

RELAZIONE DIFFIE-HELLMAN

5CI

13/11/2020

Gruppo: Mustaccio Christian, Kevin Wang

Consegna:

Realizzare due applicativi, in un linguaggio a scelta, che realizzino una comunicazione cifrata con chiave simmetrica generata tramite l'algoritmo di Diffie-Hellman.

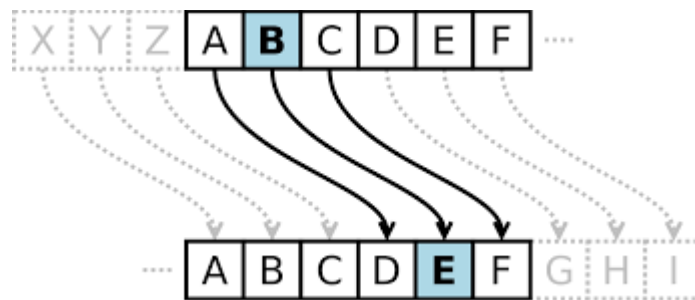
La comunicazione deve essere bidirezionale e si deve avere la possibilità di cambiare chiave in seguito alla richiesta di uno dei due algoritmi.

Ogni applicativo deve poter scrivere su una videata "console" il risultato dei vari passaggi in corso, in modo da poter essere verificato.

Occorre mostrare nella console anche il testo del messaggio criptato ricevuto e la decodifica effettuata.

Il messaggio da inviare deve poter essere scelto al momento e deve consistere in lettere maiuscole presenti nella codifica ASCII a 7 bit. Per la criptatura scegliere fra: operatore XOR, sostituzione della lettera stile cifrario di Cesare.

Metodo di criptatura utilizzato: Cifrario di Cesare.



Protocollo crittografico: Scambio di chiavi Diffie-Hellman

Link utilizzato per esempio:

https://it.wikipedia.org/wiki/Scambio_di_chiavi_Diffie-Hellman

Porta utilizzata: 49153 in quanto dalla porta 1024 alla porta 49151 sono porte registrate e non dovrebbero essere usate.

```
static final int port = 49153;
```

//consiglio di rivedere gli screenshot dalla apposita cartella//

Per ottimizzare il codice sono state utilizzate 3 funzioni:

1. Funzione per generare la chiave

```
public static void generoChiave() throws IOException {
    //scelgo i due numeri primi
    p = 23;
    q = 5;
    System.out.println("I numeri primi sono: " + p + "," + q + "...");

    //mando i numeri al server
    osw = new OutputStreamWriter(s.getOutputStream());
    bw = new BufferedWriter(osw);
    pw = new PrintWriter(bw, true);
    pw.println(p);
    pw.println(q);
    pw.flush();

    //genero numero segreto
    segreto_b = r.nextInt(20); //scegliamo un range basso per prova
    System.out.println("segreto b scelto: " + segreto_b);

    //ricevo codice segreto del server
    isr = new InputStreamReader(s.getInputStream());
    br = new BufferedReader(isr);
    A = Integer.parseInt(br.readLine());
    System.out.println("A: " + A);
    System.out.println("codice segreto b: " + (g ^ segreto_b) % p);

    //invio codice segreto al server
    pw.println((g ^ segreto_b) % p);

    //calcolo la costante KA=(g^b mod p)^a %p = B^a mod p
    ka = (A ^ segreto_b) % p;
    System.out.println("KA:" + ka);
}
```

