Cognome Nome Cognome Nome Cognome Nome

Test di valutazione N.1

1. (Punti 1) Si comprime con SHA-1 un messaggio di 248 bit ed uno di 496 bit. I tempi di esecuzione sono

RISPOSTA	non so	uguali	diversi
Prima degli esperimenti	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐

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

3. (Punti 1) In Java, il tipo di dato di un'impronta è:

RISPOSTA	non so	integer	big integer	byte array	string
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

4. (Punti 1) Supponendo che Eva abbia accesso anche al canale su cui A comunica l'impronta di un messaggio di 32 byte, che probabilità ha di forgiare un messaggio che B consideri integro?

RISPOSTA	non so	0 %	25 %	75 %	100 %
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

5. (Punti 2) Quale algoritmo di hash ha il più basso tempo di esecuzione per bit d'impronta?

RISPOSTA	non so	Whirlpool	RIPEMD	Tiger	SHA-1
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

6. (Punti 1) E' possibile invocare un metodo della classe SecureRandom che generi un integer?

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

7. (Punti 2) I due messaggi m, m' sono in collisione. Scegliete a caso un messaggio c e costruite c||m, c||m': avete trovato una nuova coppia in collisione?

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

8. (Punti 2) Quanti input casuali di 512 bit ci si deve aspettare di dover fornire in ingresso ad una funzione hash crittografica con impronta ridotta a 8 bit per ottenere un'uscita prestabilita?_____

9. (Punti 1) Alice manda a Bob un messaggio e la sua impronta concatenata con un dato segreto che condividono. Eva intercetta entrambi i dati e li rinvia a Bob dopo un po' di tempo per creare confusione. Come è possibile proteggersi da questo attacco? _____
_____
_____