Геш-функції та коди автентичності

Домашній комп'ютерний практикум №1

Геш функція згідно варіанту RIPEMD-320

ФІ-03 Кобець Денис

Мета роботи

Дослідити криптографічні властивості геш-функцій, засвоїти еталонні оцінки стійкості геш-функцій, перевірити на практиці теоретичні положення.

Хід роботи

Основне завдання практикуму: провести атаку випадкового пошуку прообразу та атаку днів народжень на задану геш-функцію, експериментально оцінити складності даних атак.

Атака прообразів 1:

1.1. Сформувати повідомлення, яке повинно містити ваше повне ПІБ. Зафіксувати геш-значення даного повідомлення.

1.2. *Перший варіант атаки.* Послідовно додавати до вашого повідомлення натуральні числа та обчислювати геші одержаних повідомлень доти, доки підраховане геш-значення не співпаде із оригінальним значенням.

Сформоване повідомлення `KobetsDenisSergiyovich661433` отримане шляхом приєднання до ПІБ випадкового значення з інтервалу. Зафіксоване геш-значення `A6998B8AEE4CDDF739F4CB7A762801FB172D63265C55236BB22FD1650B1311BD049E7D72216776E9`

Шуканим значенням буде `76E9`

Перші 30 повідомлень та їх геші:

KobetsDenisSergiyovich6614331
235245D0B9D7A9C7433E9EAE15C7ADBDCE899D290E06F037C9E234061DA19D5E9BF34AAD84EC3F87
KobetsDenisSergiyovich6614332
F11C46784125F6DC122CC1739123DEE9D7D6247AB7BB1E1B817B92DDF7343AD1C16C0B0EC960E394
KobetsDenisSergiyovich6614333
C21915E793E82835F59BE2C4971733A2FF65BC4B4316CF75E1764C095E99FE2750DC8FFAE334E6CD
KobetsDenisSergiyovich6614334
9F4867C3ACECFA2873CEEF6C9DFB5F93F4F32A5CBF3188D2D0C8E6A5E21B1E2E0FF245E9BE23D731
KobetsDenisSergiyovich6614335
7A52E0EC94743B7084C3DB117981F9AAB9D2C8EC5EFF6EB7EFAEFFC47F5B8BCE96949C4000246 3C3
KobetsDenisSergiyovich6614336
BA7162E4EE4F3077EDD021AEF27A6BF0EF699112C2CFF3F90D3442B2D8E1429410942852DFE7F977
KobetsDenisSergiyovich6614337
AEFC468BDB5DF64056556F508619EE8C60981BCB6C99BDD1B180D15B353FEEFD4E3EA39175F36CF4
KobetsDenisSergiyovich6614338
56AD378BCEC669B423A60E877E3ACDFC6D1EFDA0EE3ECDA4723FCFC4462951FD90A6F0582CE8F126
KobetsDenisSergiyovich6614339
3282DF0C54C61D366EB351CD514F76CB3C2D82D984BB913AFE775FCFBDA97C41ACDEDD99796FB2A7
KobetsDenisSergiyovich66143310
5BC4DD34534424990DCA2A5B3A7EB7DB25883668F67DA5AC87F7B3D2AAFE33715343C89DB602D8A0
KobetsDenisSergiyovich66143311
38A1B1724A755E5CF1136B985D3EBC1645B78B3D44827BF091BBF5AAB7B2BB2E9C286CB622309 9E9
KobetsDenisSergiyovich66143312
56B522EB97C9441DC6A3CCB927256DD3A9A902C25206AC3B79855AC785A556767CDE21FB4B2F5B7F

KobetsDenisSergiyovich66143313
75CE124277ADFCF35E44492280DBD81F829C30733AF8E43D05F7B20C9FC99E13A3890673696FC2F2
KobetsDenisSergiyovich66143314
4DFF5A12C352CD2B5C77512A3679FE76C6665A39EE662B00FF6B0F2D54BF0211043EA88993504B34
KobetsDenisSergiyovich66143315
A072074CDBC10DCEE56943D50B2F292F9524EF1004F0921CE0CA566A524E384622D9BDC430C6A891
KobetsDenisSergiyovich66143316
BABED2399A9B3861EBFD9D4B04BC7E47A7F1E32EBE971BCFED283E9D513E1FB749A0ED595155DD21
KobetsDenisSergiyovich66143317
7BF70DDFAA7DBCE8F525A94585EC75ACA22BE2839ADD60488967349BF4169C44698061329F120397
KobetsDenisSergiyovich66143318
C3D125C47DEEEE6EB27624B0B4CEB1F8DE8C63C95E3CA217D964CEC01A992AEC7A4DA59F4B2E567B
KobetsDenisSergiyovich66143319
06B0E4877EDCC6D491CDEAB45CC6109455ECCBD2846D5377898F277CCFB27450C9B83505899FCD25
KobetsDenisSergiyovich66143320
45EA29529639F14DF0E3D1EA4A097466E4FECFBE9A0705D1E80CDCDE4E42AC1DA298F7BAEE2D1F5D
KobetsDenisSergiyovich66143321
933BCDCB27B7CA8C1681C472C42AD55320F452B9369E908F05CF285F70EE01015A77692A7DC9A9AC
KobetsDenisSergiyovich66143322
3145D6F42D386FBBBA1AC3BBD6E0D3C9AF0575780AB1093B507EA771C2943AF9153ED5C8B899ED73
KobetsDenisSergiyovich66143323
365CC379F92570F213E1902D01D7214C224BF6513E71D07397622DA595CA7FFE53692A0AC341EADF
KobetsDenisSergiyovich66143324
78B58944931E972493247717BE9C8EA0AAEE95389C6509DDF09E0C0891762E849B63EBF43AB5EA96
KobetsDenisSergiyovich66143325
F5E1926D3C19C456A5473ECE6EC205C3FBA164FB9EBBDE33793847FF4FFFA23C0B9C624B034195560
KobetsDenisSergiyovich66143326
4CC4B19201AB9604A469C96BF4E45217625D8A66223C8D9253A000115570656002A461BA01B1D7B6
KobetsDenisSergiyovich66143327
AD3728AD70078FC3A9DCA935E8E4AB727111FCB7927246F0CDA090B2305642B3D10BB87E4B466AB9
KobetsDenisSergiyovich66143328
FFB1D131B7E00E9F5A0DFFBF630F1CF7DE1E477042C5C7A5B3FC8E34786B5FEEB12DFC8572E47A20
KobetsDenisSergiyovich66143329
3F6FDB7A2D7E9BE127DF6B165945DD4712FBAD33BB36396C3A4CB0106355211813910A5719BBD9ED