2. Funzione per criptare il messaggio

```
public static void criptoMessaggio() {
    //cripto il messaggio con i cifrario Cesare
    for (int j = 0; j < sceltaUtente.length(); j++) {
        supp = sceltaUtente.charAt(j);
        supp += ka;
        parolaCriptata = parolaCriptata.substring(0, j) + supp;
    }
    System.out.println("invio il messaggio: " + parolaCriptata);

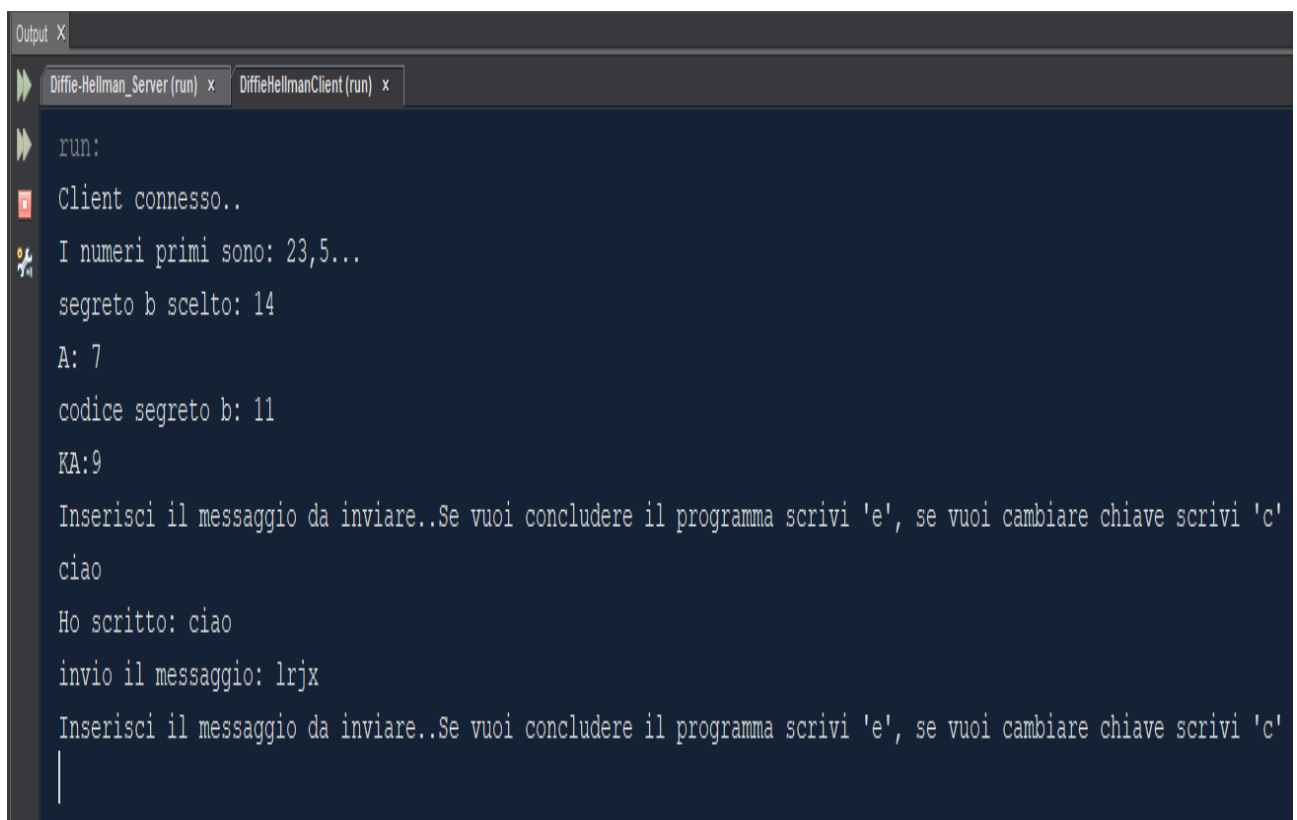
    //invio il messaggio criptato
    pw.flush();
    pw.println(parolaCriptata);
    pw.flush();
}
```

3. Funzione per decriptare il messaggio

```
public static void decriptoMessaggio() throws IOException {  
    //ricevo il messaggio criptato  
    messaggioUtente = br.readLine();  
    System.out.println("Messaggio ricevuto: " + messaggioUtente);  
  
    //decripto il messaggio  
    System.out.println("Decripto il messaggio.....");  
  
    for (int j = 0; j < messaggioUtente.length(); j++) {  
        supp = messaggioUtente.charAt(j);  
        supp -= kb;  
        parolaDecriptata = parolaDecriptata.substring(0, j) + supp;  
    }  
    System.out.println("Messaggio decriptato: " + parolaDecriptata);  
}
```

