Esame di Fondamenti di Cybersecurity

05-02-2025

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. Scrivete **Nome, Cognome e matricola** su **TUTTI** i fogli.
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 30 minuti**.
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. Alice usa il crittosistema **RSA** per ricevere messaggi da Bob. Alice sceglie:

- p=11, q=13
- il suo esponente pubblico è e=7

Alice pubblica il prodotto n=pq=143 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 P1=14 ed il testo P2=15, cifrandoli

- c) Che valori Bob invia ad Alice?
- d) Verificare che Alice riesce a decifrare tali messaggi.

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

(8 punti / 24)

SOLUZIONE:

a)

Allora: Phi(n) = (p-1)(q-1) = (11-1)(13-1)=120
120= (2^3)*3*5
gcd(7,120)=1, la scelta di e=7 è valida
L'esponente privato d=e^-1 mod(Phi(n))= 7^-1 mod(120)= **103**
Infatti **103*7= 721 = 6*120 + 1** = 1 (modulo 120)

b)

Extended_EuclideanAlgorithm/Multiplicative_Inverse(120,7):
a0 = 120, b0= 7, t0 = 0 e t=1
q = integer part of (a0/b0) = 17
r = 120 - 17*7 = 120 -119 = 1
temp = (0 -17*1) mod 120 = 103
t0 = t = 1
t = temp = 103
a0 = b0 = 7
b0 = r = 1
q = integer part of (a0/b0) = integer part of (7/1) = 7
r = 7 - 7*1 = 0

b0 = 1 => return (103)
private key d = 103

c) e d)

Ciphertext1 inviato da Bob ad Alice C1= 14^7 mod(143) = **53**
Alice decifra il plaintext P1 =**53**^103 mod (143) = **14**

Esponente b =111
b[0] = 1, risultato= 14

b[1] = 1, risultato= 27
b[2] = 1, risultato= 53
Ciphertext c: 53
—------
Esponente b =1100111
b[0] = 1, risultato= 53
b[1] = 1, risultato= 14
b[2] = 0, risultato= 53
b[3] = 0, risultato= 92
b[4] = 1, risultato= 1
b[5] = 1, risultato= 53
b[6] = 1, risultato= 14
Ciphertext c: 14

Ciphertext2 inviato da Bob ad Alice C2= 15^7 mod(143) = **115**
Alice decifra il plaintext P2 =**115**^103 mod (143) = **15**

Esponente b =111
b[0] = 1, risultato= 15
b[1] = 1, risultato= 86
b[2] = 1, risultato= 115
Ciphertext c: 115

Esponente b =1100111
b[0] = 1, risultato= 115
b[1] = 1, risultato= 70
b[2] = 0, risultato= 38
b[3] = 0, risultato= 14
b[4] = 1, risultato= 89
b[5] = 1, risultato= 5
b[6] = 1, risultato= 15
Ciphertext c: 15

2. Fornire in modo chiaro e preciso:
   (a) la definizione di **One Time Pad (OTP)**,
   (b) la definizione di **Sicurezza Perfetta di Shannon**,

   (c) provare che **OTP** è sicuro.
   (d) Specificare la condizione sotto la quale la sicurezza perfetta è garantita (in termine di lunghezza della chiave/plaintext)
   (e) Cosa sarebbe lo svantaggio principale di **OTP**?

(6 punti / 24)

Consultare le slide #5->slide#16 della lezione "OTP and Stream Ciphers"

3. Descrivere in modo chiaro e esaustivo:
   (a) il concetto di **anonimizzazione**,

(b) il **Routing a Cipolla** (**Onion Routing**).
(c) Quest'ultimo meccanismo (**Onion Routing**) come garantisce l'anonimizzazione del traffico sulla rete? (illustrare la risposta con una Figura)

(5 punti / 24)

a) Anonimato: una proprietà che garantisce che un utente possa utilizzare una risorsa o un servizio senza rivelare la propria identità (slide#18 della lezione "Network security: Definitions, Internet security and Anonimity").
b) e c) Consultare le slide#39 -> slide#45 della lezione "Network security: Definitions, Internet security and Anonimity".

4. Unix utilizza un sistema di sicurezza composto da **ACL** (Access Control List) e **Capabilities**.
   (a) Descrivere questi 2 meccanismi (evidenziandone le somiglianze e le differenze).
   (b) Quali sono i vantaggi di implementare **ACL** e **Capabilities** insieme su un sistema informatico?

(5 punti / 24)

a) Consultare le slide#17 e slide#18 e le slide #21 e slide#22 della lezione "System security: authentication - access control".
b) Consultare le slide#23 e slide#24 della lezione "System security: authentication - access control".