Cognome Nome Cognome Nome Cognome Nome

Test di valutazione N.4

1. (Punti 1) Sottoponete al test di Miller-Rabin il numero 65537. Che valore avranno i parametri r,s?

RISPOSTA	non so	r=1,s=16	r=3,s=15	r=5,s=14	r=7,s=13
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

2. (Punti 1) La chiave pubblica RSA può avere un numero pari come esponente e?

RISPOSTA	non so	si	no
Prima degli esperimenti	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐

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

4. (Punti 1) La chiave privata RSA, fornita dal provider BC e predisposta per l'impiego del CRT, contiene tra l'altro una componente denominata "PrimeExponentP". Il valore di questa componente è espresso da:

RISPOSTA	non so	d mod p	d mod (p-1)	n mod p
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

5. (Punti 2) Disponete di un programma che accetta un numero m, primo o composto, e fornisce un numero scelto a caso ed il suo inverso moltiplicativo modulo m. Fate diverse prove e misurate un tempo medio di esecuzione T1 quando m è primo, T2 quando m è composto. Quale delle seguenti relazioni è vera?

RISPOSTA	non so	T1=T2	T1<T2	T1>T2
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

6. (Punti 1) Indicate con T1 il tempo di esecuzione di una firma con l'algoritmo DSA e con T2 il tempo di verifica. Quale delle seguenti relazioni è vera?

RISPOSTA	non so	T1=T2	T1<T2	T1>T2
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

7. (Punti 1) Un cifrario RSA impiega una chiave da 1024 bit ed un numero a caso di 64 bit (standard PKCS#1) per la randomizzazione del testo cifrato. La massima lunghezza in byte del testo in chiaro è

RISPOSTA	non so	116	117	119	120
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

8. (Punti 1) Esaminando la tabella di pag. 97, individuare quale potenziale vulnerabilità ha la firma con RSA quando l'impronta del messaggio non è relativamente prima con il modulo n? _____
   _____
   _____