# Esame di Fondamenti di Cybersecurity

07-06-2023

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.

Fondamenti di Cybersecurity 07-06-2023

Nome: Cognome: Matricola:

# Crittografia

1. Fornire la definizione di One Time Pad e di Sicurezza Perfetta di Shannon, provare che OTP è sicuro. (5 punti / 24)

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……

2. Cos'è e cosa gestisce un Trusted 3rd PartyTTP? Descrivere il Puzzle di Markle. (5 punti / 24)

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……

Fondamenti di Cybersecurity 07-06-2023

Nome: Cognome: Matricola:

# Sicurezza

1. DB S.R.L. sviluppa un sistema di accesso basato su un software compilato e offuscato (l'eseguibile viene dato in pasto a Ghidra per vedere se si riesce ad analizzare e vengono messe in atto politiche di anti-debug). Questo è un buon metodo per garantire la sicurezza di un sistema? Perché o perché no? (5 punti / 24)

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……

2. Supponiamo di disporre di un sistema che prevede una password e la ricezione di un codice (OTP) via SMS, come si potrebbe aumentare la sicurezza dal punto di vista teorico? è sufficiente una seconda password? Perché o perché no? (5 punti / 24)

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……

Fondamenti di Cybersecurity 07-06-2023

Nome: Cognome: Matricola:

# Laboratorio

1. Spiegare brevemente l'obiettivo e che strategia di attacco utilizza aircrack-ng, specificando se è un attacco di tipo online o offline. (4 punti / 24)

   ……

   ……

   ……

   ……

   ……

   ……

   ……

   ……