Значення що підійшло на 145813 ітерації:
KobetsDenisSergiyovich661433145813
7973A0A52A9139A0979BED7472791FF2FFE3174718CF02D2D30887A77FAFA75ED078F59D1B7976E9

Теоретичною оцінкою складності для n-бітового геша повідомлення буде $O(2^n)$ для обох варіантів атаки, тобто $O(2^{16})$

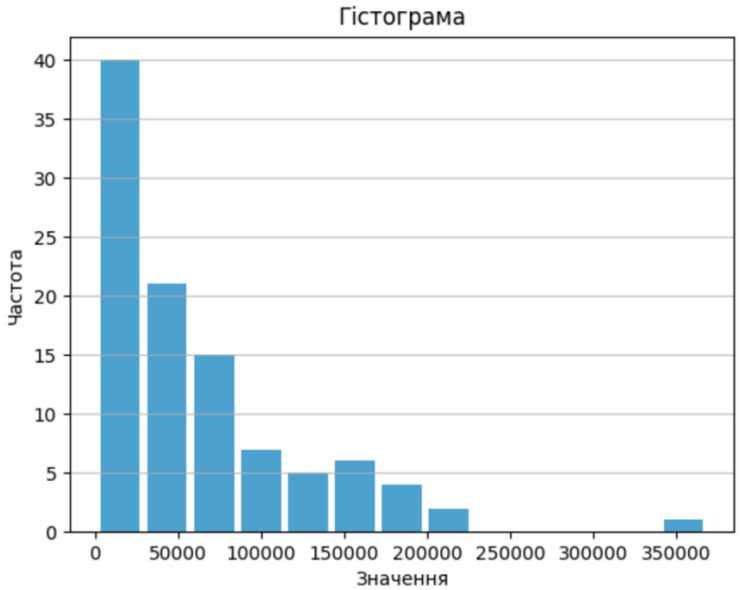
При 100 запусках отримали результати:

Математичне очікування: 62088.316831683165
Дисперсія вибірки: 3991013651.761004
0.95 довірчий інтервал: (49554.68192696118, 74621.95173640514)

Вивід кількості ітерацій атаки для 100 запусків таблицею:

0	2824	20	97807	40	148163	60	43381	80	161962
1	20095	21	13969	41	2673	61	15929	81	82221
2	117519	22	33151	42	56101	62	5850	82	32432
3	1077	23	63529	43	60763	63	7924	83	55183
4	45922	24	11523	44	30365	64	6104	84	139427
5	73226	25	71450	45	38278	65	66391	85	40653
6	221971	26	14143	46	90586	66	14637	86	34395
7	110410	27	13608	47	43079	67	5374	87	28748
8	11393	28	50446	48	13043	68	23280	88	26115
9	45793	29	66210	49	79431	69	86773	89	32857
10	11226	30	39174	50	44501	70	194815	90	155363
11	25889	31	26532	51	3454	71	16013	91	90979
12	131076	32	11215	52	24145	72	51738	92	22816
13	100272	33	86833	53	14390	73	22018	93	18514
14	804	34	137318	54	71946	74	68610	94	198142
15	3573	35	25226	55	6942	75	38781	95	59512
16	6217	36	74251	56	7379	76	20621	96	32932
17	57521	37	142820	57	152687	77	34331	97	8458
18	198142	38	218992	58	68450	78	18448	98	14948
19	195137	39	54477	59	67568	79	118829	99	368246

Гістограма значень:



Тобто приблизно у 40% запусків кількість ітерацій не перевищує 20 тисяч, а в 99% не перевищує 200 тисяч.

Атака прообразів 2:
1.1. Сформувати повідомлення, яке повинно містити ваше повне ПІБ. Зафіксувати геш-значення даного повідомлення.
1.3. *Другий варіант атаки.* Вносити у ваше повідомлення випадкові модифікації та обчислювати геші одержаних повідомлень доти, доки підраховане геш-значення не співпаде із оригінальним значенням.

