به نام خداوند جان و خرد

امتحان میان‌ترم درس مبانی رایانش امن | نیم‌سال دوم ۴۰۵-۴۰۴

تاریخ: ۱۴۰۵/۰۲/۱۲ | مدت امتحان: ۱۰۰ دقیقه

نام و نام خانوادگی: | شماره دانشجویی:

---

**با سلام و آرزوی موفقیت**

**تعداد سؤال‌ها ۷ و مدت زمان آزمون ۱۰۰ دقیقه است. دقت داشته باشید که قبل از پایان زمان پاسخ‌های خود را در سامانه آپلود کنید.**

**آزمون تشریحی است و نیاز است که مشابه آزمون حضوری پاسخ سؤالات صرفاً روی برگه به‌صورت دستی نوشته شده و از پاسخ‌های خود عکس گرفته و آپلود کنید (پاسخ‌ها به صورت تایپ‌شده قابل قبول نیست).**

**پاسخ هر سوال حتما باید با توضیح و استدلال همراه باشد و صرفا به پاسخ نهایی نمره‌ای تعلق نمی‌گیرد.**

**تشخیص مشابهت غیرعادی بین پاسخ‌های افراد یا تشخیص AI-generated بودن پاسخ‌ها تقلب محسوب می‌شود.**

**در طول آزمون اگر در صورت یا مفهوم سؤالات مشکلی داشتید می‌توانید سؤال خود را به آیدی ۳۶۹۹۷ در پیام‌رسان هما ارسال کنید.**

به نام خداوند جان و خرد

امتحان میان‌ترم درس مبانی رایانش امن | نیم‌سال دوم ۴۰۵-۴۰۴
تاریخ: ۱۴۰۵/۰۲/۱۲ | مدت امتحان: ۱۰۰ دقیقه
نام و نام خانوادگی: | شماره دانشجویی:

## میثاق‌نامه صداقت علمی آزمون

اینجانب رسماً متعهد می‌شوم که در تمام طول این آزمون، اصول صداقت و شرافت علمی را رعایت کرده و این آزمون را تنها با اتکا به دانش و تلاش فردی خود و بدون هیچ‌گونه کمک غیرمجاز به پایان برسانم.

من با آگاهی کامل، موارد زیر را می‌پذیرم و به آن‌ها عمل خواهم کرد:

۱ .تلاش فردی: پاسخ تمام سوالات، حاصل تلاش و دانش شخصی خود من است.

۲ .عدم دریافت کمک: از هیچ شخص دیگری (اعم از همکلاسی‌ها، دوستان، اعضای خانواده یا هر فرد دیگر) به هیچ شکلی (حضوری، تلفنی، پیام‌رسان‌ها و غیره) کمک نمی‌گیرم و به کسی کمک نمی‌کنم.

۳ .عدم استفاده از منابع غیرمجاز: از هیچ منبع غیرمجازی (شامل جزوه، کتاب، یادداشت، وب‌سایت، مقالات، گروه‌ها در شبکه‌های اجتماعی و غیره) استفاده نخواهم کرد، مگر مواردی که صراحتاً توسط استاد درس مجاز اعلام شده باشد.

۴ .عدم استفاده از هوش مصنوعی: متعهد می‌شوم که برای پاسخ به سوالات از هیچ‌گونه ابزار هوش مصنوعی (مانند ChatGPT، Gemini و موارد مشابه)، نرم‌افزارهای حل مسئله یا ابزارهای محاسباتی غیرمجاز استفاده نخواهم کرد.

۵ .عدم به اشتراک‌گذاری اطلاعات: سوالات یا پاسخ‌های آزمون را در حین برگزاری یا پس از آن با دیگران به اشتراک نمی‌گذارم و از هویت کاربری خود برای ورود شخص دیگری به آزمون استفاده نخواهم کرد.

با آگاهی کامل و پذیرش تمامی موارد فوق، این میثاق‌نامه را تأیید می‌نمایم.

