## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

### Гоголєва Поліна ФБ-12

# Експериментальна оцінка ентропії на символ джерела відкритого тексту

**Мета роботи:** Засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела.

## Хід роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

Єдиний пункт, з котрим не було проблем і складнощів! (формули налякали not gonna lie)

1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку Н1 та Н2 за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення Н1 та Н2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення Н1 та Н2 на тому ж тексті, в якому вилучено всі пробіли.

Для початку напишемо частину коду, що буде загружати текст з файлу та фільтрувати його відносно вимог методички, цитую: «всі символи, окрім текстових, повинні вилучатись або замінюватись на пробіли; прописні літери — замінюватись на відповідні стрічні; послідовність пробілів (або інших розділових знаків, наприклад, символів кінця рядку) повинна трактуватись як один пробіл або вилучатись, якщо пробіл не входить до алфавіту.»

Як текстовий файл я обрала біблію, там води точно більше ніж на 1Мб.

```
import re
file_path = r"C:\Users\Polya\Desktop\KPI\crypto-23-24-
main\tasks\cp1\solution\bible.txt"
with open(file_path, "r") as file:
    cleaned_text = ''
    for line in file:
        line = re.sub(r'[^a-яА-ЯёЁ]', ' ', line)
        # Видалення зайвих пробілів
        line = ' '.join(line.split())
```

```
cleaned_text += line
print (cleaned text)
```

print написала просто щоб потестити чи все правильно працює, бідний пітон ледь не вмер друкуючи всю біблію, але все працює, а всі послідовності символів і пробілів замінились на один пробіл.

```
file_nath = r"C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cpl\solution\bible.txt"

3 file_nath = r"C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cpl\solution\bible.txt"

4

CUTPUT FROBLEMS FORTS DEBUG CONSOLE TERMINAL

PS C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cpl\solution> c; cd 'c:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cpl\solution'; & 'c:\Users\Polya\
```

Тепер рахуватимемо частоти букв і біграм.

Отримуємо частотний аналіз літер у Біблії (моя віруюча бабуся зараз напевно у захваті, що я цікавлюсь Біблією). Для цього створимо словник зі значенням літера:її кількість у тексті, прогоним весь алфавіт через цикл і додаватимо до countera одиничку щоразу, як зустрічатимемо літеру.

```
import re
file_path = r"C:\Users\Polya\Desktop\KPI\crypto-23-24-
main\tasks\cp1\solution\bible.txt"
with open(file_path, "r") as file:
    cleaned_text = ''
    for line in file:
        line = re.sub(r'[^a-яА-ЯёЁ]', ' ', line)
        # Видалення зайвих пробілів
        line = ' '.join(line.split())
        cleaned_text += line.lower()
print (cleaned_text)

letter_counts={}
for letter in cleaned_text:
    if letter in letter_counts:
        letter_counts[letter] += 1
```

```
else:
```

```
letter_counts[letter] = 1
sorted_letter_counts = dict(sorted(letter_counts.items(), key=lambda item:
item[1], reverse=True))
```

(тут я поняла, що одна літера upper case і та ж літера lower case вважається за дві різні літери алфавіту і спростила собі життя, переводячи весь текст у нижній регістр).

Тож так ми дізнались, що літера «о» зустрічається у Біблії 356734 разів:

```
o: 356734
и: 291640
e: 286468
a: 238995
T: 184448
c: 181963
н: 179485
B: 162454
л: 142902
p: 130840
д: 115654
M: 105539
y: 85409
п: 83962
κ: 83675
г: 72282
я: 66468
ы: 61791
6: 60470
3: 52460
ь: 50037
x: 35422
ч: 32969
й: 31287
ж: 29909
ш: 25191
ю: 23439
ц: 15517
щ: 11862
φ: 5835
э: 3240
ъ: 458
ë: 89
```

Тепер рахуватимемо частотність біграм з перетином і без, принцип як і у минулому пункті, але беремо по два символи і ітеруємо через кожні 2( у випадку без перетину) або 1(у випадку з перетином) символ.

Нюанси: При обрахунках ми від довжини тексту віднімаємо 1, оскільки для підрахунку біграм потрібно розглядати пари символів, і останній символ не може бути початком нової біграми.