Сформоване повідомлення `KobetsDenisSergiyovich156434` отримане шляхом приєднання до ПІБ випадкового значення з інтервалу. Зафіксоване геш-значення `3AD77E3581E93CBFB8611619F1A541442945EB3D083CF9ACF4945FB56BED09ECEDAF8E70E9DCD2BB`

Шуканим значенням буде D2BB

Перші 30 повідомлень та їх геші:
KobetsDenisSergiyovichL56434
1AA7AB1D29605D1814B83A8D3D8F3FBE9D316161409670E6AD61BFD7340F1FBF4C555E8BE1E4DCA9
KoAetsDenisSergiyovichL56434
E7C299999A566732561C78FDD2993ABA1B4A9480A158C4F83C0F48FD99D500C0ABC4750BB096F302
KoAKtsDenisSergiyovichL56434
8C1B56F9CDD29C571C3F0FB66334AB17284A5090B0B71A0A576683C8FE486DEF102D94D5EC03EB3D
KoAHtsDenisSergiyovichL56434
8A48C538ACC990D52563964D4A6EBE7249B63FAD11B092742F0E8D4862B882028C79AE726FFEA716
KoAHtsDenisS`rgiyovichL56434
15D0F1DF6A4BF798B2C07DA774BF42815721E06A57B59F99BB284997FA1AC31D2342710C068BCB46
KoAHtsDe"isS`rgiyovichL56434
F6DC4DDF5F2C13FA3D1411BA0E3B8E85A61133C0DC46BD91F6AC1480E271305AA4EB31594C36377B
KoAHtsWe"isS`rgiyovichL56434
8D15D8B1CD8FB2E7552CC2F877B5D60E85A601BEF7C6CEB7AD4FF5D22265A2485720D06E504F85F7
KoAHtsWexisS`rgiyovichL56434
C5C02D43931F06C5C6C098C255C556A7A58C01EE59131DE458A4D4D9EDDE7C4C203DCF8B8A515532
KoAHtsWexisS`rgiyovichW56434
DEC9C66A4DCFE085A4AC23529495C0EC99CBB8025061384BE86C452159400EBB7F043D766394A752
KoAHtsWexisS`rgiyovicgW56434
183C8B5EDD687B773D7B05ABADCE5464E17E7AB8D940427CA2EC43A1572D0E74AEC343FDC050DF9B
KoAHtsWexlsS`rgiyovicgW56434
A6096BF467A21D1659F568D36CEA0DAADBCFC2CC1A640E3E111E5938D72EABBB6A73378D111CD55D
KoAHtsWePlsS`rgiyovicgW56434
BF3234B911F33BDC409F4F6F00DAC53AB37145EE0871CAAEB56255E1DA310FBA1A3CB5DE1DF70A07
KoAHtsWePlsS`rgiyovicgB56434
BE1924AFAA03A7603EB6E90F55C52D036D9E6C97C5CB7E34A0EAD7D2CC80860584335DFC5309FF33
'oAHtsWePlsS`rgiyovicgB56434
84E281F3BE813FCC3A3026C3F26CBEB64F7D6AA752DDDB0B551ECB5F279E574BF608D2752DC01D91
'NAHtsWePlsS`rgiyovicgB56434
D7C2CEC923B5C7AE67B17CF6D7BE8F454456FBC625A61B66644A4C8B448782F778F5F6000510A1E4
'NAHtsWePlsS`rgiyovicgB5L434
17C30ACAF47D11D3AF923B1E78660E37E89506BE3978CAD926850D05FD667A12E0AC00B7D8EAFA85
'NAHtsWePlsS`=giyovicgB5L434
A9E20699308A330E4A8B221E6EC245284FEDA398917353CA0E1696719E1585C86664A7F7216BC8F7
'NAHt6WePlsS`=giyovicgB5L434
5E76418B53049CE9FFB0458B7313109A44EFD67539424262C8C3C09BAB9C57BE3A6CAFCB49AC5E4D
'NAqt6WePlsS`=giyovicgB5L434
9C4FF9A38761B543E1914306B7E2C3CCC15B567F839E49D8CA1697F7D22A463EE31C4A9170817798
'NAqt6WePlsS`=gayovicgB5L434