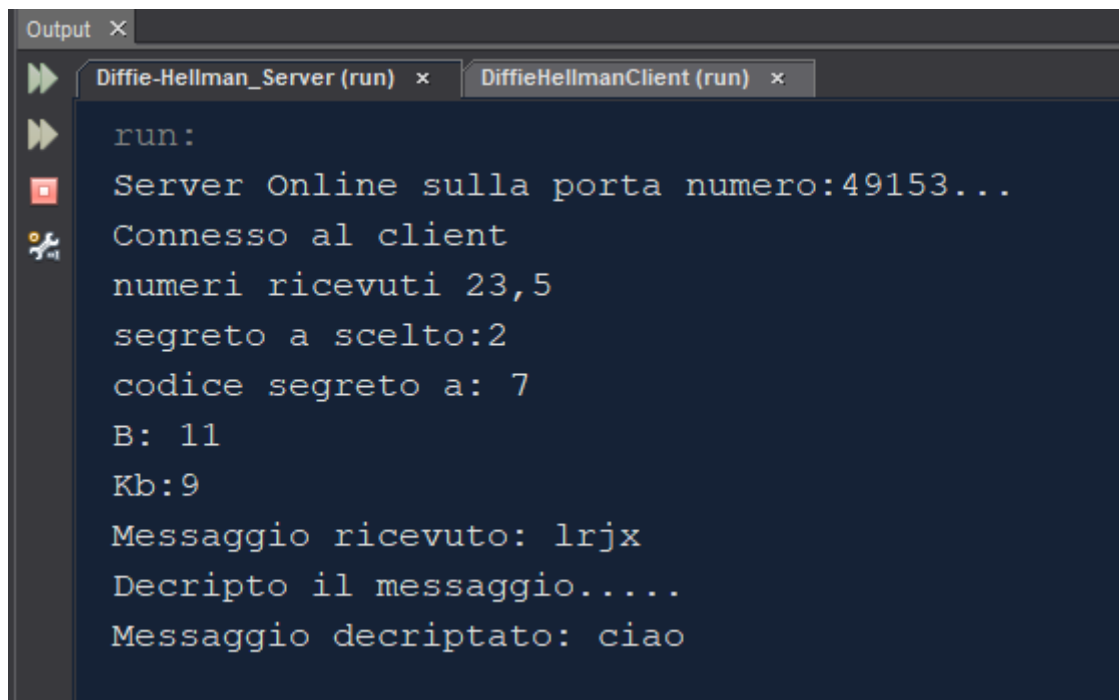
OUTPUT CONSOLE:

Il client si connette al server e invia un messaggio criptato.



