Cognome: Nome: Matricola:

## Elementi di Crittografia

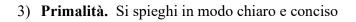
Docente: Paolo D'Arco

Appello del 26 Gennaio 2021

ı			
ı			
ı			
ı			
ı			

- 1) **Riduzioni: metodologia.** Si descriva concisamente la **struttura generale** di una riduzione di sicurezza, evidenziando **le motivazioni** alla base dell'approccio e le **proprietà** che soddisfa. Inoltre, come caso d'esempio, si dimostri che:
  - se G è un PRG, allora lo schema di cifratura che associa il cifrato **c** = G(**s**) ⊙ **m** al messaggio **m**, dove **s** è scelto uniformemente a caso e ⊙ rappresenta l'operazione di XOR bit a bit, è uno schema di cifratura EAV-sicuro.

2)	Segretezza Perfetta. Si dimostri che in ogni schema di cifratura perfettamente si delle chiavi di cifratura deve avere cardinalità maggiore o uguale alla cardinalità messaggi. Inoltre, si spieghi sotto quale condizione lo schema di Vigenere risu segreto.	dell'insieme dei



• come funziona il test di Miller e Rabin e quali risultati della teoria dei numeri utilizza

## 4) Cifratura autenticata. Si spieghi in modo chiaro e conciso

- cos'è e perché è utile
- con quale approccio generico può essere ottenuta
  che relazione sussiste con la nozione di "schema di cifratura simmetrico CCA-sicuro"

5)	Crittosistemi a chiave pubblica. Si discuta la sicurezza delle versioni randomizzate del crittosistema RSA (con random pad) e si presenti lo standard RSA-OAEP, discutendone la sicurezza.

6)	<b>Schemi di identificazione.</b> Si descriva lo schema di identificazione di Schnorr e se ne discuta la sicurezza. Inoltre, si spieghi come possa essere convertito in uno schema di firma digitale.