Також для підрахунту частот біграм з перетином ми витягаємо пару символів з тексту, розпочинаючи з індексу і і закінчуючи індексом і + 2. Це створює

біграму з перетином, оскільки дві послідовні пари символів будуть мати одну спільну літеру (перший символ наступного біграму  $\epsilon$  останнім символом попереднього).

### Вийшло щось отаке:

```
bigram with overlap counts = {}
bigram without overlap counts = {}
for i in range(len(cleaned text) - 1):
    #Підрахуємо частоту біграм з перетином
    bigram with overlap = cleaned text[i:i + 2]
    if bigram with overlap in bigram with overlap counts:
        bigram with overlap counts[bigram with overlap] += 1
    else:
        bigram with overlap counts[bigram with overlap] = 1
    if i % 2 == 0:
        #І без перетину
        bigram without overlap = cleaned text[i:i + 2]
        if bigram without overlap in bigram without overlap counts:
            bigram without overlap counts[bigram without overlap] += 1
        else:
            bigram without overlap counts[bigram without overlap] = 1
sorted bigram with overlap counts =
dict(sorted(bigram with overlap counts.items(), key=lambda item: item[1],
reverse=True))
sorted bigram without overlap counts =
dict(sorted(bigram without overlap counts.items(), key=lambda item: item[1],
reverse=True))print("Частотний аналіз біграм з перетином:")
for bigram, count in sorted bigram with overlap counts.items():
    print(f"{bigram}: {count}")
print("Частотний аналіз біграм без перетину:")
for bigram, count in sorted bigram without overlap counts.items():
    print(f"{bigram}: {count}")
```

Вивід виявився величеньким і не вміщався у термінал, тому я закинула його у текстові файли, щоб була візуалізація і було з чого робити таблички частотності і прибрала прінт, приблизно отак це виглядало для кожної з функцій

```
with open("letters_count.txt", "w") as letters_file:
```

```
letters_file.write("Частотний аналіз літер у тексті:\n")
for letter, count in sorted_letter_counts.items():
    letters file.write(f"{letter}: {count}\n")
```

Тому тепер у мене  $\epsilon$  файлики з частотним аналізом біграм і літер. Так як ми вважаємо, що пробіл  $\epsilon$  частиною нашого алфавіту, то його частотність теж підраховується і біграми формату «пробіл-літера» теж існують.

```
bigram_without_overlap_counts.txt — Блокнот
Файл Правка Формат Вид Справка
и : 54722
и: 40926
c: 33160
o: 31847
в: 31266
e : 31024
а: 27668
п: 27305
н: 26648
го: 23436
во: 19101
по: 19023
o: 19019
я : 18996
на: 18861
то: 18664
ст: 18518
ь : 17530
ни: 17387
т: 15462
T: 15129
oc: 15110
```

Ну тепер треба створити таблички частот букв та біграм, для більш зручної візуалізації і та сприйняття даних.

# Таблиця частот букв:

Символ	Частотність
пробіл	640177
О	356734
И	291640
е	286468
а	238995
Т	184448
С	181963
Н	179485
В	162454
Л	142902
р	130840
Д	115654
М	105539
У	85409
П	83962
К	83675
Γ	72282
Я	66468
Ы	61791

б	60470
3	52460
Ь	50037
Х	35422
Ч	32969
й	31287
ж	29909
Ш	25191
ю	23439
ц	15517
щ	11862
ф	5835
Э	3240
ъ	458
ë	89

Таблицю частот біграм так просто не перепишеш, тому я модифікувала код так, щоб він сам створював та виводив матрицю. Але вивід виявився нечитабельним, бо просто не вміщався на екран

Тому я вирішила експортувати результати у файли, додавши у код отаку функцію

```
def save_matrix_to_file(matrix, file_name):
    with open(file_name, "w") as output_file:
        alphabet = sorted(sorted_letter_counts.keys())
        output_file.write(f" |" + "|".join(f"{letter:^5}" for letter in alphabet) + "|\n")
        for letter1 in alphabet:
        row = []
        for letter2 in alphabet:
        bigram = letter1 + letter2
        count = matrix.get(bigram, 0)
```

```
row.append(f"{count:^5}")

output_file.write(f"{letter1} |" + "|".join(row) + "|\n")

# Зберігаємо матрицю біграм з перетином

save_matrix_to_file(bigram_with_overlap_counts,
"bigram_with_overlap_matrix.txt")

# Зберігаємо матрицю біграм без перетину

save_matrix_to_file(bigram_without_overlap_counts,
"bigram without overlap matrix.txt")
```

