Esame di Fondamenti di Cybersecurity

03-06-2024

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. Scrivete **Nome, Cognome e matricola** su **TUTTI** i fogli tranne questo foglio di istruzioni, negli spazi indicati.
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. La durata della prova e' di **un'ora e 40 minuti**.
7. L'esame va scritto tramite PENNA NERA o PENNA BLU. Non è possibile usare penne rosse o matite o bianchetto.
8. Rispondete alle domande in maniera esaustiva ma concisa.
9. La consegna dell'esame scritto invalida i precedenti voti. Per ritirarsi all'esame bisogna scrivere "**NON VALUTARE**" su TUTTI i fogli ad esclusione di questo foglio di istruzioni.

1. Alice usa il crittosistema **RSA** per ricevere messaggi da Bob. Alice sceglie:
- p=11, q=19
- il suo esponente pubblico è e=7

Alice pubblica il prodotto n=pq=209 e l'esponente e=7
- a) Verificare che e=7 è un esponente valido per l'algoritmo RSA
- b) Calcolare d, la chiave privata di Alice

Bob vuole inviare ad Alice il testo P=14, cifrandolo
- c) Che valore Bob invia ad Alice?
- d) Verificare che Alice riesce a decifrare tale messaggio. **(6 punti / 24)**

2. Consideriamo lo ***Shift Cipher*** e supponiamo che le chiavi vengono utilizzate con la stessa probabilità. Dimostrare che lo *Shift Cipher* fornisce Perfect Secrecy. **(5 punti / 24)**

3. Descrivere in cosa consiste un attacco di tipo ***buffer overflow***. Quando è possibile attuarlo? Esistono precauzioni o contromisure? **(4 punti / 24)**

4. Spiegare il meccanismo **WEP** (Wired Equivalent Privacy).
    a. In quale standard senza fili/wireless viene utilizzato per assicurare l'autenticazione e la confidenzialità?
    b. Su quale algoritmo di cifratura si basa WEP?
    c. Quale sono le debolezze di questo algoritmo di cifratura?
    d. Discutere un esempio di attacco che può avere luogo con WEP **(5 punti / 24)**

5. Quali sono i problemi della modalità ECB? **(4 punti / 24)**