



ITT Chilesotti – Anno scolastico 2016–2017

## Classe 5- Sistemi e reti

Rispondi in modo esauriente alle seguenti domande.

1. Nell'ambito della Crittografia simmetrica descrivi le caratteristiche salienti del cifrario DES. [2]
2. Quali sono le positività e le negatività della crittografia simmetrica e della crittografia asimmetrica ? [1]
3. Quali furono i metodi di valutazione dell'algorithm AES ? [1]
4. Esplica le 2 modalità di funzionamento (Confidenziale e Autenticazione) e le garanzie offerte da ognuna di esse nella crittografia asimmetrica. [2]
5. Dopo avere spiegato i principali concetti matematici che sono alla base dell'algorithm asimmetrico RSA, esegui il calcolo seguente:
  - dati i numeri  $p=5$ ,  $q=11$ , scegli il numero  $e$ , minore possibile,
  - calcola il numero  $d$ ,
  - specifica la chiave pubblica e la chiave privata che ottieni
  - supponi di trasmettere il messaggio  $m= 7$  quindi cifra e decifra  $m$  utilizzando RSA. [3]