امنیت سیستم های کامپیوتری

تحلیل رمز و ابزار های آن

مقدمه

دولت‌ها مدتهاست که مزایای احتمالی رمزنگاری را برای اطلاعات، اعم از نظامی و دیپلماتیک و سازمانهای اختصاصی مستقر در زمینه شکستن رمزها و رمزهای سایر ملل، به عنوان مثال، GCHQ و NSA، سازمانهایی که هنوز هم بسیار فعال هستند، تأسیس کرده‌اند.

اگرچه در زمان جنگ جهانی دوم از محاسبات برای تأثیرگذاری در رمزنگاری رمزنگاری لورنز و سایر سیستمها استفاده شده‌است، اما همچنین روشهای جدید دستورات رمزنگاری از بزرگی را پیچیده‌تر از گذشته کرده‌است. به‌طور کلی، رمزنگاری مدرن نسبت به سیستم‌های قلم و کاغذ گذشته، نسبت به سیستم رمزنگاری و کاغذ گذشته بسیار غیرقابل نفوذ است، و حالا به نظر می‌رسد که دست بالایی در برابر رمزنگاری خالص دارد. مورخ دیوید کان یادداشت می‌کند:

> امروزه بسیاری از سیستمهای رمزنگاری شده توسط صدها فروشنده تجاری ارائه شده‌اند که با هیچ روش شناخته شده‌ای از رمزنگاری قابل شکستن نیستند. در واقع، در چنین سیستم‌هایی حتی یک حمله متن ساده، که در آن متن متن انتخابی با متن متن آن مطابقت دارد، نمی‌تواند کلید باز کردن پیام‌های دیگر را ارائه دهد؛ بنابراین به یک معنا، رمزنگاری مرده‌است. اما این پایان داستان نیست تحلیل رمز ممکن است مرده باشد، اما برای مخلوط کردن استعاره‌های من - بیش از یک راه برای پوست کردن گربه وجود دارد.

تعریف تحلیل رمز

به بررسی متون رمز شده، رمز ها و سیستم های رمزگذاری با هدف درک چگونگی کار کردن آنها و پیدا کردن یا بهبود روشهایی برای شکست یا تضعیف آنها گویند.

روش های و راه حل های متفاوتی برای تحلیل رمز داریم که به طور مثل، یکی از مرسوم ترین روش های آن، حمله از طریق رو های مثل chosen plaintext ،brute force و man in the middle است که در اینجا این 3 را بررسی میکنیم:

- brute force : یک روش و تکنیک قدیمی است که تمامی حالات ممکن برای رمز را انتخاب میکند تا به رمز مورد نظر برسد که البته در حال حاضر، شکستن رمز های جدید که به وسیله تکنیک های رمزنگاری مدرن درست شدن، بسیار زمان بر و وقت گیر است.

به طور مثال اگر رمز ما از 3 رقم تشکیل شده باشد، در این روش تمامی 10*10*10 حالت ممکن را برای رمز مورد نظر بررسی میکند.

- chosen plaintext : در این روش، attacker ورودی های مختلفی را به سیستم رمزنگاری میدهد و ciphertext های هر ورودی را دریافت میکند.حال با بررسی جفت های ciphertext و ciphertext، میتواند حدس بزند که کلید رمزنگاری برابر با چیست.

به طور مثال، در روشی که توانسته اند به الگوریتم RSA حمله کنند، از این راه حل استفاده کردین.