## Запустили і отримали такі результати для біграм з перетином:

```
| 10 | R
6 | 392 |6903
     3588 | 2613
     3025
     3258
     1810
     2226 11405
    1162
0
    11538 | 6850
     4291 | 6905
     2244
     512 | 6143
5052 | 2041
     11176
    326 |13046|
          2676
     317
      13
           13
           0
      24
          111
     511 250
                 (на один екран все одно не вмістилось вибачте)
```

# І для біграм без перетину:

<ul> <li>bigram_without_overlap_matrix.txt — Блохнот</li> </ul>													3 ×																		
Φ	Файл Правка Формат Вид Справка																														
		a	6	В	Г	Д	e	ж	3	И	й	K	Л	M	н	0	п	l p	c	т	<b>у</b>	ф	×	ц	ч	ш	щ	Ъ	ы	Ь	Э
	0	3784	13007	31266	11464	14170	9982	4615	7387	40926	0	13713	3856	12780	26648	19019	27305	5633	33160	15129	7092	675	2641	2394	7446	825	69	0	0	0	1494
a	27668	861	1353	7709	1996	4024	2422	1781	5758	2488	1642	6438	12448	7161	5972	451	1375	6593	5635	5851	338	635	2094	43	1230	2190	436	0	0	0	7
6	521	873	108	114	4	19	3712	5	5	1501	0	16	2562	56	493	7160	0	2866	84	9	3092	0	16	6	3	12	136	143	5230	84	0
В	13261	9593	18	183	9	446	10761	0	802	6133	0	98	1507	254	1061	19101	168	1761	5114	185	1760	19	153	95	156	1131	2	0	4629	722	0
г	1592	2202	6	21	14	2171	560	0	6	1637	0	16	1137	0	943	23436	10	1360	24	7	850	2	2	0	28	19	0	0	0	0	0
Д	3636	10526	20	1239	8	88	11760	1	31	5110	0	124	1583	118	3666	7007	72	1610	460	150	4409	0	22	1139	12	142	37	10	1507	2309	2
	31024		4441	4093	9559	5338	2461	1742	1694	1152	4648	2217	11456	10474	13534	305	1372	9315	9406	10045	142	527	1513	613	2001	1729	689	0	0	0	10
ж	125	1336	54	5	53	1993	5951	192	0	3620	0	41	3	2	796	38	0	96	3	0	406	0	0	0	36	0	0	0	0	74	0
3	2946	8017	483	1696	298	1042	2129	23	294	503	0	86	970	312	2139	1030	6	1953	3	5	484	2	0	4	4	1	0	17	780	358	0
И	54722	747	2274	3383	602	3490	5692	413	5943	2982	2337	3900	11385	7413	5249	1364	621	1617	7052	8612	902	335	6552	1440	734	1179	835	0	0	0	11
	11027		24	75	15	838	26	3	9	324	0	48	6	44	451	43	57		1172	949	17	2	6	69	11	207	0	0	0	0	4
K	7767	9958	10	231	3	4	533	168	1	3833	0	68	961	3	465	12417	15	2686	122	1101	1508	2	30	1	3	13	0	0	0	0	0
	13105		82	49	126	76	8458	551	11	15090	0	208	156	82			59	5	1308	78	2267	14	47	4	152	13	6	0		3471	3
	14267		29	150	46	43	7442	6	26	6284	0	180	2043		2904		125	215	441		5327	26	7	20	40	4	42	0	1518	344	4
Н	6901	18861		13	204		16390		16	17387	0	127	1			11992		29	447		2306	8	21	375	156	2	190	0	5286	1641	0
0	31847		6165				5744	3151	2752	5001	4498	3400	7348	7755	9747	216			15110			412	629		1853	1543	309	0	0	0	45
П		2031	0	0	0		2527	0	0	1616	0	86	1444	0		19023		11905			1541	14	0	22	15	60	6	0	264	132	0
p		13855		466	265		11533	374	211	8950	0	141	117	137		12562		105		1312		26	178	71	50	404	26	0		1038	1
	4823			5175	31		9266	34	11	3525	0	6987	6410			4756				18518		56	353	109	279	84	0	55		3276	0
	15462		40	7883	19		9352	2	8	6311	0	573	174	83		18664			2446		1557	23	33	682	177	18	36	0		9276	2
У	12547		1007	828	1379	5987		1799	438	559		1634		1524	286		1482		3702	2609	14	41	863	36	1085	1408	621	0	0	0	7
φ	316		0	6	2	4	322	0	2	525	0	5	29	5	14	205	3	144	52	10	100	54	1	0	0	1	0	0	45	25	0
X	9681		30	371	35	52	405	6	23	1075	0	56	382	42	161	2690	90	927	173	80	347	3	8	8	14	11	0	0	0	0	3
ц			0	78	6	1	1546	0	0	70	0	2	2	3	1		11	6	4	4	334	4	0	1	0	0	0	0	460	0	1
ч		2166	0	0	0	0	4536	0	3	2419	0	69	33	16	753	97	3	216	0	4967	488	0	0	5	0	143	0	0	0	438	0
Ш		1710	11	17	1	2	3593	0	0	3255	0	56	1080	4	437	212	9	0	8	10	407	3	5	40	0	7	0	0	0	1393	0
Щ	17	846	0	42	0	0	2562	0	0	2008	0	0	0	0	88	3	0	13	0	1	299	0	0	0	0	0	0	0	0	49	0
Ъ	0	0	0	0	0	0	67	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	11027		97	1325	36	188	2039	44	33		2279	312	2479		3536	37	131	314	997	653	4	1	2160	5	248	1268	74	0	0	0	0
ь	17530		33	141	37	219	409	5	107	409	0	486	3	775	1194	62	87	11	1395	414	13	6	3	168	12	307	30	0	0	0	3
Э		0	0	0	3	2	0	0	0	0	1	0	7	2	2	0	1	3	1	1601	0	0	3	3	0	1	0	0	0	0	0
	7023	31	484	51	60	687	18	43	54	292	0	39	9	19	189	47	59	5	163	1117	14	1	0	3	126		1062	0	0	0	5
	18996		67	579	117	250	399	125	639	495	171	646	1223	1037	1515	89	129	128	454	3446	26	7	339	198	448		1328	0	0	0	7
ë	45	0	0	0	0	0	0	0	0	0	0	0	1	0	2	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

