به نام خدا

درس امنیت داده و شبکه

نیم‌سال اول ۱۴۰۱-۱۴۰۰

دانشکدهٔ مهندسی کامپیوتر

دانشگاه صنعتی شریف

مدرس **مهدی خرازی**

موضوع **رمزنگاری**

موعد تحویل **ساعت ۲۳:۵۹ یکشنبه ۱۴ آذر ۱۴۰۰**

طراحی چالش توسط **سارا عسگری**

با سپاس از **محمد حدادیان**

۱ مقدمه

هدف از این چالش تجربه بیشتر در تحلیل الگوریتم‌های رمزنگاری متقارن و نامتقارن میباشد. این چالش از دو بخش تشکیل شده‌است که کدها و فایل‌های مربوط به هر بخش را می‌توانید از مخزن handouts دریافت کنید. توصیه میشود پیش از حل این چالش ویدئوهای منزل رمزنگاری پرچم را مشاهده کرده و چالش‌های آن را حل کنید.

۲ بخش اول

در این بخش قسمتی از کد مربوط به رمزنگاری یک پیام در اختیار شما قرار داده شده‌است. در این قطعه کد قسمت‌هایی از متن ساده، متن رمزشده، کلید و بردار اولیه حذف شده‌است (کاراکترهای حذف شده با - مشخص شده‌اند). شما باید بتوانید ۱۶ کاراکتر اول متن ساده را به دست بیاورید. بنابراین پرچم در این بخش یک رشته ۱۶ کاراکتری است که از حروف کوچک و بزرگ انگلیسی و اعداد تشکیل شده‌است.

۳ بخش دوم

در این بخش یک فایل zip به شما داده شده‌است که شما با حل مسئله مطرح‌شده در فایل ReadMe میتوانید پسورد این فایل را به دست آورده و آن را از حالت فشرده خارج کنید. پس از آن با یک فایل به نام private_key.pem.aes_enc مواجه میشوید که این فایل رمزشده‌ی یک فایل pem (این فایل حاوی بخش آخر یک کلید خصوصی ۱۰۲۴ بیتی RSA است) با الگوریتم AES است. همچنین کد استفاده‌شده برای این رمزنگاری را میتوانید در فایل encryption.py مشاهده کنید که در این فایل کلید و بردار اولیه حذف شده‌است. شما باید بتوانید فایل private_key.pem را به دست آورید و پس از آن فایل parcham.rsa_enc که با کلید عمومی متناظر با این کلید خصوصی رمز شده‌است را رمزگشایی کرده و به پرچم دست یابید. پرچم در این بخش یک رشته ۳۷ کاراکتری است که از حروف کوچک و بزرگ انگلیسی، اعداد و _ تشکیل شده‌است.

۴ تحویل‌دادنی‌ها

شما باید یک ویدئو با حجم حداکثر ۴۰ مگابایت و مدت زمان حداکثر ۱۵ دقیقه تهیه کنید و در این ویدئو مراحلی که برای حل هر یک از بخش ها طی نموده اید را نشان داده و توضیح دهید. این ویدئو را در یکی از سرویس های میزبانی فایل مانند Google Drive آپلود کنید و سپس لینک آن را در یک فایل به نام links.txt در پوشه ی chals/chal۳ قرار داده و این فایل را به همراه یک فایل به نام parchams.txt که پرچم هر یک از بخش‌ها را در آن قرار داده‌اید در مخزن خود در طرشت push کنید. به علاوه اگر برای هر یک از بخش‌ها اسکریپتی نوشته‌اید آن را به همراه یک گزارش که نحوه‌ی اجرای اسکریپت به صورت کامل در آن توضیح داده شده‌است را در همین پوشه از مخزن خود در طرشت push کنید.