Cognome Nome Cognome Nome Cognome Nome

Test di valutazione N.3

1. (Punti 1) Impiegate l'algoritmo "repeated square and multiply" per eseguire esponenziazioni modulo p. Quale formula fornisce il numero medio di moltiplicazioni che occorrerà eseguire per ottenere il risultato?

RISPOSTA	non so	2p	3/2 log p	3/2 p	2 log p
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

2. (Punti 1) Quali tra i seguenti numeri primi sono anche "safe"?

RISPOSTA	5	7	11	13	17
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

3. (Punti 1) Per un grande numero primo di Sophie Germain il presentare la forma "6k-1" è una condizione

RISPOSTA	non so	necessaria	sufficiente	nec. & suf.
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

4. (Punti 2) Quale valore dovete attribuire al parametro "certainty" del test di primalità di Miller-Rabin per essere sicuri che l'algoritmo abbia eseguito tre iterazioni prima di fornire una dichiarazione di "probabilmente primo"?

RISPOSTA	non so	2	3	4	5
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

5. (Punti 1) Generate a caso un numero h minore di p, ove p è un grande numero primo impiegato in uno scambio DH. Quale numero approssima meglio la probabilità che h sia una radice primitiva di p?

☐ 1 ☐ 1/2 ☐ 1/3 ☐ 1/4

6. (Punti 1) Volete impiegare il componente ModPow di S-vLab per calcolare 3^{-4} mod 11. Quale intero dovete digitare come esponente?

RISPOSTA	non so	4	5	6	7
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

7. (Punti 2) Giustificare la risposta scelta:_____
_____
_____

8. (Punti 1) Volete programmare in Java uno scambio DH, impiegando la classe SecureRandom per la generazione delle chiavi private ed il metodo ModPow per le esponenziazioni. Quali package dovete importare?

RISPOSTA	non so	Java.math	Java.security	Javax.crypto
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

9. (Punti 1) Quanti numeri primi vi aspettate di trovare nell'intervallo $2^{28} \div (2^{28} + 100)$? _____