دانشکده مهندسی کامپیوتر

تمرین رادیوم (تمرین اول فصل دوم)

امنیت سیستم‌های کامپیوتری

مدرس: دکتر ابوالفضل دیانت

محمدحسین عباسپور، فرزان رحمانی

شماره دانشجویی: ۹۹۵۲۱۴۳۳، ۹۹۵۲۱۲۷۱

نیم سال دوم
سال تحصیلی ۱۴۰۳-۱۴۰۲

سوال ۱: امروزه تا چه میزان می‌توان در یک زمان معقول حمله Brute-force انجام داد؟ هدف از این سوال این است که بگویید CPU یا GPUهای فعلی تا چه میزان می‌توانند محاسبات را در ثانیه انجام دهند؟ به عنوان نمونه یکی دو مدل به همراه Becnhmark آن مثال بزنید.

برای شکستن رمز به وسیله الگوریتم Brute-force به:

۱. تعداد عملیات مورد نیاز برای شکستن رمز

۲. سرعت کامپیوتر و یا به عبارتی FLOPS

نیاز داریم.

مورد اول به عبارتی بیانگر فضای جستجوی کلید میباشد و مورد دوم هم بیانگر قدرت محاسبه‌گری کامپیوتر در واحد زمان میباشد؛ یا به عبارتی کامپیوتر در یک ثانیه چند عملیات اعشاری را می‌تواند انجام دهد. امروزه کامپیوترهایی با قدرت 10^{18} FLOPS وجود دارد. به عنوان مثال ۵ مورد از ابرکامپیوترهای حال موجود در شکل ۱ آورده شده است. برای مثال رمزی که نیاز به 10^{22} عملیات دارد، در ۱۰۰۰۰ ثانیه توسط کامپیوتر ذکرشده قابل شکستن است. همچنین باید در نظر

Rank	Supercomputer	Country	Teraflops
1	Fugaku	Japan	442,010
2	Summit	USA	148,600
3	Sierra	USA	94,640
4	Sunway Taihulight	China	93,014
5	Selene	USA	63,460

tera- = 10^12
peta- = 10^15
exa- = 10^18

شکل ۱: ۵ ابرکامپیوتر برتر دنیا

داشت که رمز در حداکثر چه مدت زمانی باید شکسته شود؛ اگر آن مدت زمان کمتر از ۱۰۰۰۰ ثانیه باشد آنگاه نمیتوان آن را توسط Brute-force شکست؛ یا به عبارتی رمز غیرقابل شکستن است.

- البته کامپیوترهای کوانتومی بسیار سریع‌تر هستند ولی به همان اندازه هم گرون قیمت‌تر میباشند.

سوال ۲: آلمان‌ها در طول جنگ جهانی اول از یک سامانه رمزگذاری به نام Double Transposition استفاده می‌کردند. در مورد این الگوریتم تحقیق کنید و به طور مختصر آن را توضیح دهید.

الگوریتم رمزگذاری Double Transposition یکی از رمزهای دستی بسیار ایمنی بود که در جنگ جهانی استفاده میشد. این الگوریتم توسط هر دو طرف متحدان و محور به کار گرفته میشد و به خوبی عمل می‌کرد. اما نقطه ضعف اصلی آن این بود که اگر حمله‌کننده دو یا بیشتر پیام‌هایی با همان طول و با استفاده از همان کلید را از دسترس برد، می‌توانست با یک فرآیند خسته‌کننده به نام "آناگرام‌گیری چندگانه" راه‌حال‌هایی برای هر دو پیام پیدا کند. این ضعف مهم نبود اگر فقط یک پیام با هر کلید ارسال میشد. همچنین، اجرای صحیح این الگوریتم نیاز به دقت زیاد داشت و اگر در نقطه‌ای حساس خطا اتفاق می‌افتاد، رمزگشایی دشوار میشد. در ایالات متحده، اطلاعات مربوط به CryptoAnalyse این رمز تا چند سال پیش محرمانه بود. الگوریتم دوگانه تبدیل از دوبار استفاده از تبدیل ستونی برای یک پیام تشکیل شده است. این دو بار ممکن است از همان کلید برای هر دو مرحله استفاده کنند یا ممکن است از کلیدهای متفاوتی استفاده کنند. حال به عنوان مثال میخواهیم متن "attackxatxdawn" را رمزگذاری کنیم: x) بیانگر فاصله بین کلمات میباشد)

حمله در سحر

۱. ابتدا یک جدول اولیه با ابعاد مشخص درست میکنیم؛ سپس حروف متن را به ترتیب داخل جدول قرار میدهیم:

	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

شکل ۲: مرحل اول Double Transposition

۲. در مرحله بعد یک جایگشت از ستون‌ها و یک جایگشت از ردیف‌ها را انتخاب میکنیم. به عنوان مثال برای:

ستون‌ها (۲، ۳، ۱) و برای ردیف‌ها (۲، ۴، ۱، ۵، ۳)

