Esame di Fondamenti di Cybersecurity

26-06-2023

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

1. Non e' amesso 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 e' 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 tre ore.
7. Potete usare il retro del foglio come brutta copia o considerazioni aggiuntive sulla vostra risposta. I fogli saranno corretti separatamente da singoli docenti, **NON USATE FOGLI DI CATEGORIE DIVERSE PER CONTINUARE LE RISPOSTE** (i.e. sul foglio di crittografia va solo crittografia).
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 ad esclusione di questo foglio di istruzioni.

Fondamenti di Cybersecurity 26-06-2023

Nome: Cognome: Matricola:

Crittografia

1. Dare la definizione di PRG (PseudoRandomGenerator) e, quindi, di cifrari a flusso (*stream cipher*). Un cirfrario a flusso può essere perfettamente sicuro? Dare la definizione formale di PRG impredicibile e connetterla con la definizione di PRG sicuro. (6 punti / 24)

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Fondamenti di Cybersecurity 26-06-2023

Nome: Cognome: Matricola:

2. Descrivere il protocollo di Diffie-Hellman (idea ad alto livello, descrizione protocollo, e analisi sicurezza/attracchi). (4 punti / 24)

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Fondamenti di Cybersecurity 26-06-2023

Nome: Cognome: Matricola:

Sicurezza

1. Descrivere un esempio pratico di security by obscurity e un attacco al sistema in esame. (5 punti / 24)

……..

……..

……..

……..

……..

……..

……..

……..

2. Descrivere il meccanismo di challenge e response e come potrebbe essere usato per migliorare la sicurezza dell'apertura delle automobili. Descrivere inoltre almeno un attacco a un sistema che utilizza challenge e response. (5 punti / 24)

……..

……..

……..

……..

……..

……..

……..

……..

Fondamenti di Cybersecurity 26-06-2023

Nome: Cognome: Matricola:

Laboratorio

1. É sensato eseguire un attacco con le Rainbow Tables in caso di hash di password con salt? Perchè? (4 punti / 24)

……..

……..

……..

……..

……..

……..

……..

……..