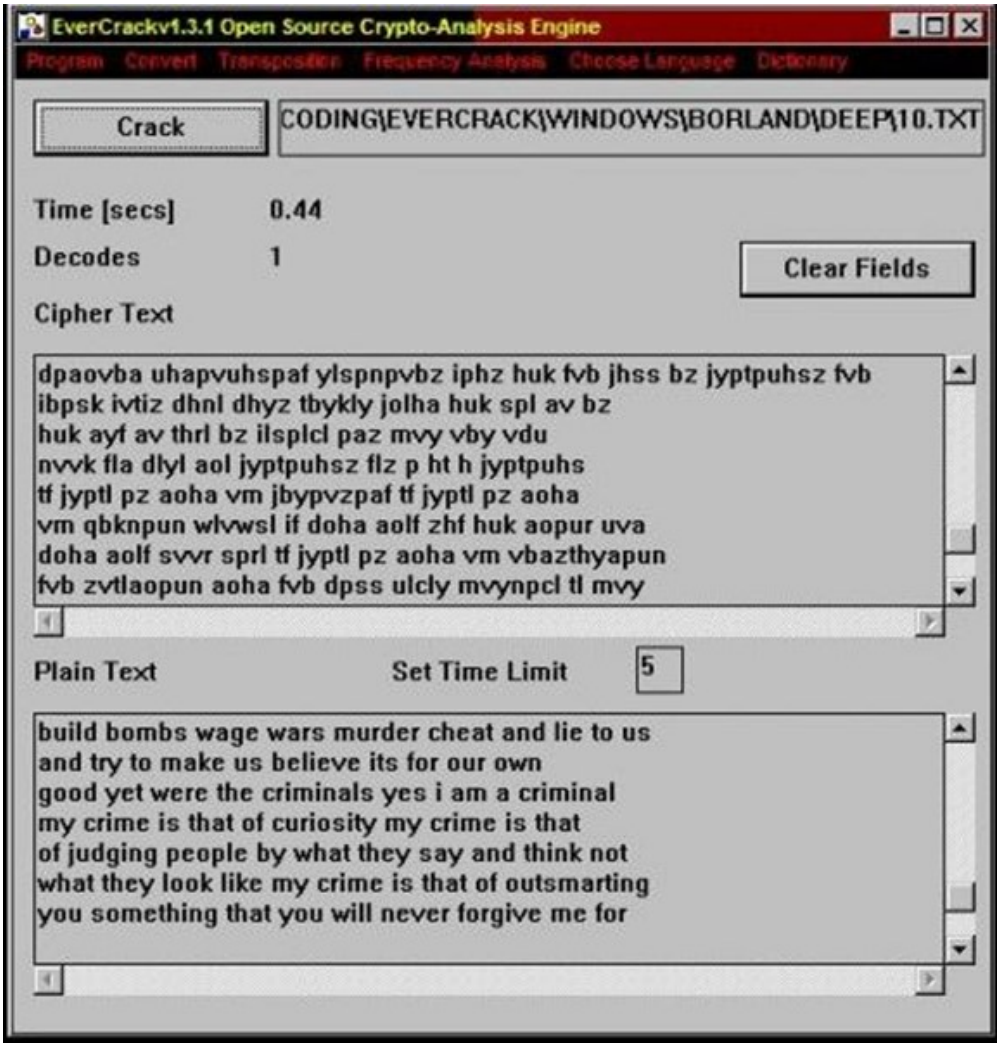
- man in the middle : در این نوع حمله، Eve هر دوی Alice و Bob به سخره میگیره. Alice کسی است که میخواهد با Bob ارتباط برقرار کند و روی کلید عمومی خود تکیه میکند. در این بین Eve هویت خود را جعل میکند و و خود را بین Bob و Alice قرار میدهد.

در اینجا الیس کلید عمومی خود را برای باب ارسال میکند ولی در این بین، Eve این کلید عمومی را دریافت میکند و خود را جای باب جا میزند و فرایند تبادل کلید را با Alice شروع میکند. از طرفی، Eve کلید عمومی خود را برای Bob ارسال میکند و خود را به عنوان Alice جا میزند و فرایند تبادل کلید را با Bob نیز شروع میکند.

حال وقتی Alice پیامی را برای Bob ارسال میکند، چون با رمزی که در تشکیل آن Eve دخالت کرده،Eve میتواند تمامی متن ارسالی را بخواند و دوباره آن را با کلیدی که با Bob تبادل کرده رمز میکند و برای Bob ارسال میکند. با اینکه Alice و Bob به صورت کامل با هم ارتباط برقرار میکنند ولی در این وسط تمامی پیام ها توسط Eve هم قبول مشاهده است.