) э	ю	Я	ë	
1494	203	3408	0	
7	1780	1293	1	
0	0	1514	0	
0	0	1597	0	
0	0	1	0	
2	5	931	0	
10	1116	727	0	
0	0	0	0	
0	16	595	0	
11	779	3410	0	
4	1	12	0	
0	0	0	0	
3	2223	3437	0	
4	0	1126	0	
0	240	3010	0	
45	2518	1014	0	
0	0	593	0	
1	452	1653	0	
0	146	6526	38	
2	2	992	0	
7	1343	96	0	
0	0	19	0	
3	1	12	0	
1	0	0	0	
0	0	0	0	
0	0	0	0	
0	0	0	0	
0	0	163	0	
0	8	6	0	
3	635	878	0	
0	0	0	0	
5	52	11	0	
7	254	132	0	
0	0	0	0	

Таблиці частотності отримали, тож видаляємо функцію для друку матриць, щоб на це не витрачався час при кожному запуску.

Тепер нам треба знайти за означенням H1 та H2, тобто ентропію для окремих літер і для біграм у тексті, але у формулі імовірності замінити відповідними частотами, що ми тільки що знайшли.

Ентропія тексту обчислюється як сума ентропій для кожної літери (H1) або біграми (H2) окремо. Тобто ми обчислюємо ентропію для кожного можливого символу або біграми в тексті і потім сумуємо ці значення. Це дає

загальну ентропію тексту і вказує на ступінь невизначеності або «непередбачуваності» тексту.

Загальні формули для ентропії:

$$H1(X) = -\sum_{i=1}^{n} P(x_i) \cdot \log_2(P(x_i))$$

# $H2(X) = -\sum_{i=1}^{n} P(bigram_i) \cdot \log_2(P(bigram_i))$

Ну а у нашому випадку, ми замість P(xi) і P(bigram) ставитимо обраховане значення частоти для цієї літери або біграми.

