تمرین دوم امنیت سیستم های کامپیوتری

امیررضا ویشته - ۹۹۵۲۲۲۲۱ و عرفان زارع - ۹۸۴۱۱۴۳۲

ابان ۱۴۰۲

سوال اول تمرین ۱:

امروزه بهترین cpu ها و gpu های مرسوم در جامعه و موجود قدرت محاسباتی حدود، ۴۰ ترا فلاپس دارند. برای مثال AMD Ryzen 9 5950X قدرت محاسباتی مغادل ۷۴۹ گیگافلاپس دارد و این تعداد را در ثانیه محاسبه می نماید.

از طرفی gpu همچون NVIDIA GeForce RTX 3090 قدرت محاسباتی ۶.۳۵ ترا فلاپس را دارد .البته این اعداد بسته به شرایط و موقعیت و و بازدهی، میتواند کمتر هم باشد. این درحالی است که سوپرکامپیوتر هایی همچون Fugaku) ، قدرت محاسباتی حدود ۴۴۲ پتافلاپس دارد. (داده ها و نکات بیان شده در منابع موجود است و عکس بنچمارک cpu,gpu اولیه، بدلیل عدم وضوح درست تصویر، گذاشته نشده است ولی در لینک موجود می باشد.) درمقام مقایسه دیگر، یک کارت گرافیک GeForce GTX 460 تقریباً ۴ برابر عملکرد یک CPU Core i5-2500K را دارد . در این مورد GeForce GTX 460 می‌تواند حدود ۱۸،۱۰۵ رمز عبور در ثانیه را با استفاده بررسی کند، در حالی که Core i5-2500K تنها می‌تواند ۴۷۵۲ رمز عبور در ثانیه را بررسی کند. برای حملات Brute-Force GPU ها به دلیل داشتن تعداد زیاد هسته‌های محاسباتی ، نسبت به CPU (که معمولاً دارای چندین هسته است) سرعت بسیار بالاتری دارند. این ویژگی باعث می‌شود □□□ ها بتوانند عملیات رمزگشایی را با سرعت بسیار بالاتری انجام دهند. بنابراین، با توجه به توانایی‌های فعلی GPU CPU، می‌توان گفت که حملات Brute-Force با سرعت بسیار بالاتر و کارآمدتری نسبت به گذشته انجام می‌شوند. البته باید توجه داشت که سرعت و کارآمدی این حملات به بسیاری از عوامل دیگر نظیر نوع رمز عبور و الگوریتم رمزگذاری نیز بستگی دارد و مسلما شکاندن رمز پیچیده، سختی و زمان بیشتری نیاز دارد.

SUPERCOMPUTER FUGAKU - SUPERCOMPUTER FUGAKU, A64FX 48C 2.2GHZ, TOFU INTERCONNECT D

Site:	RIKEN Center for Computational Science
System URL:	https://www.r-ccs.riken.jp/en/fugaku/project
Manufacturer:	Fujitsu
Cores:	7,630,848
Processor:	A64FX 48C 2.2GHz
Interconnect:	Tofu interconnect D
Installation Year:	2020
Performance	
Linpack Performance (Rmax)	442.01 PFlop/s
Theoretical Peak (Rpeak)	537.21 PFlop/s
Nmax	21,288,960
HPCG [TFlop/s]	16,004.5

References:

- https://www.top500.org/system/179807/
- https://gadgetversus.com/processor/amd-ryzen-9-5950x-specs/
- https://gadgetversus.com/graphics-card/nvidia-geforce-rtx-3090-specs/
- https://www.tomshardware.com/reviews/wireless-security-hack,2981-8.html
- fhttps://securityboulevard.com/2022/05/brute-force-attacks-what-you-need-to-know/
- https://security.stackexchange.com/questions/118147/how-are-gpus-used-in-brute-force-attacks

سوال دوم تمرین ۱

در جنگ جهانی اول، آلمان ها از سامانه رمزگذاری "Transposition Double" استفاده می‌کردند. این الگوریتم رمزگذاری به روش جابجایی اطلاعات و کلمات در متن اصلی بر اساس یک الگوی خاص اقدام می‌کند. در این روش، ابتدا یک الگوی جابجایی مشخص می‌شود. سپس متن اصلی بر اساس این الگوی جابجایی مورد تغییر قرار می‌گیرد. در این جابجایی، هر قسمت از متن به جایگاه دیگری در متن منتقل می‌شود. برای مثال، فرض کنید متن اصلی "HELLO WORLD" باشد و الگوی جابجایی به صورت "۲-۵-۳-۱-۴" تعیین شده باشد. در این صورت، ابتدا حرف اول به جایگاه دوم، حرف دوم به جایگاه پنجم، حرف سوم به جایگاه سوم، حرف چهارم به جایگاه اول و حرف پنجم به جایگاه چهارم منتقل می‌شوند. بنابراین، متن رمزگذاری شده به صورت "LHLOE LWRDO" خواهد بود. فواید این روش رمزگذاری این است که الگوی جابجایی به عنوان کلید رمزنگاری نقش ایفا می‌کند و تغییر الگوی جابجایی می‌تواند باعث تولید رمزهای متفاوت شود. این روش به دلیل سادگی ، آسیب‌پذیری زیادی نیز دارد و به راحتی قابل شکستن است. در ادامه جنگ جهانی اول، روش‌های قوی‌تری برای رمزنگاری معرفی شدند و استفاده از "Transposition Double" کم شد. رمزگذاری جابجایی شامل جابجایی حروف یا مجموعه ای از متن است تا پیامی مخفی شود. در حالت Transposition Double، متن بر اساس یک الگوی خاص و مشخص جابجا می‌شود