	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

شکل ۳: مرحله دوم Double Transposition

۳. در مرحله آخر حروف را به ترتیب کنار هم مینویسیم. متن رمزگذاری شده برابر است با:

xtawxnattxadakc

سوال ۳

با استفاده از تحلیل فرکانسی تک حرف‌ها و دو حرف‌ها را میشماریم:

```
Counter({'W': 125, 'I': 100, 'P': 92, 'X': 85, 'K': 84, 'A': 76, 'M': 58, 'R': 56, 'J': 49, 'Q': 48, 'T': 40, 'C': 37, '
D': 34, 'U': 31, 'F': 23, 'S': 20, 'Z': 20, 'N': 17, 'Y': 17, 'E': 16, 'V': 13, 'B': 4, 'O': 4, 'G': 2})
--------------------------------------------------------------------------------------------------------------------------
Counter({'PI': 28, 'IX': 25, 'PW': 22, 'AX': 18, 'KP': 17, 'WQ': 16, 'WM': 16, 'KX': 16, 'WJ': 15, 'QA': 15, 'RW': 14, '
PF': 13, 'JW': 13, 'IA': 13, 'XC': 13, 'WT': 12, 'WX': 12, 'IR': 12, 'RR': 12, 'XP': 12, 'PA': 11, 'JK': 11, 'AZ': 11, '
IP': 11, 'FW': 11, 'AJ': 10, 'XT': 10, 'MI': 10, 'AU': 10, 'MW': 9, 'QK': 9, 'YI': 9, 'RI': 9, 'KR': 9, 'TI': 9, 'XW': 9
, 'WR': 8, 'XQ': 8, 'XM': 8, 'WK': 8, 'WP': 8, 'TP': 7, 'IQ': 7, 'MK': 7, 'KM': 7, 'MM': 7, 'CX': 7, 'XK': 7, 'KT': 7, '
DW': 6, 'QP': 6, 'JP': 6, 'PK': 6, 'VW': 6, 'KD': 6, 'NI': 6, 'XA': 6, 'JA': 6, 'MP': 6, 'UD': 6, 'IM': 5, 'DA': 5, 'TK'
: 5, 'KJ': 5, 'KN': 5, 'RA': 5, 'DK': 5, 'NW': 5, 'QW': 5, 'TW': 5, 'UK': 5, 'RE': 5, 'XI': 5, 'IC': 5, 'DS': 5, 'SP': 5
, 'UW': 5, 'CW': 5, 'CI': 4, 'WB': 4, 'DD': 4, 'MA': 4, 'FI': 4, 'KQ': 4, 'DJ': 4, 'DR': 4, 'CY': 4, 'CP': 4, 'AD': 4, '
ZI': 4, 'AV': 4, 'IV': 4, 'VI': 4, 'AC': 4, 'IU': 4, 'CF': 4, 'ZJ': 4, 'WU': 4, 'QF': 4, 'TT': 4, 'WW': 4, 'YA': 4, 'JO'
: 4, 'BD': 3, 'MS': 3, 'EP': 3, 'WD': 3, 'ZQ': 3, 'QI': 3, 'PE': 3, 'RK': 3, 'RN': 3, 'WA': 3, 'MQ': 3, 'IW': 3, 'YK': 3
, 'VK': 3, 'KC': 3, 'US': 3, 'SQ': 3, 'KU': 3, 'IT': 3, 'IZ': 3, 'WC': 3, 'AR': 3, 'IK': 3, 'UA': 3, 'TC': 3, 'PY': 3, '
OM': 3, 'AM': 2, 'SD': 2, 'NE': 2, 'JM': 2, 'MR': 2, 'EK': 2, 'QE': 2, 'EY': 2, 'WS': 2, 'SX': 2, 'JZ': 2, 'JU': 2, 'CK'
: 2, 'QJ': 2, 'WY': 2, 'XX': 2, 'IJ': 2, 'WG': 2, 'GS': 2, 'SW': 2, 'MY': 2, 'ZK': 2, 'CJ': 2, 'EN': 2, 'UN': 2, 'UU': 2
, 'KV': 2, 'MU': 2, 'UI': 2, 'EM': 2, 'PJ': 2, 'AP': 2, 'TV': 2, 'FX': 2, 'CE': 2, 'AN': 2, 'AK': 2, 'TQ': 2, 'PT': 1, '
ZP': 1, 'WV': 1, 'TR': 1, 'XD': 1, 'TY': 1, 'BP': 1, 'ZA': 1, 'ZC': 1, 'CR': 1, 'EX': 1, 'RU': 1, 'UM': 1, 'ZY': 1, 'EQ'
: 1, 'CC': 1, 'NR': 1, 'FZ': 1, 'CM': 1, 'PR': 1, 'PP': 1, 'FJ': 1, 'AS': 1, 'SC': 1, 'FD': 1, 'TF': 1, 'JT': 1, 'ZM': 1
, 'SN': 1, 'NU': 1, 'UY': 1, 'FM': 1, 'FK': 1, 'SM': 1, 'ZZ': 1, 'AT': 1, 'NM': 1, 'JD': 1, 'DP': 1, 'XJ': 1, 'XY': 1, '
YF': 1, 'ZU': 1, 'AI': 1, 'WN': 1, 'NS': 1, 'SI': 1, 'RP': 1, 'RC': 1, 'FU': 1, 'UR': 1, 'EI': 1, 'MD': 1, 'XZ': 1, 'JS'
: 1, 'PS': 1, 'SJ': 1, 'WZ': 1, 'ON': 1, 'AE': 1, 'EW': 1, 'RD': 1, 'XE': 1, 'ED': 1, 'MC': 1, 'QR': 1, 'RS': 1, 'ST': 1
, 'QQ': 1})
```

