

RELAZIONE LABORATORIO 1

09/04/2024

Membri del gruppo:

Enrico Ferraiolo 0001020354 enrico.ferraiolo2@studio.unibo.it

Simone Folli 0000974629 simone.folli2@studio.unibo.it

Gianlorenzo Urbano 0001020548 gianlorenzo.urbano@studio.unibo.it

ESERCIZIO 1:

Per svolgere questo esercizio dobbiamo prima di tutto trovare $\text{GCD}(57, 93)$, una volta fatto troviamo che $\text{GCD}(57, 93) = 3$.

L'esercizio chiede inoltre di trovare due interi, s e t , tali per cui $57s + 93t = \text{GCD}(57, 93)$.

Per fare ciò possiamo passare attraverso l'algoritmo di Euclide esteso.

Si trova che $57 \cdot (-13) + 93 \cdot 8 = 3$. Quindi $s = -13$, $t = 8$

```
Insert a (57): 57
Insert b (93): 93
gcd(57,93):
([0, 1, 1, 1, 1, 2, 2], 3)
extended_euclidean_algorithm:
s = -13, t = 8
57*-13 + 93*8 = 3
```

ESERCIZIO 2:

Al fine di risolvere e trovare la risoluzione all'esercizio bisogna scrivere l'algoritmo del "Multiplicative inverse".

Adesso possiamo trovare le soluzioni ai quesiti richiesti:

a) $17^{-1} \bmod 101 = 6$

```
Insert first number (17, 357, 3125): 17
Insert second number (101, 1234, 9987): 101
Multiplicative inverse:
17^-1 mod 101 = 6
```

(b) $357^{-1} \bmod 1234 = 1075$

```
Insert first number (17, 357, 3125): 357
Insert second number (101, 1234, 9987): 1234
Multiplicative inverse:
357^-1 mod 1234 = 1075
```

(c) $3125^{-1} \bmod 9987 = 1844$

```
Insert first number (17, 357, 3125): 3125
Insert second number (101, 1234, 9987): 9987
Multiplicative inverse:
3125^-1 mod 9987 = 1844
```

ESERCIZIO 3:

Ipotizziamo che Bob voglia creare la sua coppia di chiavi

dobbiamo verificare che: $\gcd(\phi(n), b) = 1$

Bob deve scegliere due numeri primi p e q :

$p = 101$, $q = 113$,

quindi calcoliamo $n = p \cdot q = 11413$,

e $\phi(n) = 100 \times 112 = 11200$,

ora scegliamo b tale che il Massimo comune divisore $\gcd(\phi(n), b)$ sia uguale a 1,

$b = 3533$, $\gcd(\phi(n), b) = 1$, abbiamo verificato la validità della selezione di b .

Passiamo a calcolare il secret decryption exponent, applicando l'algoritmo del Multiplicative Inverse Algorithm per trovare a : $a = 6597$, questa sarà la chiave privata di Bob

```
insert the values of p, q and n
p (101): 101
q (113): 113
n: 11413
b (3533): 3533
The RSA Cryptosystem
gcd( $\phi(n)$ , b): 1
a: 6597
```

ESERCIZIO 4:

Per fare il quarto esercizio abbiamo riscritto lo square and multiply algorithm.

Ora ipotizziamo che Alice voglia mandare un messaggio cifrato a Bob

Alice deve prendere b e n condivisi da Bob

ora per criptare il messaggio "9726" calcola $9726^b \bmod n$

$b = 3533$, $n = 11413$

il messaggio cifrato è: 5761

ora Bob deve solo calcolare $5761^a \bmod n$, per ottenere il messaggio in chiaro

```
Insert x (9726): 9726
Insert x (3533): 3533
Insert x (11413): 11413
alice wants to send the plaintext 9726 to bob
cyphertext 5761
bob wants to decrypt the cyphertext 5761 using the secret decryption exponent a: 6597
plaintext 9726
```