دانشکده مهندسی کامپیوتر

امنیت سیستم‌های کامپیوتری

زمستان ۱۴۰۰

تمرین اول

فصل مقدمات درس

آخرین ویرایش ۱۳ اسفند ۱۴۰۰

استاد درس . . . . . دکتر دیانت

نام . . . . . علی صداقی

شماره دانشجویی ۹۷۵۲۱۳۷۸

فهرست مطالب

۱ زمان حمله Brute-force ۲

۲ انواع رمزهای جانشینی ۴

۳ منابع ۵

۱ زمان حمله Brute-force

در این نوع حملات کل فضای حالت بایستی پیمایش شود. البته در صورتی که پاسخ رسیدیم ادامه فضا را بررسی نمی‌کنیم. اعدادی که در ادامه داده خواهد حالت Worst case می‌باشد. بدیهی است هرچه طول کلید بیشتر باشد فضای حالت نیز بزگ‌تر می‌باشد و این نوع حمله زمان بیشتری برای رمزگشایی نیاز دارد. در این نوع حملات همه حالات ممکن برای کلید یکی یکی بررسی می‌شوند پس طبیعی است که زمان زیادی طول بکشد. در گذشته این عملیات روی CPU صورت می‌گرفت که تعداد هسته کمی داشتند و قدرت TFLOPS آن‌ها پایین بود. امروزه با معرفی کارت‌های گرافیک (GPU) قدرتمند که دارای هسته‌های زیادی هستند و سرعت عملیات اعشاری در آن‌ها زیاد است، این زمان کمتر شده است. سه فاکتور مهم در مدت زمان این حملات شامل الگوریتم، طول کلید و سخت افزار است.

اگر فرض کنیم در کلید از تمامی کاراکترهای موجود در ASCII استفاده شده باشد پس ۹۵ کاراکتر داریم. عامل تاثیرگذار دیگر طول رمز می‌باشد. اگر یک CPU هشت هسته‌ای بخواهد همچین رمزی را بشکند نیازمند زمانی زیاد است. زیرا این سخت افزار تقریبا در هر ثانیه حدود نیم میلیون رمز را امتحان می‌کند، اما فضای حالت مسئله برابر ۸ به توان ۹۵ است.

اگر از یک GPU قدرتمند مانند NVIDIA RTX 3090 که جزو کارت‌های گرافیک جدید این شرکت است استفاده کنیم زمان بسیار کمتری طول خواهد کشید. این سخت افزار می‌تواند تا چند میلیون رمز را در ثانیه امتحان کند. چیزی حدود ۲۷ میلیون رمز در ثانیه با حساب کتابی ساده می‌توان گفت این سخت افزار نیازمند ۶۸۲۰۰ ساعت برای شکاندن رمز است. این عدد معادل ۸ سال زمان است!

یکی از کارهایی که برای کاهش این زمان انجام می‌دهند موازی سازی است. به این ترتیب که از چند کامپیوتر به طور همزمان برای شکاندن یک رمز استفاده می‌کنند. همچنین کامپیوترهای کوانتمی نیز جهش بزرگی در محسابات دارند و قدرت حدس ۶۳ میلیارد رمز در ثانیه را دارند و می‌توانند رمزها را در زمان کوتاه‌تری بگشایند. برای مثال این سیستم‌ها قادر هستند رمز ۸ کاراکتری را در ۳۰ ساعت رمزگشایی کنند. همچنین این عدد برای رمز ۱۰ کاراکتری به ۳۰ سال می‌رسد.

اگر یک سیستم غیرکوانتومی را در نظر بگیریم رمز ۱۰ کاراکتری حدود ۵۲۵ سال زمان می‌برد تا شکسته شود. این زمان برای تعداد کاراکتر پایین بسیار کوتا هست مثلا رمز ۵ کاراکتری در کسری

از ثانیه شکسته می‌شود. اما رمز ۶ کاراکتری حدود ۱۰ ثانیه زمان می‌برد.

۲ انواع رمزهای جانشینی

همانطور که در کلاس درس نیز بررسی شد، در این نوع رمزنگاری به جای یک یا تعدادی از کاراکترها یک یا چند کاراکتر دیگر قرار می‌گیرد. در ادامه چند روش از این نوع رمزنگاری را بررسی می‌کنیم:

- Simple Substitution Cipher: رایج ترین روش است. به ازای هر حرف یک حرف دیگر قرار می‌گیرد. فضای حالت آن معادل ۲۶ فاکتوریل است. این نوع رمزها در برابر تحلیل فرکانسی بسیار شکننده هستند. اگر ترتیب جایگذاری حروف را تعریف کنیم می‌توانیم به رمزنگاری سزار برسیم.
- Poly-gram Substitution Cipher: در این روش بلاک‌هایی از کاراکترها با بلاکی دیگر جابجا می‌شود. یکی از نمونه این نوع جانشینی الگوریتم Hill Cipher است. این نوع رمزنگاری در برابر تحلیل فرکانسی مقاوم است. یک نکته همه دیگر این است که تشابه حروف دو بلاک به معنی تشابه حروف رمز شده نیست. این نوع رمزها در دوران رنسانس بسیار مورد استقبال بودند.
- Homo-phonic Substitution Cipher: در این حالت یک کاراکتر می‌تواند به چند کاراکتر نگاشت پیدا کند. مثلا می‌توانیم یک حرف را با چهار حرف جایگزین کنیم. نمونه معروف این نوع رمزنگاری الگوریتم‌های Beale است.
- Poly-alphabetic Substitution Cipher: در این روش قانون و نگاشت جانشینی ثابت نیست و در طول رشته می‌تواند تغییر کند. مثلا کاراکتر A می‌تواند در ابتدا به P نگاشت شود. اما در تکرار دوم A به M نگاشت شود. رمزنگاری ویگنر و انیگما از این نوع است. این نوع روش‌ها برای اولین بار توسط Leon Battista معرفی شد.

برخی از روش‌های بالا را می‌توان با هم ترکیب کرد و موارد جدید ساخت. مثلا Poly-alphabetic and Homo-phonic

۳ منابع

لینک پروژه لاتک درون فایل LaTeX_Link.txt موجود است.

Link 1

Link 2

Link 3

Link 4

Link 5

Link 6

Link 7

Link 8

Link 9

Link 10