n1:=rand(10^round(z/2)..10^round(z/2+1))();`
`n2:=rand(10^round(z/2)..10^round(z/2+1))();`
- Per determinare due numeri primi vicini ai numeri generati e moltiplicarli
`p:=nextprime(n1);`
`q:=prevprime(n2);`
`n:=p*q;`
- Per determinare la lunghezza di n
`floor(evalf(log[10](n)+1));`
- Per determinare il tempo di calcolo di un'operazione data
`st:=time();`
`w:=operazione;`
`time() - st;`

La fattorizzazione in numeri primi Con il comando

`ifactor(n);`

Maple è in grado di fattorizzare in numeri primi un numero n dato.

1. Genera dei numeri decimali n (con una lunghezza da 12 a 48, per esempio per passi di 4);
2. calcola la lunghezza ℓ e il tempo di fattorizzazione di n ;
3. riporta i valori ottenuti in una tabella Excel;
4. costruisci il grafico della funzione $T(\ell)$;
5. fai tracciare la linea di tendenza con equazione e coefficiente R^2 .

Il calcolo della funzione $\varphi(n)$ di Euler Con il comando

```
with(numtheory):  
phi(n);
```

Maple è in grado di calcolare la funzione $\varphi(n)$ di Euler.

1. Genera dei numeri decimali n (con una lunghezza da 12 a 48, per esempio per passi di 4);
2. calcola la lunghezza ℓ e il tempo di calcolo di $\varphi(n)$;
3. riporta i valori ottenuti in una tabella Excel;
4. costruisci il grafico della funzione $T(\ell)$;
5. fai tracciare la linea di tendenza con equazione e coefficiente R^2 .

Conclusione

1. Che relazione c'è tra i due problemi?
2. Calcola i valori di $T(\ell)$ per $\ell = 300$ (come nei protocollo reali di RSA).
3. Qual è la base della sicurezza della crittografi RSA?