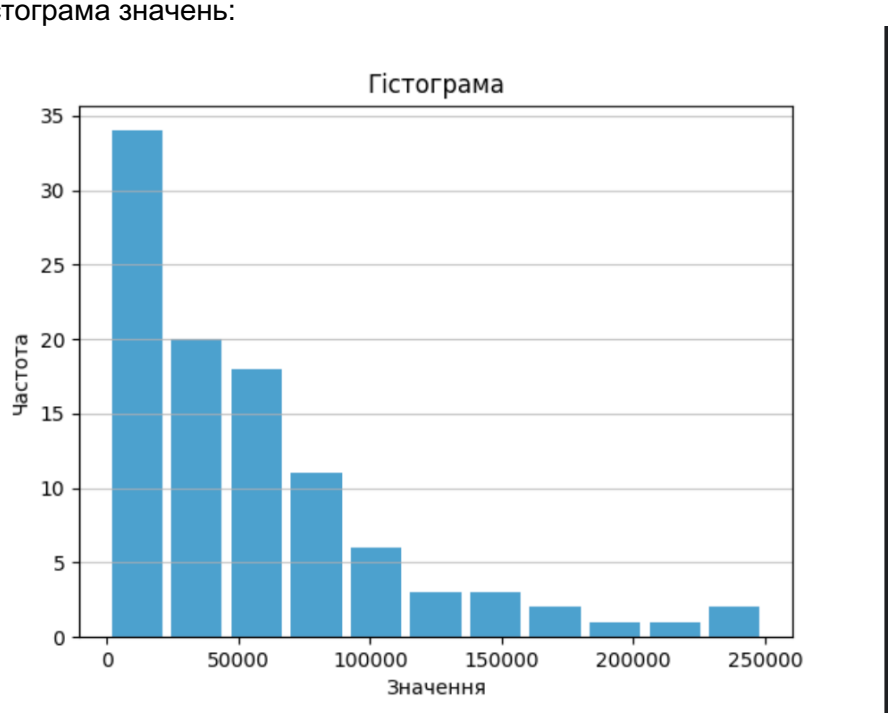
2C3E69FC880020AB814BEA2BB56029EF40F4573E8CCADC4EB46A8FBD905AE4C0A0113E4542D07824
'NXqt6WePlsS`=gayovicgB5L434
1FF1CC3418D1200F5E0B4334BAD85548F88FBE3DD7B813DFFA685A2B14F4C71944435809AFFD8DDA
'NXqt6WePlsS`=gayovicgB5L4X4
A44B35735E4260BBE6245E1F946D12091F749D24677EDF1616FFDA8B74B764C10D92D3EAC21D3C7D
'NXqt6WePlsS`=gayogicgB5L4X4
334C96CE46DF45F27F4DC8D2893FD7F862B224E12AF125B9BF5FFE78AC3FF77FAD79754E0E20AA2C
'NXqt6WePlsS`=gayogicFB5L4X4
91D00203888AECA0D7C6EE28D260193E955407788C5F227EB929A39AD380EDEEDE6B014E4E849EBC
'NXqt6WePlsS`qgayogicFB5L4X4
7B4C3D387150CAD5B02EAC07227C9E782AAFE9B03535F51C28BB90D7C8C56666CDC06115D44661D78
'NXqt6WePlsS`qgayogicFB5L4&4
E9CD15395B0DE10652B2C622BD052F783842A2960FDECB0B645BE868C7D8AE92793FB5FFE71470E7
'NXqt6WePlsS`qgayogPcFB5L4&4
1FBB2072A892C99FF1DE18D22DE480611F051201309AA19C7B79A51AC133325DA8F3023981171809
'NXqt6WePlsS`qgayogPc'B5L4&4
32EEB7B56AF0F5E18102FF2FBFA2564F7DE41266FD835097780CF2C4235C9ACCCDE1B54F24B5D640
'NXqt6WePls7`qgayogPc'B5L4&4
36299F0705248C75F2D6FE9CC36A260FBE3D8A823DB50B6171CCA76F4BF7ADC0A865399EFAD8FDB4

Значення що підійшло на 266787 ітерації:
b3sdVA=*o1Be`{3YB^d2ATFVsRG;
1DA3E55D9635838D220BF4796EA029BAB3F43B9E09D45F2153548644F10D9E25F79723BDA731D2BB

При 100 запусках отримали результати:

Математичне очікування: 55188.683168316835
Дисперсія вибірки: 2722290256.335261
0.95 довірчий інтервал: (44837.198396370906, 65540.16794026276)

Гістограма значень:



Вивід кількості ітерацій атаки для 100 запусків таблицею:

0	65774	20	15775	40	69283	60	13567	80	35970
1	26	21	47880	41	26300	61	4302	81	28559
2	99120	22	97027	42	68515	62	6215	82	8086
3	27824	23	79809	43	73182	63	38679	83	40463
4	23811	24	9224	44	54932	64	109288	84	19395
5	107715	25	13847	45	57570	65	16625	85	92132
6	735	26	15272	46	13172	66	16357	86	7335
7	243773	27	17757	47	2488	67	137800	87	63762
8	179083	28	7143	48	20419	68	126257	88	80835
9	86961	29	9043	49	4574	69	48746	89	31202
10	137044	30	36871	50	17827	70	11616	90	5854
11	30988	31	13500	51	21328	71	83752	91	33570
12	47786	32	113784	52	86617	72	32851	92	68869
13	153537	33	9443	53	30078	73	50777	93	39235
14	17954	34	5237	54	249824	74	58972	94	58995
15	32237	35	183093	55	42886	75	33836	95	212481
16	19134	36	104765	56	64457	76	59508	96	35220
17	49377	37	24048	57	25652	77	64902	97	163361
18	16717	38	1074	58	81822	78	65217	98	60558
19	123344	39	54500	59	75126	79	11547	99	21199

Атака днів народжень 1:
2.1. Сформувати повідомлення, яке повинно містити ваше повне ПІБ і яке відрізняється від повідомлення з п. 1.1. Зафіксувати геш-значення даного повідомлення.
2.2. *Перший варіант атаки.* Послідовно додавати до вашого повідомлення натуральні числа та обчислювати геші одержаних повідомлень доти, доки серед підрахованих геш-значень не виникне колізія (тобто два з одержаних повідомлень будуть мати однакове значення гешу).

