به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

دانشجو: علیرضا توفیقی محمدی

# تمرین : سری ۵

مدرّس: دکتر شهرام خزائی

شماره‌ی دانشجویی: ۹۶۱۰۰۳۶۳

## مسأله‌ی ۱

## مسأله‌ی ۲

کافی است حمله کننده دو متن دلخواه $m_1, m_0$ را به چالشگر بدهد و سپس بعد از دریافت $c$، حرف آخر $c$ را از ۰ به یک تبدیل کرده و $c'$ را ساخته و سپس $\mathsf{Dec}_k(c')$ را پرسده و اگر $m_1$ بود یک و در غیر اینصورت صفر بدهد و با مزیت یک برنده شود.

## مسأله‌ی ۳

آ)

$$3x + 2 = 19k + 7 \implies 3x = 19k + 5 = 19k' + 24 \implies x = 19k'' + 8$$

ب)

$$Z*_{35} = 35\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 4 \times 6 = 24$$

ج)

$$2^{10001} = (2^{10})^{1}000 \times 2 = 2 \mod 11$$

د)

چراکه $gcd(a,b) = 1$ و یکی از تعاریف ب.م.م این است که: $gcd(a,b) = \min(\{x > 0 | \exists y, z : ay + xz = x\}$.