# Algoritmo per tutelare la privacy dello studente usando l'aritmetica modulare o aritmetica dell'orologio

Di Cristiano Armellini, cristiano.armellini@alice.it

**Problema: pubblicare i risultati degli esami senza violare la privacy dello studente.**

**Algoritmo:**

- ogni studente ha matricola che è un numero (es 45713)
- il docente dopo aver corretto i compiti, stabilisce un intero ***n*** minore dei numeri di matricola degli studenti che hanno sostenuto l'esame. Esempio ***n = 700*** (le matricole hanno in genere 5 cifre, quindi ***n*** può essere preso da 3 cifre o 4 cifre )
- calcola ***Mod(a,n)=b , a modulo n, ovvero il resto della divisione di a con n***
- quindi pubblica ***b, n*** e il voto dell'esame associato a ***b (213, voto 30/30)***
- anche lo studente conosce la sua matricola, calcola ***Mod(a,n)=b***, quindi verifica nella lista pubblicata il voto che ha preso. Nel nostro caso ***(voto 30/30 per Mod(45713, 700) = 213 =65*700+213***)
- Attenzione in teoria è possibile che ci siano due valori ***a1, a2*** tali che ***Mod(a1,n)=Mod(a2,n)=b*** ma dovrebbe capitare che sia ***a1,*** che ***a2*** dovrebbero essere numeri di matricola validi e in ogni caso il

docente se si imbatte in questo situazione rarissima e sfortunata potrà risolverla cambiando il numero ***n***.

- Per un estraneo conoscendo ***b,n*** ricavare ***a*** non è affatto facile (non che sia impossibile), tuttavia l'operazione richiede elevate competenze matematiche e l'uso di programmi ad hoc su personal computer.
- La potenza dell'algoritmo sta nel fatto che il numero ***n*** può essere cambiato ogni volta che si pubblicano gli esiti di un esame , usando invece una semplice funzione invertibile del tipo ***f(a)=b*** si impiegherebbe poco tempo, nota ***f,*** per tutti a ricavare i valori ***a*** da ***b***
- Se i numeri di matricola fossero non a 5 cifre ma a 10 cifre l'operazione di decifrazione sarebbe ovviamente ancora più difficile per un estraneo.
- ***Variante:*** **il numero *n* invece di renderlo pubblico potrebbe essere noto solo agli studenti : ad** esempio il docente potrebbe comunicarlo alla fine dell'esame e prima di rendere noti i risultati. In questo caso la decrittazione dei risultati da parte di un estraneo sarebbe praticamente impossibile.