Сформоване повідомлення `KobetsDenisSergiyovich151686` отримане шляхом приєднання до ПІБ випадкового значення з інтервалу. Зафіксоване геш-значення
`E72D16C9042653A6B0F67F00E818BDC9767C429C999DF26864998A0313AD7980E6BD9EC9352C1E9D`

Перші 30 повідомлень та їх геші:

```
KobetsDenisSergiyovich1516861
B751189DEB519C2C8572FE910CE08678B995FF14DC965009EC0AB6E5A51458E6BFF2DA49359773F3
KobetsDenisSergiyovich1516862
F50F0F853CEDF7469848BCE49213644FD4BE0C12D2234A885506AA3D5C4860BAA5369916BE8DCCBE
KobetsDenisSergiyovich1516863
D32106E7DE018A4C5AEF5C5C84E8563C862E1E3D2931640B510713F6E0063A0AAA3A51AF14EE316B
```

KobetsDenisSergiyovich1516864
798D930A02A7CE07F6B4BBE84F727A325ABD8E7059E0D35E91021A120A7DB2053B9ACC1C449F69C7
KobetsDenisSergiyovich1516865
5DA2716DFD9DFCBEC9C77614D8780B2AC8DA8C7A43B9FE6BD6947F4314DFEB42689078CB840B26CE
KobetsDenisSergiyovich1516866
9852CBD659B24F1F17FE26313EA0C59F80FC19C2C91AFEF9E40469E2CE057508F124E0EFAC4FC497
KobetsDenisSergiyovich1516867
CC0A60D3FFB1AA85C785C0C3508D82A421F19E52E3C280EC04409A659CED47939D9E47CE7BD098B5
KobetsDenisSergiyovich1516868
706FADAC1009A9BD57E59259DBEF26084370D74F450EFB8AFF0933F2EE3EFAC2AB46704E2FDB704E
KobetsDenisSergiyovich1516869
1E6387D474CA0FE372EF61811F537C0C1DF165CD037B29C291CAF8A70F1E02F43DE53D71C607816A
KobetsDenisSergiyovich15168610
9B5A28A5B0805C976CEB65991C53E52FE8FDBD680D2E9319A45D0AFAF18F518BB6EB3E20B04A4CE2
KobetsDenisSergiyovich15168611
E5080D3535D1ABAA6596B6B04407B8B406B11A4CC7D7125B417A702053F65E20B83250EAACA1459B
KobetsDenisSergiyovich15168612
CC32F24B43B8AF85B223F8A666A50E1C79AE9178641B4230C6F66FF98054A4B3BADA71FB8B4FA4A6
KobetsDenisSergiyovich15168613
6B04123F85DD8E0A18B573CEBFF597E97CACDD0DC0B0B432FFD6A0ED5AAC2B05F9D2E58611BCEE2C
KobetsDenisSergiyovich15168614
8767523ADE0F561B447B0DA8D785C49B98F2F03BEB6E99F45BDBF00E7716F511266E6E1F1D1B8271
KobetsDenisSergiyovich15168615
BED201A21362C0AC615010B64274B317A56BAE3508E7B9EE685614828E94C4E814EB49D2930523DC
KobetsDenisSergiyovich15168616
00EC57C30782790C02A3E6800800BA50C215CBE23E0E5FF9BA3CD1AABE01D744C6061CEDED4A4596
KobetsDenisSergiyovich15168617
EB4C4509A4B4DB4F6BEC98D9D756FC82519D1297F2D02C90D551E7DCDA4700B2A0CAD7FC42FAB7D2
KobetsDenisSergiyovich15168618
A90CC108238787A4788F7B8F153E0548008EBBC9EAF12D711740AC74C62A64EFB5765E85F81FEE94
KobetsDenisSergiyovich15168619
FCD9E675A95A6319E0C2B7B69CD6F663FA36C5E241D3F79F6A9D6ECB19E4EBF429C4C8C7DEB3EC76
KobetsDenisSergiyovich15168620
F8D4E2121B3E15EB7D30F6202F8FC9E1008799E82B2EA71A90DD6661E4E2DB982D2979C6A8C2F48E
KobetsDenisSergiyovich15168621
3BA7C53013106427C03A1DF5955BB042EEB3027584C3BED0C3B2E9C62F402E48F06D24C58097B4FC
KobetsDenisSergiyovich15168622
56D4F531F74F7BEC14BA5CB30DA85B56F25FCD3CE6641334D8C17669C3B5C27E64E9930CA2A6ED9A
KobetsDenisSergiyovich15168623
3BCF9D48A03EB7DDF901EFBE464BD37C804A62B7F4EB8C65E175C984EC40B300B6214606C98A8E84
KobetsDenisSergiyovich15168624
2D29AF1D0FE757DAB2D951AC2CFDE2CD76C2B71DD7891370B8433D3FD5B78D99DAE7808F6B86CC79
KobetsDenisSergiyovich15168625
69181EF8FE4FB0D112CC182140E5FC2E05E8544321C19B485ABF4EA5483A2C7B728A8F7A8B0407B0
KobetsDenisSergiyovich15168626
C0B5A23E8015556BC36FB38FE1B32969E772B2DD6CC02400689760EA2C100BEE8BE25FF887E64D42
KobetsDenisSergiyovich15168627
B853FECC829CC1A281638D084B432ABAD437842C7A851FBBF2A4BEE9572C6BDCF9177869DFC6135D
KobetsDenisSergiyovich15168628
8703B49174944A8808EE0C00CA70B6EC7A4D0C59296572E2D08451B6ED73869F140BD8EDA34AF79A
KobetsDenisSergiyovich15168629
DE3EE776F6F0E6A8DAFE0AD14D4D6107B09866DE59FEFE86C668873DEBC6EA3DED8DCB6F99A0CA31

