دانشکده مهندسی کامپیوتر

تمرین اول

امنیت سیستم های کامپیوتری

استاد درس: دکتر ابوالفضل دیانت

نیم‌سال اول سال تحصیلی ۱۴۰۱-۱۴۰۰

تمرین ۱

تمرین اول

رامتین احسانی - ۱۴۰۰/۷/۲۳

تمرین اول درس امنیت سیستم های کامپیوتری تهیه شده توسط رامتین احسانی با استفاده از سیستم حروف چینی `LaTeX` و بسته ی `XePersian`

۱.۱ در حال حاضر تا چه میزان می توان در یک زمان معقول حمله Brute-force انجام داد؟

میدانیم که از `Brute-force attack` برای حمله به سیستم ها برای شکستن رمز آن ها و دسترسی **غیر مجاز** به آن ها استفاده میشود. در این نوع حمله تمام حالت های ممکن فضای کلید را امتحان میکنیم تا بالاخره کلید درست را پیدا کنیم. انواع مختلفی از این نوع حمله وجود دارد مانند:

- Simple brute force attack
- Dictionary attacks
- Reverse brute force attack
- ...

۱.۱.۱ میزان درصد حمله های Brute-force

در کل، طبق اطلاعات ثبت شده از حمله های سایبری تایید شده چیزی حدود **۵ درصد** از حمله ها از نوع Brute-force هستند. در صورت استفاده از این روش به احتمال ۱ به ۵ احتمالا موفق خواهید شد.

۲.۱.۱ سرعت

سرعت شکستن رمز با استفاده از Brute-force به دو چیز بستگی دارد:

- قدرت رمز سیستم هدف
- قدرت سیستم حمله کننده

در کل سیستم های حمله کننده میتوانند چیزی حدود ۱۰،۰۰۰ تا **۱ بیلیون** رمز در ثانیه را تست کنند. یک سیستم با سخت افزار `Pentium 100` میتواند ۱۰ هزار رمز را در ثانیه چک کند. در حالی که یک سوپر کامپیوتر با سخت افزار های قوی میتواند تا ۱ بیلیون رمز را در ثانیه امتحان کند.

- چیزی حدود ۹۴ کاراکتر در یک کیبورد استاندارد وجود دارد که در کل میتوانند ۲ بیلیون رمز ۸ کاراکتری به وجود بیاورند.
- هر چقدر این رمز ها رندوم تر و پیچیده تر باشند، شکستن آن ها سخت تر میشود. یک رمز با طول ۹ با کاراکتر های متفاوت چیزی حدود ۲ ساعت طول میکشد تا شکسته شود. اگر کاراکتر ها یکسان باشند چیزی حدود ۲ دقیقه طول میکشد.
- یک رمز با ۱۲ کاراکتر متفاوت به ۳ قرن زمان احتیاج دارد تا شکسته شود!
- یک کلید با **۲۵۶-bit**، 2^{256} حالت مختلف برای حمله کننده ایجاد میکند که شکستن آن به **تریلیون ها** سال احتیاج دارد.

یک رمز ساده حاوی کاراکتر های **lowercase** در سیستمی حاوی `Pentium 100` در ۸.۵ ساعت شکسته میشود و در یک سوپر کامپیوتر این اتفاق با سرعت بسیار زیادتر و تقریبا بلافاصله صورت میگیرد. با افزایش طول رمز، زمان لازم برای شکستن آن به صورت **نمایی** بیشتر میشود.

۲.۱ انواع رمزهای جانشینی

در این نوع از رمزگذاری، جایگاه حروف در یک متن بهم نمی خورد، تنها هر حرف یا گروهی از حروف با یک حرف یا گروهی دیگر از حروف جابجا می شوند. در این گزارش انواع این رمز ها را معرفی میکنم.

۱.۲.۱ Mono-alphabetic Cipher

انواع:

- Atbash Cipher
- ROT13 Cipher
- Caesar Cipher
- Affine Cipher
- Baconian Cipher
- Polybius Square Cipher
- Simple Substitution Cipher
- Codes and Nomenclators Cipher

برای مثال، الگوریتم `ROT13` همان الگوریتم سزار با شیفت ۱۳ است. این الگوریتم ها بخاطر سادگی که دارند در جاهای حساس استفاده خاصی ندارند و بیشتر در `Online Forum` ها برای مخفی کردن متن ها استفاده میشوند.

۲.۲.۱ Homophonic Substitution Cipher

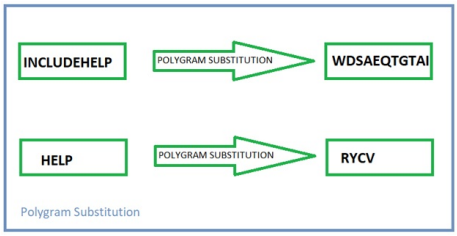
انواع:

- Beale ciphers

این نوع الگوریتم ها مانند `Mono-alphabetic Cipher` هستند با این تفاوت که یک حرف به چند حرف تبدیل میشود. `Beale ciphers` یک نوع از این الگوریتم ها است که مکان یک گنج را در داخل ۳ متن مخفی کرده است.

۳.۲.۱ Polygram Substitution Cipher

در این نوع از سایفر، بلوکی از کلمات با بلوکی از کلمات دیگر جایگزین میشوند.



شکل ۱.۱: Polygram Substitution Cipher

انواع:

- Four-Square Cipher
- Hill Cipher
- Caesar Cipher
- Playfair Cipher

بریتانیا از الگوریتم `Playfair cipher` در جنگ جهانی اول استفاده کرد.

۴.۲.۱ Polyalphabetic Substitution Cipher

همانطورکه از اسم مشخص است این الگوریتم ها چند الفبایی هستند. انواع:

- Autokey Cipher
- Beaufort Cipher
- Porta Cipher
- Running Key Cipher
- Enigma Cipher
- Vigenère and Gronsfeld Cipher

الگوریتم ویگنر را در کلاس بررسی کردیم. الگوریتم `Autokey cipher` فرقی کوچکی با ویگنر دارد که وقتی کلید مشخص شد، برای رمزگشایی از خود PlainText هم در کلید استفاده میکنیم. مثال: کلید ما **FORTIFICATION** است.

```
FORTIFICATIONDEFENDTHEEASTWA
DEFENDTHEEASTWALLOFTHECASTLE
```

شکل ۲.۱: Autokey Cipher

با تشکر، تهیه شده توسط رامتین احسانی

Bibliography

[1] Wikipedia, "Brute-force." https://en.wikipedia.org/wiki/Brute-force_attack.

[2] Imperva, "Brute-force." https://www.imperva.com/learn/application-security/brute-force-attack/.

[3] Forcepoint, "Brute-force." https://www.forcepoint.com/cyber-edu/brute-force-attack.

[4] Varonis, "Brute-force." https://www.varonis.com/blog/brute-force-attack/.

[5] Wikipedia, "Substitution cipher." https://en.wikipedia.org/wiki/Substitution_cipher.

[6] PracticalCryptography, "Substitution cipher." http://practicalcryptography.com/ciphers/substitution-category/.

[7] IncludeHelp, "Substitution cipher." https://www.includehelp.com/cryptography/substitution-techniques.aspx.