شکل ۴: تحلیل فرکانسی متن

حال با استفاده از جداول ۶ و ۵ پر تکرارترین حروف و بایگرام‌های داخل متن را به ترتیب با پر تکرارترین حروف و بایگرام‌های در انگلیسی جایگزین میکنیم و تست میکنیم که آیا متن معنادار میشود یا خیر. به عنوان مثال حرف w که پر تکرارترین متن میباشد با حرف e جایگزین میشود. و به همین ترتیب.

No	Unigram	Frequencies	No	Unigram	Frequencies
1	TH	2.71	16	OR	1.06
2	HE	2.33	17	EA	1.00
3	IN	2.03	18	TI	0.99
4	ER	1.78	19	AR	0.98
5	AN	1.61	20	TE	0.98
6	RE	1.41	21	NG	0.89
7	ES	1.32	22	AL	0.88
8	ON	1.32	23	IT	0.88
9	ST	1.25	24	AS	0.87
10	NT	1.17	25	IS	0.86
11	EN	1.13	26	HA	0.83
12	AT	1.12	27	ET	0.76
13	ED	1.08	28	SE	0.73
14	ND	1.07	29	OU	0.72
15	TO	1.07	30	OF	0.71

شکل ۵: پر تکرار ترین بایگرام های انگلیسی

Letter	Frequency
e	12.7
t	9.1
a	8.2
o	7.5
i	7.0
n	6.7
s	6.3
h	6.1
r	6.0
d	4.3
l	4.0
c	2.8
u	2.8
m	2.4
w	2.4
f	2.2
g	2.0
y	2.0
p	1.9
b	1.5
v	1.0
k	0.8
j	0.15
x	0.15
q	0.10
z	0.07

شکل ۶: پر تکرار ترین حروف انگلیسی

متن اصلی پس از رمزگذاری به شکل زیر خواهد بود:

گشایی

GIS EXPECTED TO SUPPORT DATA RATES OF TERABYTE PER SECOND THIS LEVEL OF CAPACITY AND LATENCY WILL BE UNPRECEDENTED AND WILL EXTEND THE PERFORMANCE OF GAPPLICATIONS AL ON GWI THE XPANDING THE SCOPE OF CAPABILITIES IN SUPPORT OF INCREASINGLY NEW AND INNOVATIVE APPLICATIONS ACROSS THE REAL MS OF WIRELESS CONNECTIVITY COGNITIONSENSING AND IMAGING HIGHER FREQUENCIES WILL ENABLE MUCH FASTER SAMPLIN GRATES IN ADDITION TO PROVIDING SIGNIFICANTLY BETTER THROUGH PUT AND HIGHER DATA RATES THE COMBINATION OF SUBMMWAVEEG WAVE LENGTHS SMALLER THAN ON EMILLIMETER AND THE USE OF FREQUENCY SELECTIVITY TO DETERMINE RELATIVE ELECTRO MAGNETIC ABSORPTION RATES IS EXPECTED TO LEAD TO POTENTIALLY SIGNIFICANT ADVANCES IN WIRELESS SENSING TECHNOLOGY ADDITIONALLY WHERE AS THE ADDITION OF MOBILE EDGE COMPUTING IS APOINT OF CONSIDERATIONAS AN ADDITIONTOGNET WORKS MOBILE EDGE COMPUTING WILL BE BUILT IN TO ALL GNET WORKS EDGE AND CORE COMPUTING WILL BECOME MUCH MORE SEAMLESSLY INTEGRATED AS PART OF A COMBINED COMMUNICATIONS COMPUTATION INFRASTRUCTURE FRAMEWORK BY THE TIME GNET WORKS ARE DEPLOYED THIS WILL PROVIDE MANY POTENTIAL ADVANTAGES AS GTECHNOLOGY BECOMES OPERATIONAL INCLUDING IMPROVED ACCESS TO ARTIFICIAL INTELLIGENCE CAPABILITIES

شکل ۷: متن اصلی پس از رمزگشایی