Теоретичною оцінкою складності для n-бітового геша повідомлення буде $O(2^n)$, аналогічно до складності попередніх атак для обох варіантів атаки, тобто $O(2^{32})$

Значення що дали колізію:
10926) KobetsDenisSergiyovich15168610926
83326) KobetsDenisSergiyovich15168683326

Та відповідні геші:
73BAB17879FFEB3626AEA3B320A8758ECDB564D95D83DE53A631857F675BB59FE2345295DEF9CF0C
93074E5134CB1E5385F306FA2AAC99DC6C2CCA0FE8706B7ADA0D0ABE75397F2C7EEF332CDEF9CF0C

Сталося це на 83326 ітерації

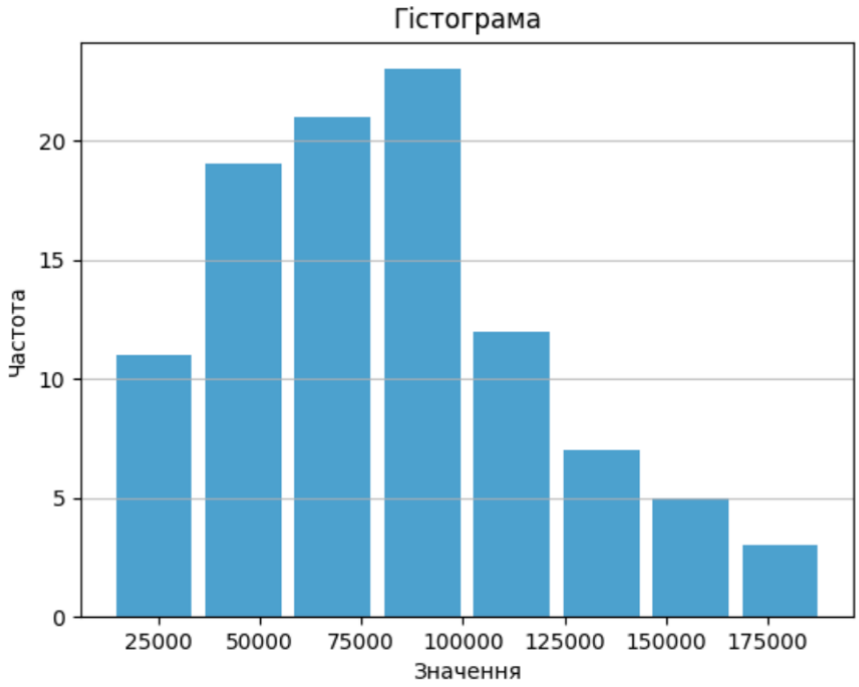
При 100 запусках отримали результати:

Математичне очікування: 80901.13861386139
Дисперсія вибірки: 1477796059.6045487
0.95 довірчий інтервал: (73274.33286389013, 88527.94436383265)

Вивід 100 ітерацій атаки таблицею:

0	51938	20	45111	40	74099	60	47191	80	81527
1	95400	21	173090	41	76572	61	37517	81	89521
2	94110	22	103992	42	105908	62	33019	82	78340
3	45485	23	103215	43	75251	63	93005	83	58935
4	23020	24	20690	44	95102	64	115515	84	40202
5	77105	25	12898	45	133317	65	100360	85	113470
6	24177	26	149035	46	100931	66	60123	86	63949
7	171737	27	101461	47	80476	67	41619	87	156856
8	38038	28	76120	48	52057	68	101415	88	36608
9	89778	29	59114	49	82381	69	98345	89	18367
10	43319	30	35710	50	68679	70	42686	90	97600
11	100249	31	81677	51	43837	71	75682	91	48112
12	104896	32	75285	52	59930	72	99154	92	23996
13	69886	33	127482	53	100466	73	142451	93	64793
14	106448	34	148320	54	105782	74	30595	94	131891
15	43912	35	22634	55	85173	75	69758	95	128034
16	86715	36	118553	56	123175	76	24107	96	138648
17	28247	37	75999	57	56011	77	57624	97	116947
18	145600	38	189136	58	86579	78	65325	98	82704
19	56318	39	88688	59	148906	79	43817	99	85827

Гістограма частот значень:



Атака днів народжень 2:
2.1. Сформувати повідомлення, яке повинно містити ваше повне ПІБ і яке відрізняється від повідомлення з п. 1.1. Зафіксувати геш-значення даного повідомлення.
2.3. *Другий варіант атаки.* Вносити у ваше повідомлення випадкові модифікації та обчислювати геші одержаних повідомлень доти, доки серед підрахованих геш-значень не виникне колізія.