فرایند رمزگذاری با استفاده از Transposition Double با انتخاب یک الگوی جابجایی انجام می شود. این الگو مشخص می‌کند که چگونه متن اصلی قرار است رمزگذاری شود. الگو می‌تواند یک دنباله اعداد یا هر نوع دستور دیگری باشد.

بعد از تعیین الگو، متن اصلی بر اساس الگوی جابجایی تغییر شکل می‌یابد. هر بخش از متن بر اساس دستورات الگو به یک موقعیت دیگر در متن منتقل می‌شود. این بازترتیب دادن معمولاً به صورت مرحله به مرحله و به ترتیب متن انجام می‌شود.

برای رمزگشایی پیام، گیرنده نیاز به دانستن الگوی جابجایی استفاده شده برای رمزگذاری دارد. با اعمال الگوی جابجایی معکوس، متن می‌تواند به حالت اصلی خود برگردانده شود.

۱ تمرین ۱: سوال سوم

در ابتدا، تعداد هر یک از حروف زبان انگلیسی در متن را محاسبه می نماییم که کد آن در فایل پیوست موجود است. آنگاه با توجه به اینکه الگوریتم رمزنگاری متن ، از نوع مستوی هست ، پس الگوریتم ما به شکل $AX + B = \{alphabet\} \mod 26$ است . ما میدانیم حروف پرتکرار در زبان انگلیسی، شامل A, E, C می باشند. پس ابتدا ، مقادیر پرتکرار ترین حروف هارا مطابق آن ها درنظر میگیریم. سپس با توجه به آنکه متن ما با جایگذاری این حروف تاحدی داری معنا شد،(در تعداد کمی از حرف های دو تا سه حرفی، یا کلماتی پرتکرار در نگارش متن) انگاه می آییم و بررسی میکنیم که آیا اگر مقادیر A, B موجود در فرمول،را با استفاده از دو حرف A, E محاسبه نماییم ، ابتدا به مقادیر و خروجی می رسیم؟ (مقادیری ما به ازای آن ها هست؟) و سپس به سراغ جایگذاری اعداد و فرمول ها و به دست آوردن کلمات دیگر میرویم. درنهایت طبق توضیحات بالا، هرکدام از حروغ کلید که به همراه تکرارشان در سمت راست آمده اند، معادل حروف سمت چپ اند. مقدار $A = 3$ و $B = 10$ می باشد .

K :58	$\rightarrow A$
W :52	$\rightarrow E$
Q :47	$\rightarrow C$
X :47	$\rightarrow N$
J :46	
P :41	
T :42	
R :38	
I :36	
M :32	$\rightarrow S$
A :30	
D :26	$\rightarrow P$
N :19	
E :19	
U :18	
Z :18	
V :18	
C :17	$\rightarrow G$
F :16	
B :12	$\rightarrow X$
Y :11	
S :10	
O :5	
G :1	
H :0	
L :0	

در نهایت با جایگذاری نکات بالا در متن ، به خروجی با معنای زیر میرسیم.

Plain_text:

g is expected to support data rates of terabyte per second this level of capacity and latency will be unprecedented and will extend the performance of g applications along with expanding the scope of capabilities in support of increasingly new and in novative applications across the realms of wireless connectivity cognition sensing and imaging g higher frequencies will enable much faster

sampling rates in addition to providing significantly better throughput and higher data rates the combination of sub mm wave eg wave lengths smaller than one milli meter and the use of frequency selectivity to determine relative electromagnetic absorption rates is expected to lead to potentially significant advances in wireless sensing technology additionally where as the addition of mobile edge computing is a point of consideration as an addition to g networks mobile edge computing will be built in to all g networks edge and core computing will be come much more seamlessly integrated as part of acombined communications computation infrastructure framework by the time g networks are deployed this will provide many potential advantages as g technology becomes operational including improved access to artificial intelligence capabilities.