به نام خدا

آزمونک میدان متناهی درس مبانی امنیت شبکه- بهار ۱۴۰۵

لطفا پاسخ ها را خوانا و شفاف به صورت **دستی روی کاغذ** نوشته و تصویر آن را در قالب فایل PDF بارگذاری کنید. در پاسخ دهی به سوالات استفاده از هرگونه منابع آنلاین و آفلاین **مجاز نمی باشد**. در صورت هر گونه سوال در چت ایلرن سوال خود را بپرسید.

مدت زمان آزمون **۴۵ دقیقه** می باشد و پاسخ های ارسال شده با تاخیر پذیرفته نمی شود.

موفق باشید.

۱-میدان را تعریف کنید.

۲-نشان دهید که برای هر عدد اول p و هر عدد طبیعی $n\geq ۱$، میدانی متناهی با p^n عنصر وجود دارد.

۳-معکوس ضربی x^2+1 در $GF(2^3)$ با چند جمله ای $m(x)=x^3+x-1$ را محاسبه کنید.

۴-چند جمله ای کاهش ناپذیر با درجه ۳ زیر را در نظر بگیرید. با استفاده از آن میدان $GF(2^3)$ را تعریف کنید.

$(x^3+ x^2 + 1)$

۵-دو مولد (ریشه اولیه) برای میدان Z_{17} نام ببرید و نشان دهید که ریشه اولیه هستند.

۶-برای $GF(2^5)$ با چند جمله ای $m(x)=x^5+x^4+x^3+x+1$ اعضای میدان را بر اساس ریشه $m(x)$ بنویسید. به عبارت دیگر نشان دهید توان های ریشه چندجمله ای $m(x)$ همه اعضای میدان $GF(2^5)$ تعریف شده روی این چند جمله ای را تولید می کند.