Сформоване повідомлення `KobetsDenisSergiyovich258814` отримане шляхом приєднання до ПІБ випадкового значення з інтервалу. Зафіксоване геш-значення
`4E1FF57C0BAA133C1E65C331899F24FD7B2A27DFCC323747220D4FDA9CE0672B8D7C468DE294FEBB`

Перші 30 модифікованих повідомлень та їх геші:
KobetsDenisSergiyovich25881,
929068E450C6CA917A929A9F36D773FAB3407A453F5C1970F07D42BDA9E54BFA67F5E63176EFD5B4
KobetsDeoisSergiyovich25881,
197FC0A6973ACDBC4DF9A8C6EA5AB8752B3758415E250B0459E9AEF1C4411C80080B0FE911B3A01A
KobetsDeoisSergmyovich25881,
F18244174F78A1ADB4D00B658203B730B549125E2A7EA7C70262AED433B37351C33D159B603E99FB
KobetsDeoisSergmyo{ich25881,
AB002F5CB6EED6AE728AA60396A64E33F41057D093C4C1ACAFBA703FA7DF8416FE271D35F474DF3F
KobetsDeoisSergmyo{ich\5881,
84FDC7E5D79E751E5350F48649DE91AE3A614393FDBFAB1C7F901FDA362094B8E41A556949CDDA20
KobetsueoisSergmyo{ich\5881,
A9EE82D68C52EB5037642C5D591E6455E47F42A8D00F0BDE33E78715BDC0F2349F5312382F3C1305
KobetsueoisSergmyo{ich\w881,
57A86497B6CBA7DE33882B2DC08B5A82001CD9C70E7B6861679C1D61AB0A576E9A6AC07333BAB1903
Kobetsueoi|Sergmyo{ich\w881,
83F4AB8A61CCC2120611401A49CCC301E6C3D9B21D290048305D6260CB9F18CCA1E8EAA0B29EDD4A
Kobetsueoi|SergmUo{ich\w881,
A71127B20B20557CCA5A549DAFE36723D251A7E578D5148A2CFD046B908B717982FEECAD7E6753D1

Kobetsueoi|SergmUo{ich\w88Q,
813ABE4C7BAEE5B4A889D839E8C135DC473E99D3B8497E9F7C4955950026714C7584C8C493519943
Kobetsueo;|SergmUo{ich\w88Q,
83B8558E1616E0032081E9243CECC7750CD8EFC5B5428ED60793C8DBCD70F87647C2270008F0CB8C4
`obetsueo;|SergmUo{ich\w88Q,
92454717B83FACB9CE53B782D8009D24934351AD4E9C515BCDBA52A65CF0D1264AB2EA652A3A36E4
`obetsueo;|SergmUo{ich\w8/Q,
7243BB6A9866FABAAF01BE0AF49AC1658BD59C5F98B74D564CDD213617584B30B4AC3E7D752B91A2
`obetsue[;|SergmUo{ich\w8/Q,
96A5B170277763C25AC5CF4AEE68B625A51AD5168F4E9B016782744AE0E26AFB2F40FC08E33CFC28
`obetsue[;|Ser!mUo{ich\w8/Q,
47212B9F9C36464459D9AC63D3866ABC03E3A873461FDD60F4330FF5E5F5A7A2A1BF0A57C9DB0965
`obetsue[;|Ser!mUo{ich\w8/0,
B64E9C52C100AE298BD741BFDAD8E416795C18813F6D9F1DC2494653ACC3903D2B74489644C286A32
`obetsu@[;|Ser!mUo{ich\w8/0,
EDE230B8303735930DC90A25354AB87A3DB12F5061464B9EC110F3F59C0F175B45AAD3C1AAF5A70A
`obetsu@[;|Ser!mUo{ic^\w8/0,
4429420439CD4CC6F0294E1B9509427EDB3E18E4B73B2456D69B06B80AE0D57E888B958287728221A
`obets|@[;|Ser!mUo{ic^\w8/0,
8C3E03CFBD35962DBC66E76BFD8F75E141BB870760D046F9FE36F462EF4E0F046824402FF31E6378
`obetsL@[;|Ser!mUo{ic^\w8/0,
A455AE519EC259C805F730CC00F0C52B035E4AFC4108AB235E1CAB944AB6C161E80B145B8CDD2CCF
`obetsL@[;|Ser!mUo{ic^\w8/0,
A455AE519EC259C805F730CC00F0C52B035E4AFC4108AB235E1CAB944AB6C161E80B145B8CDD2CCF
`obetsL@[;|Ser!mUo{ic^&w8/0,
FEA782456762806145F6F7066D95F46AB72BFB82BB1A53E04615DE95A95010025CBD386FAEBBB112
`obetsL@[;BSer!mUo{ic^&w8/0,
9857CF13F3C187BC098A66433C6136DAFE41D43FD4128F2B0ABEE3E0DB5EEB06F58B9536D0397787
`obetsL@[;BSer!mUo{i@^&w8/0,
DECACD4221D1A79785FAEBBFAF7D32DB00981DD2FD7320F4D6F82740C31B8A227EB79952B5244A65
`obetsL@[;BSer!mUo{i@^&`8/0,
B8E9B1A2D1F54D041264356549D468726D580476A7667D82DCA27753F228EFBE881522D18B5D6CE8
`obetsL@[;BSer!mUo{i@^&k8/0,
F66D741EDF100AE79791B4F6F8B3C2B6C6B8CCE465F017A784FD6D3199FFCD7959301C8E6994B19F
`obetsL@[;B%er!mUo{i@^&k8/0,
FE104C182CFF5009CA215D8B9A57E95A88D593C1A16D65C43DE55FEEDC39521D013098FA57040A37
`obetsL@[;B%&r!mUo{i@^&k8/0,
DC992C22B92DBBBC632479E4EF6B76A62EB307EA4DB5AD09C241FBEE6D23434C5C1B667EDF6E2341
`obetsL@[;B%&r!mUo{iu^&k8/0,
CA3E3AF19284E8995BF7CCB826EC712F153C8519B17E25952585BC2B714A24065EC42459F3A407C2
`obetsL@[;B%&r!mUo{iu^&k850,
52F4E33C96DF509C39D682C547B5C222315A3F17D0A877A7B8457FE7C6853C1E61E2225D999DD8FB

