КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1

з курсу

ГЕШ-ФУНКЦІЇ ТА КОДИ АВТЕНТИЧНОСТІ

Побудова атак на геш-функції

Мета роботи

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

Хід роботи

Аналіз завдання

Розглянувши методичні вказівки було визначено наступне:
Для виконання практикуму необхідно побудувати дві моделі атак, а саме:

1. Атака пошуку прообразу.
2. Атака днів народження.

Для обох атак прийнято взяти обрізаний геш, в моєму випадку BLAKE2b може бути параметризований, і давати на виході розмір геш-значення від 1 до 64 байт. Таким чином, за згоди викладача, мною було прийняте рішення про використання параметру довжини виходу геш-значення замість обрізання N старших біт.

Для кожної з атак необхідно обрати унікальне початкове повідомлення що міститиме ПІБ студента. Для обох атак необхідно побудувати два варіанти генерації нових повідомлень, в першому випадку ми будемо дописувати до повідомлення порядковий номер ітерації, в другому випадку ми будемо змінювати випадкові байти випадковим чином. Для того аби це краще виглядало в протоколі (і мало трішки більше сенсу, адже ми в теорії намагаємось знайти "схожі" повідомлення), замість повноцінного проміжку байт 0-255, я обрав лише ті які є printable, в інакшому випадку в протоколі було б багато не надто гарних рядків вигляду `\xde\xad\xbe\xefMy name\xba\xdc\x0d\xed`.

Для кожного виду генерації нових повідомлень ми виконаємо >100 ітерацій, з різними початковими повідомленнями, і заміряємо вихідні параметри.

Для атаки пошуку прообразу ми будемо генерувати нові повідомлення на основі вхідного (початкового для поточної ітерації) і перевіряти чи геш-значення нового повідомлення однакове з геш-значенням вхідного. Як тільки ми знайшли перше таке повідомлення ми повертаємо його як прообраз.

Для атаки днів народження ми будемо генерувати нові повідомлення і додавати їх в словник в пам'яті вигляду hash-digest:message і на кожному циклі перевіряти чи геш-значення нового повідомлення вже є в словнику, якщо так ми повертаємо пару повідомлень які мають однаковий геш, якщо ні то додаємо повідомлення і геш-значення до словника.

Теоретичні оцінки складності

Для успіху p кількість ітерацій алгоритму атаки випадкового пошуку прообразу повинна бути не менше $N * ln(\frac{1}{1-p})$, де N - кількість можливих вихідних значень.
Для успіху p кількість ітерацій алгоритму атаки днів народжень повинна бути не менше $\sqrt{2N * ln(\frac{1}{1-p})}$.

Атака випадкового пошуку прообразу

Стартовим повідомленням було обрано:
`Wake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...`
Його геш-значення з параметром вихідної довжини $16/8 = 2$ байт:
`a8b6`

Було вирішено провести 1000 ітерацій атак з різними мутаціями вхідного повідомлення. Таким чином, 30 повідомлень і останнє та їх геш значення для першої з 1000 атак.

Для першого (послідовне додавання натуральних чисел) методу генерації нових повідомлень:

initial iteration message: `e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'`
hash: `0c37`

iteration	message	hash hexdigest
0	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'0"	06a2
1	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'1"	6582

iteration	message	hash hexdigest
2	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'2"	f5f3
3	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'3"	af8e
4	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'4"	0470
5	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'5"	fb5e
6	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'6"	62ea
7	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'7"	d94f
8	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'8"	2a3e
9	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'9"	1ba7
10	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'10"	d0b4
11	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'11"	20e5
12	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'12"	bc7c
13	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'13"	74c7
14	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'14"	3b33
15	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'15"	7680
16	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'16"	2a4e
17	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'17"	78e2
18	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'18"	f0e7
19	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'19"	d262

iteration	message	hash hexdigest
20	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'20"	099a
21	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'21"	847a
22	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'22"	3157
23	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'23"	3323
24	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'24"	63cc
25	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'25"	4ee7
26	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'26"	d514
27	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'27"	21c2
28	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'28"	bedb
29	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'29"	9f49
71104	b"e+fSsaw\tWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...'jb9Kn*'71104"	0c37