Пройшла ніч і я зрозуміла, щоб не порушувати логіку формули ентропії ми можем розрахувати ці ймовірності, просто поділивши частотність літер/біграм на загальну кількість літер/біграм. Бо просто замінивши значення Р на частотність навряд вийде розрахувати ентропію за означенням, бо ми викинемо логічну частину формули. Тому мій розрахунок виглядає так:

```
# Підрахунок ентропії для літер (Н1)
entropy letter = 0.0
total_letters = len(cleaned_text)
for count in sorted_letter_counts.values():
   probability = count / total letters
    entropy letter -= probability * math.log2(probability)
print(«H1 у тексті з пробілами:», entropy letter)
# Ентропія для біграм з перетином (Н2)
entropy bigram with overlap = 0.0
total bigrams with overlap = len(cleaned text) - 1
for count in sorted bigram with overlap counts.values():
   probability = count / total bigrams with overlap
    entropy bigram with overlap -= probability * math.log2(probability)
print («H2 з перетином у тексті з пробілами:», entropy bigram with overlap)
# Ентропія для біграм без перетину (Н2)
entropy bigram without overlap = 0.0
```

```
total_bigrams_without_overlap = len(cleaned_text) // 2

for count in sorted_bigram_without_overlap_counts.values():
    probability = count / total_bigrams_without_overlap
    entropy_bigram_without_overlap -= probability * math.log2(probability)

print(«H2 без перетину у тексті з пробілами:»,
entropy_bigram_without_overlap)
```

## Запустимо і збережемо значення:

```
esktop\KPI\crypto-23-24-main\tasks\cp1\solution\entropy.py'
H1 у тексті з пробілами: 4.345653112220377
H2 з перетином у тексті з пробілами: 7.893956273614829
H2 без перетину у тексті з пробілами: 7.893911836431902
PS C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cp1\s
```

Тепер виконаємо ті ж самі розрахунки, але попередньо вилучивши всі пробіли з тексту. Для цього створю окремий файл.

Код виглядатиме так само, просто з трошки зміненим кодом фільтрації тексту

```
with open(file_path, «r») as file:
    cleaned_text = ''
    for line in file:
        line = re.sub(r'[^a-яА-ЯёЁ]', '', line) # Вилучення всіх символів
окрім літер
        cleaned_text += line.lower()
print (cleaned text)
```

### Тепер наш текст виглядатиме отак

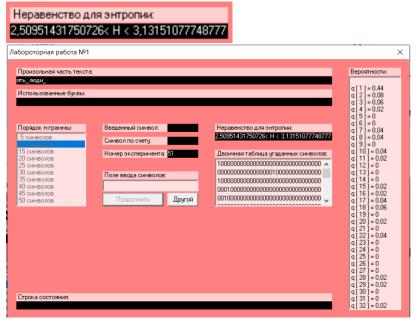
PS C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cp1\solution> & 'C:\Users\Polya\AppData\Local\Programs\Python\Python\Python.exe' 'c:\Users\Polya\\ranger\python.exe' 'c:

## А значення ентропії:

```
esktop\KPI\crypto-23-24-main\tasks\cp1\solution\entropy_without
H1 у тексті без пробілів: 4.433878685419472
H2 з перетином у тексті без пробілів: 8.242649200341408
H2 без перетину у тексті без пробілів: 8.242535867621065
PS C:\Users\Polya\Desktop\KPI\crypto-23-24-main\tasks\cp1\solut
```

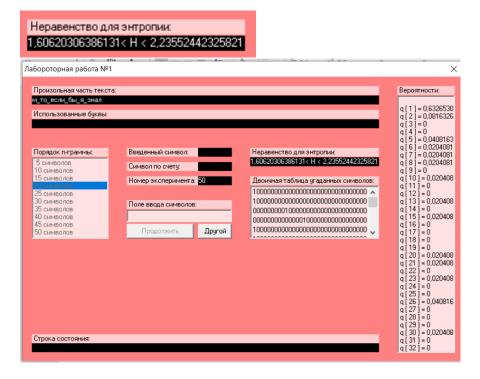
- 2. За допомогою програми CoolPinkProgram оцінити значення (10)Н, (20)Н, (30)Н.
  - Оцінюємо значення для 10 символів:

## Нерівність для ентропії:



• Для 20 символів:

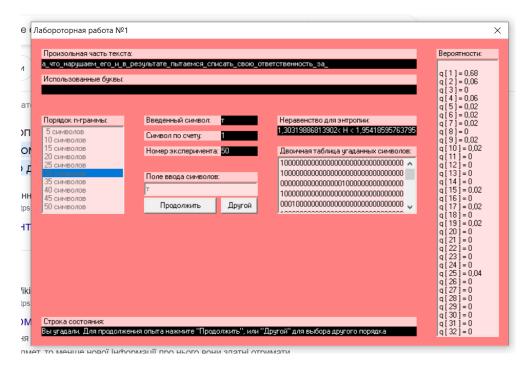
## Нерівність для ентропії:



Для 30 символів:

Нерівність для ентропії:





За моїми спостереженнями, чим більше символів ми бачимо – тим менше загальне значення ентропії = менша «хаотичність» і невизначеність тексту.

