بسمه تعالی

دانشکده مهندسی کامپیوتر

آمار و احتمال مهندسی

نیم‌سال اول ۱۴۰۰-۱۴۰۱

مدرس: سید ابوالفضل مطهری

امتحان میان‌ترم(ـ نمره)

سوال۱: نمرات امتحان (- نمره)

استاد درسی ، دانشجویان کلاس را با توجه به نمرات تمارین‌شان به دو دسته‌ی متوسط و زرنگ تقسیم کرده است که به ترتیب ۷۰ و ۳۰ درصد کل دانشجویان هستند. احتمال اینکه دانشجویان متوسط و زرنگ در امتحان زیر ۱۰ شوند به ترتیب ۰.۳ و ۰.۱ است. یکی از دانشجویان کلاس را به صورت تصادفی انتخاب می‌کنیم. احتمال آن که این دانشجو در امتحان پایان‌ترم زیر ۱۰ شود به شرط آنکه در امتحان میان‌ترم نیز زیر ۱۰ شده باشد را بیابید. واقعه زیر ۱۰ شدن در میان‌ترم و پایان‌ترم به شرط زرنگ بودن (ونیز به شرط متوسط بودن) را مستقل از هم در نظر بگیرید.

سوال دوم: تابع چکیده ساز (- نمره)

تابع چکیده ساز (hash function) یکی از توابعی است که در رمز نگاری از آن استفاده می‌شود. ورودی این تابع یک پیام به طول دلخواه است و خروجی آن نیز، یک پیام با طول ثابت می‌باشد که به آن hash یا اثر انگشت دیجیتال نیز گفته می‌شود. چون طول ورودی دلخواه است ولی طول خروجی ثابت است بنابراین تابعی یک به یک نیست و ممکن است دو پیام اثر انگشت دیجیتال یکسانی داشته باشند. در چنین حالتی می‌گویند "برخورد" رخ داده است. حمله جستجوی جامع یکی از حملاتی است که به توابع چکیده ساز صورت می‌گیرد. در این حمله اثر انگشت دیجیتال تعداد زیادی پیام محاسبه می‌شود تا برخورد رخ دهد. یعنی دو پیام متفاوت با اثر انگشت یکسان پیدا شود. اگر طول خروجی برابر با N بیت باشد، تعداد حداقل پیام‌هایی که باید اثر انگشت دیجیتال آن‌ها حساب شود تا با احتمال حداقل $\frac{1}{2}$ دو پیام با اثر انگشت یکسان یافت شود را بیابید.

سوال سوم: تاس هرمی (- نمره)

در کیسه بزرگی سه نوع تاس هرمی شکل A,B,C وجود دارد که ظاهرا همگی مثل هم هستند. وجوه تاس‌ها با اعداد ۱و۲و۳و۴ شماره‌گذاری شده است و احتمال ظاهر شدن هر یک از وجه‌های مختلف در هر یک از این تاس‌ها مطابق جدول زیر است:

جدول ۱: مشخصات تاس‌ها

وجه/نوع	A	B	C
۱	۰.۲	۰.۱	۰.۲۵
۲	۰.۳	۰.۷	۰.۳
۳	۰.۴	۰.۰۵	۰.۰۵
۴	۰.۱	۰.۱۵	۰.۴

تاس های A و B و C به ترتیب ۳۰ و ۵۰ و ۲۰ درصد کل تاس ها را تشکیل می‌دهند. بصورت کاملا تصادفی تاسی را از کیسه بر می‌داریم و سپس تاس را می‌اندازیم. بر اساس نتیجه انداختن تاس می‌خواهیم با کمترین احتمال خطا تصمیم بگیریم که تاس از کدام یک از این سه نوع است. بر اساس نتیجه انداختن تاس تصمیم شما در مورد نوع تاس چه خواهد بود و احتمال خطای استراتژی شما چقدر است؟

موفق باشید.