دانشکده‌ی مهندسی کامپیوتر

آمار و احتمال مهندسی

تمرین سری اول

مدرس: دکتر مطهری **مهلت: ۲۲ مهر ساعت ۲۳:۵۵**

سوال ۱

در یک کلاس ۲۰ دانشجو حضور دارند. هر دانشجو مشخص کرده است که به پروژه عملی علاقه دارد یا به پروژه نظری. ۱۰ نفر به پروژه عملی علاقه دارند و ۱۰ نفر به پروژه نظری. می‌خواهیم برای پروژه نهایی درس کلاس را به گروه‌های دو نفری تقسیم کنیم. با فرض اینکه گروه‌بندی به صورت کاملا تصادفی انجام می‌شود به پرسش‌های زیر پاسخ دهید.

الف)

یک سه تایی (Ω, F, P) مناسب به عنوان فضای احتمال تعریف کنید. که Ω فضای نمونه، F مجموعه زیرمجموعه‌هایی از فضای نمونه است که برای آن‌ها احتمال تعریف می‌کنیم. و P تابع احتمال است، یعنی تابعی از F به اعداد حقیقی است که در خواص تابع احتمال صدق کند و در خاصیت کاملا تصادفی بودن هم صدق کند.

ب)

زیر مجموعه‌ای از Ω را تعیین کنید که پیشامد زیر را مدل کند:
هر گروه یا علاقه‌مند به پروژه عملی باشد یا علاقه‌مند به پروژه نظری باشد.

ج)

احتمال پیشامد اول (نوشته شده در قسمت ب) را به دست بیاورید.

سوال ۲

فرض کنید $a_۱, ...a_{۱۰۰}$ یک جایگشت تصادفی از اعداد ۱ تا ۱۰۰ باشند. چقدر احتمال دارد که هیچ یک از اعداد $S_۱ = a_۱ \ , \ S_۲ = a_۱ + a_۲ \ , \ \dots \ , \ S_{۱۰۰} = a_۱ + ... + a_{۱۰۰}$ بر ۳ بخش پذیر نباشند؟

سوال ۳

سیستم رمزنگاری OTP تنها سیستم رمزنگاری است که با یک تعریف ایده‌آل از امنیت، دارای امنیت کامل می‌باشد. این سیستم رمزنگاری بسیار ساده بوده و به این صورت عمل می‌کند که یک کلید دودویی (که

دارای طولی یکسان با پیام اصلی است) را با پیام اصلی xor کرده و پیام رمزشده را ارسال می‌کند. این سیستم دو مشکل اساسی دارد:

۱. طول پیام با طول کلید یکسان است که ویژگی مناسبی برای کلید نیست. در واقع طول کلید زیاد است.

۲. کلید ایجاد شده یک بار مصرف است و نمی‌توان دو بار از کلید استفاده کرد.

برای این که سیستم بهتری برای این کار ایجاد کنیم از یک دستگاه مولد کلید استفاده می‌کنیم. دستگاه مولد کلید یک رشته ۳۲ بیتی و یک کلمه کمکی را به عنوان ورودی دریافت کرده و یک جایگشت دوری از حروف این کلمه را برای تولید کلید استفاده می‌کند. بدین شکل، بر حسب رشته ۳۲ بیتی و جایگشت دوری انتخاب شده کلید به صورت یکتا و بیت به بیت تا طولی دلخواه تولید خواهد شد.
فرستنده، گیرنده و مهاجم هر سه به کلید دستگاه دسترسی دارند و می‌دانند کلمه عبور جایگشتی دوری از حروف کلمه probability است. ولی این که کدام جایگشت دوری از این کلمه برای ایجاد کلید استفاده شده‌است و رشته ۳۲ بیتی چیست برای مهاجم نامعلوم است. اما وی خبر دارد که در جایگشت دوری دو حرف b کنار هم نیستند. اگر مهاجم بتواند در هر ثانیه 10^5 ترکیب مختلف را تست کند، محاسبه کنید که به چقدر زمان نیاز دارد تا با احتمال ۵۰ درصد بتواند رمز عبور را بیابد.

سوال ٤

گزاره‌های زیر را اثبات و یا با زدن مثال نقض رد کنید. دقت کنید که $A \perp B$ یعنی دو پیشامد A و B از هم مستقل هستند.

الف)

$$P(A|B \cap C) = \frac{P(A \cap B|C)}{P(B|C)}$$

ب)

$$P(A_1 \cap A_2 \cap ... \cap A_n) = P(A_1)P(A_2|A_1)...P(A_n|A_1 \cap A_2 \cap ... \cap A_{n-1})$$

ج)

$$A \perp B \Rightarrow (A \perp B)|C$$

د)

$$A \perp B, A \perp C, B \perp C \Rightarrow P(A \cap B \cap C) = P(A)P(B)P(C)$$

ه)

$$(X \perp W|Z \cap Y), (X \perp Y|Z) \Rightarrow (X \perp (Y \cap W)|Z)$$

سوال ۵

در یک مسابقه تلویزیونی یک شرکت‌کننده باید از بین سه جعبه یکی را انتخاب کند. در یکی از جعبه‌ها یک جایزه است و در دوتای دیگر جایزه‌ای نیست. بعد از اینکه شرکت‌کننده جعبه‌ای را انتخاب کرد مجری از بین جعبه‌های باقی‌مانده جعبه‌ای که پشت آن جایزه‌ای نیست را انتخاب می‌کند و پوچ می‌کند. سپس از شرکت‌کننده می‌پرسد که آیا می‌خواد انتخابش را عوض کند یا می‌خواهد جعبه‌ای که انتخاب کرده‌است را نگه دارد. احتمال برنده شدن فرد در صورتی که انتخابش را تغییر دهد و در صورتی که انتخابش را نگه دارد حساب کنید.

سوال ۶

در جعبه‌ای $k+1$ سکه موجود است. برای مقادیر $i = 0, \ldots, k$، احتمال آمدن شیر در پرتاب کردن i مین سکه‌ی جعبه عبارت است از $\frac{i}{k}$. از جعبه یک سکه را به صورت تصادفی انتخاب کرده و آن را n بار پیاپی پرتاب می‌کنیم. اگر نتیجه تمام n پرتاب اول شیر باشد، احتمال شرطی اینکه نتیجه $n+1$ امین پرتاب نیز شیر باشد چقدر است؟