- EverCrack

یک نرم افزار متن باز EverCrack ،GPL عمدتاً با جایگزینی و جابجایی رمزهای تک الفبایی سر و کار دارد. این یک موتور تحلیل رمزنگاری با پشتیبانی چند زبانه از انگلیسی، آلمانی، فرانسوی، اسپانیایی، ایتالیایی، سوئدی، هلندی و پرتغالی است. در ابتدا به زبان C توسعه داده شد. در حال حاضر بر روی برنامه های کاربردی مبتنی بر وب آنلاین متمرکز شده است. اکنون، برنامه نویسی مبتنی بر هسته است، یعنی رمزگشایی رمزهای پیچیده برای هسته. هدف کلی طراحی این است که رمزهای پیچیده را به صورت سیستماتیک به اجزای سیمپلکس آنها برای تحلیل رمز (توسط هسته) تجزیه کنیم. هسته از یک طرح جبری (مقایسه و کاهش) برای شکستن رمزهای تک الفبایی یک طرفه به صورت آنی تشکیل شده است. سرعت محاسبات با log O(n) متناسب است. یک EverCrackGUI مانند شکل زیر به نظر می رسد.



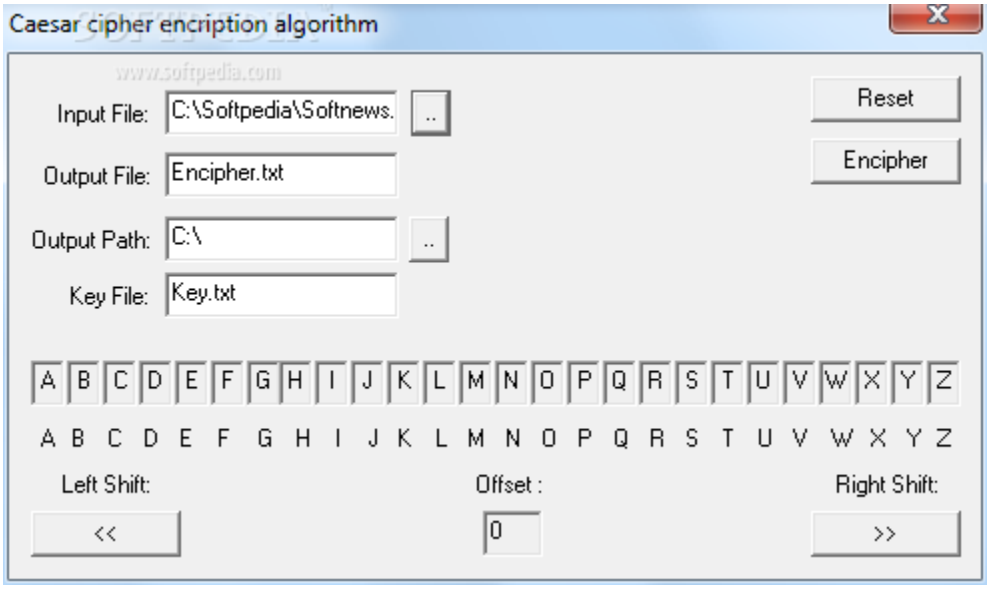
- **AlphaPeeler**

AlphaPeeler یک محصول نرم افزار رایگان / غیرتجاری برای استفاده آموزشی و شخصی است. توسعه آن در سال 1997 آغاز شد و AlphaPeeler 1.0 در ژوئن 1998 به کار گرفته شد. شامل موارد زیر است:

MD5, SHA – 1, RSA key generation, RIPEMD – 16

رمزهایی مانند Playfair در اینجا مورد مطالعه قرار می گیرند.

Alpha Peeler Professional 1.0 بتا در 4 جولای 2001 در مالکیت عمومی منتشر شد. Alpha Peeler با هدف خاصی برای ارائه به روزترین تحقیقات برای کمک به شرکت ها، فروشندگان و اپراتورها برای ایمن سازی محیط تجاری و توسعه خود تاسیس شد. گروه توسعه Alpha Peeler همچنین طیف گسترده ای از راه حل های فناوری نرم افزار را ایجاد می کند که در بخش خدمات فهرست شده است. به عنوان توسعه نرم افزار، تجزیه و تحلیل و طراحی سیستم، مستندسازی و طراحی گرافیک.



Crypto Bench

Crypto Bench نرم افزاری است که عملکردهای مختلف رمزنگاری را انجام می دهد. می تواند 14 هش رمزنگاری و دو چک سام تولید کند. این می تواند با 29 کلید مخفی مختلف یا طرح های متقارن رمزگذاری کند. می تواند با شش کلید عمومی مختلف یا طرح نامتقارن رمزگذاری، رمزگشایی، امضا و تأیید کند.