Esame di Fondamenti di Cybersecurity

03-06-2025

Leggere attentamente ogni punto del regolamento prima di svolgere l'esame, non rispettare queste regole comporterà l'annullamento (anche in corso) dell'esame:

- 1. Non è ammesso nessun tipo di materiale, cartaceo o elettronico, questo va da materiale "ufficiale" del corso come slide o registrazioni a materiale autoprodotto o semi prodotto (e.g. appunti o soluzioni di esercitazioni). Chat GPT rientra in questa categoria.
- 2. Non è ammesso parlare con altre persone via qualsiasi canale, l'esame e' individuale.
- 3. <u>Scrivete Nome, Cognome e matricola su TUTTI i fogli.</u>
- 4. E' necessario presentare il badge universitario.
- 5. I punteggi di ogni domanda sono riportati a fianco della domanda stessa, il massimo punteggio ottenibile tramite questo esame scritto e' 24. L'esame si considera superato se la somma del punteggio di questo esame con il punteggio delle esercitazioni risulta essere maggiore o uguale a 18.
- 6. <u>La durata della prova e' di un'ora e 40 minuti.</u>
- 7. Potete usare il retro del foglio come brutta copia o considerazioni aggiuntive sulla vostra risposta.
- 8. L'esame va scritto tramite PENNA NERA o PENNA BLU. Non è possibile usare penne rosse o matite o bianchetto.
- 9. Rispondete alle domande in maniera esaustiva ma concisa.
- 10. La consegna dell'esame scritto invalida i precedenti voti. Per ritirarsi all'esame bisogna scrivere "NON VALUTARE" su TUTTI i fogli.

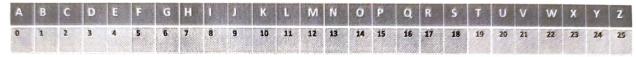
Fondamenti di Cybersecurity 05-02-2025

Nome:

Cognome:

Matricola:

- 1. Consideriamo il seguente Cifrario Affine: $e(x) = ax+b \mod 26$, con a=11 e b=4
- 1) a=11 è una scelta valida per il parametro "a"? Giustificare il perché della propria risposta.
- 2) b=4 è una scelta valida per il parametro "b"? Giustificare il perché della propria risposta.
- 3) Quante chiavi sono possibili?
- 4) Cifrare con questo cifrario il plaintext "security"
- 5) Calcolare la funzione di decifratura d(y)
- 6) Decifrare il ciphertext "qropc"
- 7) Decifrare il ciphertext "wuegw"



(7 punti / 30)

- 2. Alice usa il crittosistema RSA per ricevere messaggi da Bob. Alice sceglie:
- p=17, q=19
- il suo esponente pubblico è e=11

Alice pubblica il prodotto n=pq=323 e l'esponente e=11

- a) Verificare che e=11 è un esponente valido per l'algoritmo RSA
- b) Calcolare d, la chiave privata di Alice

Bob vuole inviare ad Alice il testo P=15, cifrandolo

- c) Che valore Bob invia ad Alice?
- d) Verificare che Alice riesca a decifrare correttamente tale messaggio.

[Scrivere tutti i passaggi per ottenere il risultato per tutte le domande a) b) c) e d)]

(8 punti / 30)

3. Descrivere in modo chiaro ed esaustivo i principi di sicurezza AAA e CIA.

(4 punti / 30)

4. Descrivere il Denial of Service (DoS) "Syn Flooding" di TCP, illustrando il problema in modo chiaro, anche con una figura.

(3 punti / 30)

5. Quali sono i problemi di WEP, e come WPA ver. 2 ha risolto questi problemi?

(4 punti / 30)

6. Descrivere il concetto di Hash chain e Rainbow Table che abbiamo visto nel LAB2, e che sì utilizzano per gestire le password.

(4 punti / 30)