به نام خداوند جان و خرد

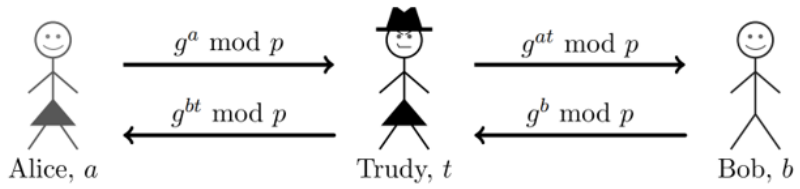
امتحان میان‌ترم درس مبانی رایانش امن | نیم‌سال دوم ۴۰۵-۴۰۴

تاریخ: ۱۴۰۵/۰۲/۱۲ | مدت امتحان: ۱۰۰ دقیقه

نام و نام خانوادگی: | شماره دانشجویی:

---

**۱. ترودی قصد دارد حمله man-in-the-middle را در دیفی-هلمن به‌صورتی تغییر دهد که بتواند یک کلید مشترک بین خودش و آلیس و باب به اشتراک بگذارد. به این منظور سناریوی زیر را طراحی می‌کند. توضیح دهید که آیا ترودی با این سناریو موفق شده است به هدف خود برسد.**




**۲. در یک سیستم مبتنی بر RSA، از یک جفت کلید یکسان برای رمزگذاری پیام‌ها و همچنین امضای دیجیتال استفاده می‌شود. با یک سناریوی ساده توضیح دهید چرا این کار می‌تواند منجر به ضعف امنیتی شود.**

**۳. آلیس با استفاده از مود CBC چهار بلوک پیام P0, P1, P2, P3 را رمز کرده و بلوک‌های متن رمز C0, C1, C2, C3 به همراه IV را برای باب ارسال می‌کند. فرض کنید ترودی قادر است بلوک‌های ciphertext را در مسیر تغییر دهد و همچنین مقدار P1 را می‌داند. نشان دهید که ترودی می‌تواند بدون دانستن کلید، مقدار P1 را با مقدار دلخواه X جایگزین کند (یعنی کاری کند که خروجی رمزگشایی C1 به جای p1 برابر با X شود).**

**۴. یک Block Cipher به صورت زیر پیام را رمز می‌کند:**

$$C_0 = E(IV \oplus P_0, K)$$

$$C_i = C_{i-1} \oplus E(P_i, K) \quad \text{برای } i \geq 1$$

**فرض کنید در حین انتقال، یک بیت از بلوک رمز $C_j$ دچار خطا می‌شود. توضیح دهید این خطا چگونه در فرآیند رمزگشایی انتشار پیدا می‌کند و آن را با رفتار انتشار خطا در CBC استاندارد مقایسه کنید. به‌طور مشخص در هر دو مورد بیان کنید که آیا هر یک از بلوک‌های متن آشکار سالم می‌مانند، به‌صورت کامل خراب می‌شوند، یا فقط یک بیت آن‌ها تغییر می‌کند.**

**۵. فرض کنید آلیس از یک تابع هش رمزنگاری امن با خروجی ۲۵۶ بیتی استفاده می‌کند، اما در یک کاربرد خاص تنها به یک مقدار هش ۱۲۸ بیتی نیاز دارد. به این منظور آلیس دو نیمه‌ی ۱۲۸ بیتی خروجی هش ۲۵۶ بیتی را با هم XOR می‌کند. به نظر شما امنیت این روش نسبت به استفاده مستقیم از یک هش ۱۲۸ بیتی کمتر است یا بیشتر یا مساوی؟ چرا؟**

به نام خداوند جان و خرد

امتحان میان‌ترم درس مبانی رایانش امن | نیم‌سال دوم ۴۰۵-۴۰۴

تاریخ: ۱۴۰۵/۰۲/۱۲ | مدت امتحان: ۱۰۰ دقیقه

نام و نام خانوادگی: | شماره دانشجویی:

**۶. فرض کنید آلیس پیشنهاد می‌دهد برای افزایش امنیت، ابتدا روی پیام یک MAC محاسبه شود و سپس مقدار MAC با استفاده از امضای دیجیتال امضا گردد. توضیح دهید که آیا این روش ویژگی عدم انکار (non-repudiation) را برای پیام فراهم می‌کند؟**

**۷. ترودی یک متن رمز C در اختیار دارد که با کلید عمومی RSA آلیس رمز شده و متن اصلی آن M است. آلیس حاضر است هر متن رمز دیگری غیر از C را برای ترودی با کلید خصوصی خود رمزگشایی کند. با فرض اینکه RSA به‌درستی و بدون ضعف در انتخاب پارامترها پیاده‌سازی شده است و امکان انجام حملاتی از قبیل brute force وجود ندارد، توضیح دهید آیا برای ترودی راهی وجود دارد که بتواند در زمان معقول M را به‌دست آورد؟**

موفق باشید