## Esame di Fondamenti di Cybersecurity

13-07-2023

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. sui fogli 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 13-07-2023

	Toridamenti di Oybersedanty 10	01 2020
Nome:	Cognome:	Matricola:

## Crittografia

1. Cosa sono le trapdoor function e come si descrive il funzionamento di RSA attraverso le trapdoor permutations? Descrivere, infine, un attacco alla versione textbook di RSA. (6 punti / 24)

## Fondamenti di Cybersecurity 13-07-2023

Cognome: Nome: Matricola: 2. Descrivere il funzionamento del 3DES e spiegare il meet in in the middle attack sul 2DES e

3DES. (4 punti / 24)	

Fondamenti di Cybersecurity 13-07-2023 Cognome:

Matricola:

Nome:

1. genere	Qual e' un metodo per anonimizzare un attacco di rete? L'anonimizzazione e' utile per questo et di attacchi? (5 punti / 24)

Fondamenti di Cybersecurity 13-07-2023 Cognome: Nome: Matricola:

2. Descrivere il modello di permessi su file in UNIX, come questo modello evita che un determinato utente possa, ad esempio, modificare i byte agendo direttamente su un disco? Quali sono le limitazioni del modello e i modelli alternativi che possono essere utilizzati per aumentare la sicurezza. (5 punti / 24)

Fondamenti di Cybersecurity 13-07-2023 Cognome:

Matricola:

	_				_	
2	h	$\cap$	ra	to	ri	$\cap$

Nome:

Quali strategie di cracking si possono avere con hashcat? (4 punti / 24)