Cognome Nome Cognome Nome Cognome Nome

Test di valutazione N.2

1. (Punti 1) Si vuole impiegare un Cifrario a blocchi per cifrare un testo in chiaro di lunghezza non multipla della lunghezza del blocco. E' possibile genera un testo cifrato di uguale lunghezza?

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

2. (Punti 1) Quando si usa la modalità CTR, occorre fornire al Counter un vettore di inizializzazione. E' sicuro impiegare lo stesso IV per cifrare più messaggi consecutivi?

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

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

4. (Punti 1) Quali altre modalità di cifratura hanno bisogno di un intialization vector?

RISPOSTA	non so	ECB	CBC	OFB	CFB
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

5. (Punti 2) Per quali modalità occorre configurare in Encrypt Mode anche il blocco Cipher di ricezione?

RISPOSTA	non so	ECB	CBC	OFB	CFB
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

6. (Punti 1) In Java, il tipo di dato di un testo cifrato è

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

7. (Punti 2) Eva, per creare confusione, modifica il valore di un bit di ogni testo cifrato che transita sul canale; quali modalità di cifratura consentono a Bob di perdere il meno possibile del messaggio di Alice?

RISPOSTA	non so	CTR	ECB	CBC	CFB
Prima degli esperimenti	☐	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐	☐

8. (Punti 2) Quale cifrario simmetrico a blocchi ha il più basso tempo di esecuzione per bit di cifrato?

RISPOSTA	non so	DES	TDES	AES
Prima degli esperimenti	☐	☐	☐	☐
Dopo gli esperimenti	☐	☐	☐	☐

9. (Punti 1) Quale valore esadecimale deve avere un Counter da 1 byte per azzerarsi con un solo Execute? ___