Значення що дали колізію:
32849))q73~WJIx@OiWpwq0\'w9J3<7oe6
106255) g_Tku5;Y%S1/Yx;Qj)$??,qf{3Z_

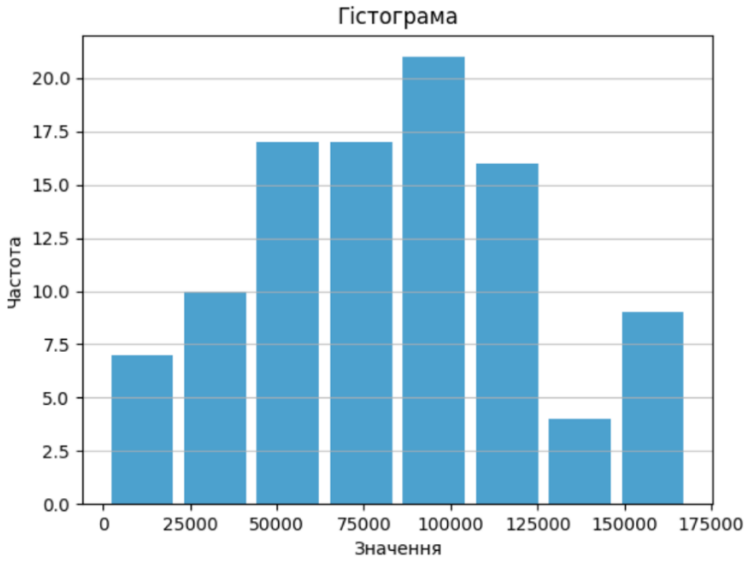
Та відповідні геші:
B1674031833D20F9B2EFE302255E5526620904402 4052BDA32BF4DB978B1D27CAB9381675D76E5E0
38216BB0CDFE2500FC632180AF7C27FE5D4274CD07A41BEEF4ACE6B16656D0533F0FB11E5D76E5E0
Сталося це на 106255 ітерації
При 100 запусках отримали результати:

Математичне очікування: 82127.44554455446
Дисперсія вибірки: 1628701709.0391133
0.95 довірчий інтервал: (74120.6966360698, 90134.19445303912)

Подання отриманої кількості ітерацій табличкою:

0	72662	20	7895	40	98243	60	111224	80	92991
1	42215	21	27058	41	145292	61	61713	81	99955
2	4529	22	23859	42	70860	62	104597	82	151158
3	87337	23	57556	43	107232	63	95380	83	70240
4	94664	24	69676	44	55546	64	121098	84	89416
5	61074	25	120535	45	45991	65	124010	85	71453
6	108124	26	46911	46	102383	66	86518	86	87316
7	102111	27	132571	47	64150	67	69835	87	105998
8	31908	28	93738	48	47693	68	57772	88	88048
9	67278	29	98396	49	32424	69	57989	89	66341
10	4499	30	155909	50	55071	70	116392	90	20601
11	715	31	40113	51	118381	71	56496	91	65163
12	129846	32	52794	52	59818	72	49590	92	64006
13	119636	33	41091	53	15951	73	44278	93	106942
14	30869	34	126601	54	52680	74	87236	94	27535
15	69334	35	149090	55	93710	75	106640	95	16617
16	168671	36	71485	56	121491	76	78698	96	78810
17	88494	37	108756	57	22757	77	168569	97	152129
18	143394	38	108037	58	168276	78	150813	98	88175
19	57741	39	99988	59	158111	79	85685	99	81662

Гістограмою:



Висновок:

Порівнявши практичні значення математичного сподівання кожної з атак, можемо зробити висновок що статистично найкращою атакою буде атака пошуку прообразу з використанням випадкової зміни повідомлення, значення маточікування в ній є найменшим, найбільшу кількість ітерацій в середньому потрібно зробити для атаки днів народжень з випадковими змінами повідомлень, майже на 59% більше ніж для зазначеної вище атаки прообразів.

При тому зі значень дисперсії дізнаємось що найточніше можна передбачити кількість ітерацій для атаки днів народжень з послідовним збільшенням числового значення в кінці, адже там середньоквадратичне відхилення є найменшим.

З гістограм можемо побачити, що для великої кількості запусків найкращим методом є перший – пошук колізії з прообразом зі зміною повідомлення у вигляді збільшення числа, майже 40% всіх атак будуть закінчуватись до 25 тисяч ітерацій. Але при цьому інколи виникають «аномалії» у вигляді 350+ тисяч ітерацій, хоча і ймовірність появи такої близька до 1%. При тому якщо оцінювати до 100 тисяч ітерацій, найкращим методом буде пошук прообразу з випадковими змінами повідомлень, там лічильник у 85% зупиниться не дійшовши до 100 тисяч, у першому варіанті атаки така ймовірність ≈ 80.

Посилання на програму: https://github.com/msverr/Hash-functions/blob/main/RIPEMD-320.py
Для запуску потрібно перейти за посиланням https://www.example-code.com/chilkat2-python/hash_ripemd.asp та згідно інструкції встановити бібліотеку