Специјални курс - криптографија, пример испита

1. Шта су једносмерне функције? Навести пример једносмерне функције.

2. ЕлГамалов криптосистем.

3. Дефинисати операције на елиптичкој кривој. Групни закон на елиптичкој кривој.

4. Алиса и Бобан користе Дифи-Хелманов криптосистем са параметрима $p = 29$ и $g = 2$ (2 је генератор $\mathbb{Z}_{29}$).
   а) Ако је Алисин тајни кључ 12 одредити њен јавни кључ.
   б) Бобан је изабрао јавни кључ 5, приказати како он рачуна усаглашени кључ.

5. Одредити све тачке елиптичке криве $y^2 = x^3 + x + 3$ над пољем $\mathbb{Z}_7$.