12-01

```
Compito scritto in classe sui seguenti argomenti:
Inverso di e (mod f)
Algoritmo di Diffie-Hellman
Funzione di Eulero Φ(n)
Calcolare la chiave pubblica
Calcolare la chiave segreta d
Codificare e decodificare un messaggio m
```

ARITMETICA MODULARE → NUMERI PRIMI

(1) → INVERSO DI UN NUMERO

($\equiv$) → CONGRUENZA

↓

STESSO RESTO PER DIV. INTERA

L'inverso di un numero e modulo f è un numero d tale che:

$$e \cdot d \equiv 1 \pmod{f}$$

INVERSO? → USATO IN ALG. CRITTOGRAFICI

RSA DIFFIE-HELLMAN.

⇓

ALGORITMO DI EUCLIDE ESTESO

(SERIE DI DIVISIONI E MODULI)

GCD / MASSIMO COMUN DIVISORE → GREATEST COMMON DIVISOR

Per calcolare l'inverso di e modulo f, si può usare l'algoritmo di Euclide esteso. Se $\gcd(e, f) = 1$, allora esiste un inverso modulo di e. L'algoritmo di Euclide esteso permette di trovare anche i coefficienti x e y tali che:

$$e \cdot x + f \cdot y = \gcd(e, f)$$

Se $\gcd(e, f) = 1$, allora x è l'inverso di e modulo f.

Esempio: Supponiamo di voler trovare l'inverso di $e = 7$ modulo $f = 72$. Si usa l'algoritmo di Euclide esteso:

EUCLIDE (1)

1. $72 = 10 \cdot \boxed{7} + 2$
2. $7 = 3 \cdot 2 + 1$
3. $2 = 2 \cdot 1 + 0$

GCD (7, 72)

Poi, risolviamo per $1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (72 - 10 \cdot 7)$.

Da qui otteniamo $1 = 31 \cdot 7 - 3 \cdot 72$, quindi l'inverso di 7 modulo 72 è 31.

(1) FACCIO (EUCLIDE) → GCD

Algoritmo di Euclide per il calcolo del gcd:

1. Dividi a per b e calcola il **resto** della divisione:

$$a = b \times q + r$$

   Dove q è il **quoziente** e r è il **resto**.

2. Se il resto $r = 0$, allora b è il **gcd** di a e b.
3. Se $r \neq 0$, sostituisci a con b e b con r, e ripeti il passo 1.

Esempio pratico: Calcolare $\gcd(72, 36)$

1. Dividi 72 per 36:

$$72 = 36 \times 2 + 0$$

   Qui il resto è zero, quindi il **gcd** è 36.

(2) VERIFICA CHE EUCLIDE / INVERSO FUNZIONA

$$e \cdot x + f \cdot y = \gcd(e, f)$$

⟹ $1 = 31 \cdot 7 - 3 \cdot 72$, quindi l'inverso di 7 modulo 72 è 31.

2. Algoritmo di Diffie-Hellman

↓ CRITTOGRAFIA SIMMETRICA = 1 CHIAVE SOLA

L'algoritmo di Diffie-Hellman per la condivisione di una chiave segreta è il seguente:

- Alice sceglie un numero segreto a, calcola $A = g^a \mod p$, e invia A a Bob.
- Bob sceglie un numero segreto b, calcola $B = g^b \mod p$, e invia B a Alice.
- Alice calcola la chiave segreta come $K = B^a \mod p$.
- Bob calcola la chiave segreta come $K = A^b \mod p$.

SCRIPT = COPIONE

DIFFIE-HELLMAN = CONDIVISIONE CHIAVE IN CANALE NON-SICURO

A e B conoscono due numeri g e p pubblici (p **primo** *cioè un numero naturale maggiore di 1 che sia divisibile solamente per 1 e per sé stesso*)
A conosce un numero segreto a
B conosce un numero segreto b

A calcola	$A = g^a \bmod p$	e lo comunica a	B
B calcola	$B = g^b \bmod p$	e lo comunica a	A
A calcola	$K = B^a \bmod p$		
B calcola	$K = A^b \bmod p$		

Ma:

$$K = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$
$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

A e B hanno condiviso un segreto (**il numero K**) senza comunicarlo esplicitamente!
Un eventuale attaccante può osservare A, B, g, p ma questa informazione non è sufficiente per ricavare K.
K è calcolabile solo conoscendo a o b, che tuttavia sono segreti e non vengono mai trasmessi. Ricavare a da A (o analogamente b da B) significa risolvere un logaritmo discreto, difficile dal punto di vista computazionale.

FUNZIONE DI EULERO → RSA / MODULO INVERSO

La funzione di Eulero $\varphi(n)$ per un numero n che è il prodotto di due numeri primi p e q è:

$$\varphi(n) = (p-1)(q-1)$$

↓ ESEMPIO IN RSA ...

La φ(n) di Eulero serve a tale scopo e Il risultato è **$f = \varphi(n) = (p-1)(q-1) = n - p - q + 1$**.

RSA

4. Calcolare la chiave pubblica

φ - PHI = EULERO

La chiave pubblica (n, e) in RSA viene calcolata come segue:

- Scegli due numeri primi p e q, calcola $n = p \cdot q$.
- Calcola $\varphi(n) = (p-1)(q-1)$.
- Scegli un numero e tale che $1 \leq e < \varphi(n)$ e che sia coprimo con $\varphi(n)$ (ossia $\gcd(e, \varphi(n)) = 1$). → ASSICURA NUMERI UNIVOCI E DIFFICILI ALL'ESTERNO...

PRIMI TRA DI LORO = EULERO = GCD

La chiave pubblica è quindi la coppia (n, e).

5. Calcolare la chiave segreta d

La chiave segreta d è l'inverso di e modulo $\varphi(n)$, ossia:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

RIFERIMENTO (PAG. 7 - 9 PDF_CRITTOGRAFIA) GENERALE

6. Codificare e decodificare un messaggio m (EULERO/EUCLIDE)] ...

- **Cifratura**: Data la chiave pubblica (n, e) e un messaggio m, il messaggio cifrato c è:

$$c = m^e \mod n$$

- **Decifratura**: Data la chiave privata (n, d) e il messaggio cifrato c, il messaggio m è:

$$m = c^d \mod n$$

RSA

RSA - cifratura e decifratura

Dato un messaggio m (0 < m < n)

1. Cifratura: calcolare $c = m^e \mod n$
2. Decifratura: calcolare $m = c^d \mod n$

Esempi:

La chiave pubblica è (33, 7)

La chiave privata è (33, 3)

$c = 2^7 \mod 33 = 29$

$m = 29^3 \mod 33 = 2$

$c = 15^7 \mod 33 = 27$

$m = 27^3 \mod 33 = 15$

PAGINA 9 - CRITTOGRAFIA GENERALE

LEGGI ALLEGATI ...