مبانی رایانش امن

تمرین دوم

فایل‌های پاسخ خود را با الگوی HW2-9431XXX-StudentName.pdf نامگذاری نمایید.
در صورت مشاهده تقلب برای طرفین نمره صفر درنظر گرفته خواهد شد.
در صورت وجود هرگونه اشکال یا سوالی از طریق ایمیل alireza97hi@gmail.com موارد را بیان کنید.

ادامه تمرینات فصل دوم

۱.از ایده‌های استفاده شده در رمزنگاری توسط دستگاه انیگما، استفاده از جایگشت حروف انگلیسی است. برای مثال تابع πرا در نظر میگیریم که به صورت زیر تعریف می‌شود:

x	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
$\pi(x)$	۲۳	۱۳	۲۴	۰	۷	۱۵	۱۴	۶	۲۵	۱۶	۲۲	۱	۱۹

x	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵
$\pi(x)$	۱۸	۵	۱۱	۱۷	۲	۲۱	۱۲	۲۰	۴	۱۰	۹	۳	۸

که هر یک از اعداد ۰ تا ۲۵مندرج در جداول بالا بیانگر حروف لاتین متناظر با آن است(شماره صفر بیانگر حرف لاتین a است). برای رمزنگاری یک متن به صورت stream عمل میکنیم. اگر حروفی که به صورت stream وارد می‌شوند را با اندیس i شماره گذاری کنیم i برای حرف اول یک درنظر گرفته می‌شود و با پیش‌روی در حروف، مقدار این اندیس افزایش داده می‌شود. z_iبرای حرف iام ورودی به صورت زیر تعریف می‌شود:

$z_i = (K+i-1) \bmod ۲۶$

برای رمزنگاری و رمزگشایی حرف iام ورودی به صورت زیر عمل میکنیم:

$e(x) = \pi(x) + z \bmod 26$
$d(y) = \pi^{-1}(y - z \bmode 26)$

برای رمزگشایی متون در واقعیت به دلیل نداشتن کلید باید تمام حالت‌های آن را بررسی کرده و بهترین گزینه ممکن را انتخاب کرد. اما برای حل مسئله زیر از بین کلیدهای ۱۰ و ۲۳ یکی به عنوان کلید اصلی است که با رمزگشایی چند حرف از حروف اولیه میتوانید کلید اصلی را تشخیص دهید.
متن زیر را با استفاده از توضیحات بالا رمزگشایی کنید.(برای ساده‌سازی، بین کلمات موجود در متن رمز شده زیر نقطه قرار داده شده و این نقاط جزو اندیس به حساب نمی‌آیند و شمارش اندیس‌ها فقط برای حروف انگلیسی است)

ndgd.bhkzxs.cogbq.bstp

۲.فرض کنید رمزگشایی متن x با کلید k را توسط الگوریتم DES به صورت DES(x,k) نمایش دهیم. اگر تابع c نمایانگر مکمل بیتی باشد و داشته باشیم:

y1 = DES (x,k)
y2 = DES (c(x),c(k))

آنگاه ثابت کنید که y2 = c(y1)

(دقت کنید که این اثبات به s-box و موارد نظیر آن در سطح‌های پیچیده DES ربطی ندارد و از خاصیت توابع استفاده شونده در رمزنگاری DES نشأت می‌گیرد)

۳.در یک رمزنگاری با کمک CFB مراحلی به صورت زیر را دارا هستیم به این صورت که برای رمز کردن یک متن با طول n به یک IV با طول n نیاز داریم و آن را تولید میکنیم و به اولین ciphertext block میدهیم. برای بلاک‌های ciphertext بعدی خواهیم داشت:

$c_1 = x_1 \oplus Enc(I\ V)$

$c_2 = x_2 \oplus Enc(c_1)$

...

$c_i = x_i \oplus Enc(c_{i-1})$

الف) مراحل رمزگشایی(decryption) برای الگوریتم بالا را بیان کنید.
ب) آیا میتوان عمل رمزگشایی را موازی سازی کرد.

تمرینات فصل سوم

۴.ویژگی‌های توابع hash زیر را بیان کنید.
الف) preimage resistant
ب) collision resistant
ج)weak collision resistant

۵.محتوی خانه‌های padding field و length field برای داده‌هایی با طول زیر را که توسط SHA-512 هش شده‌اند را محاسبه کنید.
الف) ۲۰۶۷
ب) ۲۹۴۴
ج) ۳۰۰۰

۶.میخواهیم عدد زیر را توسط الگوریتم RSA رمزنگاری کنیم.برای یافتن کلیدهای مناسب فرض کنید از عددهای اول ۱۳ و ۱۷ برای شروع روند یافتن کلیدها در RSA استفاده میکنیم.پس از مشخص کردن کلیدها، عدد زیر را رمز کنید.(کلیدها حالت‌های مختلفی دارند. انتخاب آن‌ها بر عهده خود شماست)

PlainText = 88

۷.استیو راجرز و تونی استارک با پروتکل DIFFIE-HELLMAN Key Exchange جهت تبادل اطلاعات، ارتباط برقرار می‌کنند. توافق آن‌ها برای موارد عمومی به صورت زیر است:

p (prime) = 5

g (primitive root) = 2

کلیدهای مخفی خصوصی هرکدام به شرح زیر است:

Tony Stark Secret Key -> 4

Steve Rogers Secret Key -> 3

shared secret key بین تونی و استیو را مشخص کنید.

۸.نحوه کار الگوریتم DSS و کاربردهای آن را بیان کنید.