3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела.

Надлишковість джерела відкритого тексту (мови) розраховується за формулою:

```
R=1-\frac{H_{\infty}}{H_0} , де ми прийматимемо за H(inf) наші розраховані значення
```

```
r_for_monograms = 1 - (entropy_letter/math.log2(total_letters))

r_for_bigram_with_overlap = 1 -
(entropy_bigram_with_overlap/math.log2(total_bigrams_with_overlap))

r_for_bigram_without_overlap = 1 -
(entropy_bigram_without_overlap/math.log2(total_bigrams_without_overlap))

print(«Надлишковість для монограм:»,r_for_monograms)

print(«Надлишковість для біграм з перетином:»,r_for_bigram_with_overlap)

print(«Надлишковість для біграм без перетину: «,r_for_bigram_without_overlap)
```

## Результат:

```
Н1 у тексті з пробілами: 4.345653112220377
Н2 з перетином у тексті з пробілами: 7.893956273614829
Н2 без перетину у тексті з пробілами: 7.893911836431902
Надлишковість для монограм: 0.8013513691606089
Надлишковість для біграм з перетином: 0.6391512180027582
Надлишковість для біграм без перетину: 0.6218680704424144
```

Тепер розрахуємо це значення для джерела без пробілів.

```
esktop\KPI\crypto-23-24-main\tasks\cp1\solution\entropy_without_sp
H1 у тексті без пробілів: 4.433878685419472
H2 з перетином у тексті без пробілів: 8.242649200341408
H2 без перетину у тексті без пробілів: 8.242535867621065
Надлишковість для монограм: 0.7948574270390547
Надлишковість для біграм з перетином: 0.6186367692678757
Надлишковість для біграм без перетину: 0.6001417514266217
```

#### Висновки

Під час виконання цієї лабораторної роботи я не тільки покращила свої навички у програмуванні, а й зрозуміла, чому значення ентропії і надлишковості  $\epsilon$  важливими у кібербзпеці, а не нас просто вирішили задовбати вищою математикою.

Як ми визначили, ентропія - це міра невизначеності чи непередбачуваності. У контексті тексту ентропія вимірює, наскільки випадковим є розподіл символів чи біграм у тексті (у нашому випадку, можна так то рахувати триграми і т.д.) . Чим більше ентропія, тим більше невизначеність та непередбачуваність.

Різниця ентропій для тексту з пробілами та без пробілів може бути пояснена тим, що пробіли - це також символи, котрі вважаються частиною алфавіту, і вони додаються до загальної кількості символів у тексті. Якщо текст має багато пробілів, то розподіл символів буде менш випадковим, оскільки пробіли будуть домінувати серед інших символів. Таким чином, ентропія тексту з пробілами буде нижчою порівняно з текстом без пробілів.

Надлишковість - це міра того, наскільки розподіл символів чи біграм у тексті відрізняється від рівномірного розподілу. Висока надлишковість вказує на невизначеність мови та може бути використана для криптографічних цілей, так як важко передбачити наступний символ. Висока надлишковість джерела мови вказує на те, що мова має багато невизначеності та непередбачуваних залежностей між символами чи біграмами. Це означає, що для побудови криптосистеми буде складно передбачити, які символи чи біграми випадуть наступними, що робить шифрування більш надійним перед атакою.

В криптографії, ентропія та надлишковість важливі, оскільки вони впливають на стійкість криптосистем. Висока ентропія тексту робить його складнішим для аналізу і підірвання. Надлишковість джерела мови може використовуватися для побудови надійних шифрів, де важко передбачити, який символ або біграм вийде наступним.

Тож ми розібрались з базовими поняттями та принципами роботи криптографії та надійності шифрування, було весело ©