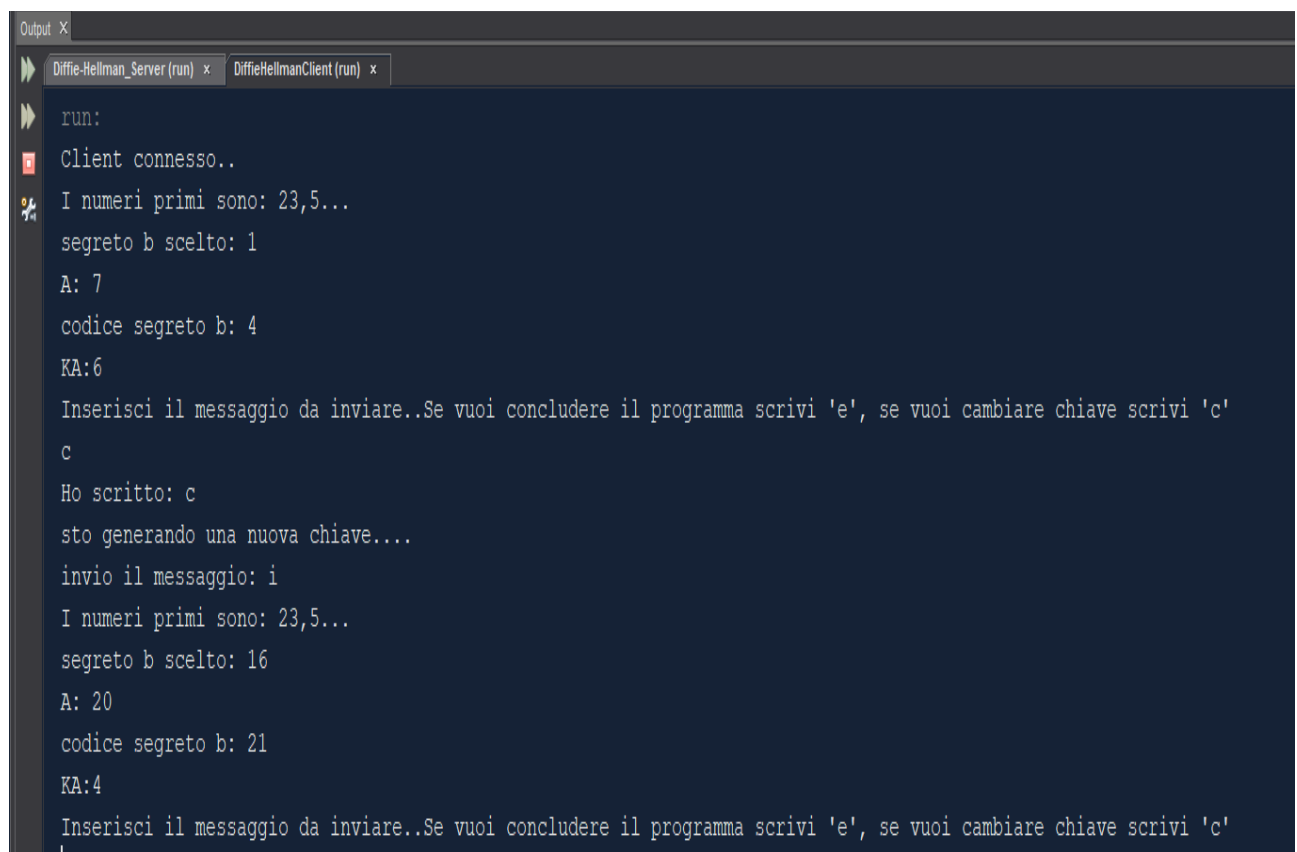
```
Output X  
Diffie-Hellman_Server (run) x DiffieHellmanClient (run) x  
run:  
Client connesso..  
I numeri primi sono: 23,5...  
segreto b scelto: 14  
A: 7  
codice segreto b: 11  
KA:9  
Inserisci il messaggio da inviare..Se vuoi concludere il programma scrivi 'e', se vuoi cambiare chiave scrivi 'c'  
ciao  
Ho scritto: ciao  
invio il messaggio: lrjx  
Inserisci il messaggio da inviare..Se vuoi concludere il programma scrivi 'e', se vuoi cambiare chiave scrivi 'c'  
|
```

Il server è connesso al client e decripta il messaggio ricevuto..



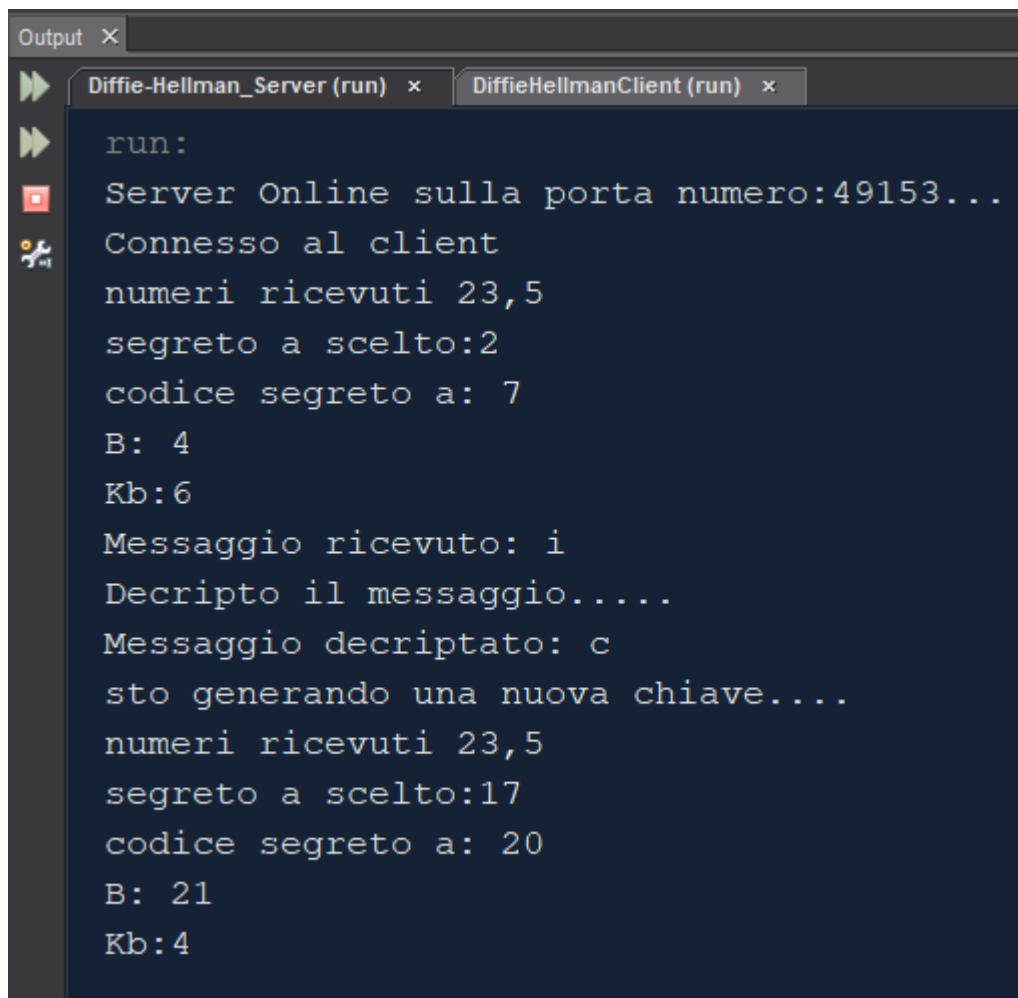
```
Output X
Diffie-Hellman_Server (run) x DiffieHellmanClient (run) x
run:
Server Online sulla porta numero:49153...
Connesso al client
numeri ricevuti 23,5
segreto a scelto:2
codice segreto a: 7
B: 11
Kb:9
Messaggio ricevuto: lrjx
Decripto il messaggio.....
Messaggio decriptato: ciao
```

Il client decide di cambiare la chiave di criptatura..



```
Output X
Diffie-Hellman_Server (run) x DiffieHellmanClient (run) x
run:
Client connesso..
I numeri primi sono: 23,5...
segreto b scelto: 1
A: 7
codice segreto b: 4
KA:6
Inserisci il messaggio da inviare..Se vuoi concludere il programma scrivi 'e', se vuoi cambiare chiave scrivi 'c'
c
Ho scritto: c
sto generando una nuova chiave....
invio il messaggio: i
I numeri primi sono: 23,5...
segreto b scelto: 16
A: 20
codice segreto b: 21
KA:4
Inserisci il messaggio da inviare..Se vuoi concludere il programma scrivi 'e', se vuoi cambiare chiave scrivi 'c'
|
```

Il server cambia chiave di criptatura...



```
Output X
Diffie-Hellman_Server (run) X DiffieHellmanClient (run) X
run:
Server Online sulla porta numero:49153...
Connesso al client
numeri ricevuti 23,5
segreto a scelto:2
codice segreto a: 7
B: 4
Kb:6
Messaggio ricevuto: i
Decripto il messaggio.....
Messaggio decriptato: c
sto generando una nuova chiave....
numeri ricevuti 23,5
segreto a scelto:17
codice segreto a: 20
B: 21
Kb:4
```