Для другого (внесення випадкових змін) методу генерації нових повідомлень

initial iteration message: `<7:20(&eWake up, Prikhodko Yuriy Oleksandrovych!\nThe Matrix has you...U#tx1$*`

hash: `5703`

iteration	message	hash
0	b'<7:20(&eWake up, Prikhodko Yuriy Oleksandrovych:\nThe Matrix has you...U#tx1$*\x0c'	6c09
1	b'<7:20(&eWake up, Erikhodko Yuriy Oleksandrovych:\nThe Matrix has you...U#tx1$*\x0c'	21a8

iteration	message	hash
2	b'<7:20(&eWake up, Erikhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#tx1$*\x0c'	6bf0
3	b'<7:20(&eWake up, Erikhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#txX$*\x0c'	9ba7
4	b'<7:20(&eWake up, ErIkhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#txX$*\x0c'	5ce8
5	b'<7:20(&eWake up, ErIkhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#txX$*'"	245a
6	b'<7:20(&eWake up, ErIkhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#txX$*_'	c5a8
7	b'<7:20(&eWake p, ErIkhodko Yuriy Oleksandrovych:\nThe MaUrix has you...U#txX$*_'	5dd5
8	b'<7:20(&eWake p, ErIkhodko Yuriy Oleksandrovych:\nThe :aUrix has you...U#txX$*_'	f47a
9	b'x7:20(&eWake p, ErIkhodko Yuriy Oleksandrovych:\nThe :aUrix has you...U#txX$*_'	f1fa
10	b'x7:20(&eWake p, TrIkhodko Yuriy Oleksandrovych:\nThe :aUrix has you...U#txX$*_'	7eee
11	b'x7:20(&eWake p, TrIkhodko Yuriy?Oleksandrovych:\nThe :aUrix has you...U#txX$*_'	f1e6
12	b'x7:20(&eWake p, TrIkhodko Yuriy?Oleksandrbvych:\nThe :aUrix has you...U#txX$*_'	a98b
13	b'x7:20(&eWake p, TrIkhodko Yuriy?Oleksandrbvych:\nThe :aUrix has you...U#txXi*_'	f7d3
14	b'x7:20(&eWake p, TrIkhodko #uriy?Oleksandrbvych:\nThe :aUrix has you...U#txXi*_'	c2c5
15	b'x7:20(&eWake p, TrIkhodko #urAy?Oleksandrbvych:\nThe :aUrix has you...U#txXi*_'	8698
16	b'x7:20(&eWake p, Tr0khodko #urAy?Oleksandrbvych:\nThe :aUrix has you...U#txXi*_'	bdb6
17	b'x7:20(&eWake p, Tr0khodko #urAy?OleksaNdrbvych:\nThe :aUrix has you...U#txXi*_'	b24c
18	b'x7:20(&eWake p, Tr0khodko #urAy?OleksaNdrbvych:\nThe :aUrix has you.\x0b.U#txXi*_'	715b
19	b'x7:20(&eWake p, Tr0khodkD #urAy?OleksaNdrbvych:\nThe :aUrix has you.\x0b.U#txXi*_'	71e0

iteration	message	hash
20	b'x.:20(&eWake p, Tr0khodkD #urAy?OleksaNdrbvych:\nThe :aUrix has you.\x0b.U#txXi*_'	4972
21	b'x.:20(&eWake p, Tr0khodkD #urAy?OleksaNdrbvych:\nThe :aUrix hes you.\x0b.U#txXi*_'	40e7
22	b'x.:20(&eWake p, Tr0yhodkD #urAy?OleksaNdrbvych:\nThe :aUrix hes you.\x0b.U#txXi*_'	9c42
23	b'x.:20(&eWake p, Tr0yhodkD #urAy?OjeksaNdrbvych:\nThe :aUrix hes you.\x0b.U#txXi*_'	8ed3
24	b"x.:20(&eWake p' Tr0yhodkD #urAy?OjeksaNdrbvych:\nThe :aUrix hes you.\x0b.U#txXi*_"	ffa2
25	b"x.:20(&eWake p' Tr0yhodkD #urAy?OjeksaNdrbvych:\nThe :aUrix hes you.\x0b.U#txXi*-"	a3ef
26	b"x.:20(&eWake p' Tr0yhodkD #urAy?OjeksaNdrbvych:!The :aUrix hes you.\x0b.U#txXi*-"	a420
27	b"x.:20(&eWake p' Tr0yhodkD #urAy?OjeksaNdrbvycr:!The :aUrix hes you.\x0b.U#txXi*-"	1b54
28	b"x.:20(&,Wake p' Tr0yhodkD #urAy?OjeksaNdrbvycr:!The :aUrix hes you.\x0b.U#txXi*-"	b16f
29	b"x.:20(&,Wake p' Tr0yhodkD #urAy?OjeksaNdrbvycr:!The :aUrix hos you.\x0b.U#txXi*-"	a0bb
174493	b',\x0c9=A\/v~LhkxxnDT-(/ZDhWQ4h\\rUowpY6"!9~qMGW\n``sD"VVR6FEmN\x0 cSUyl<$Y!#Cv>X^Fw!ZTg'	5703

Атака днів народження

Початкове повідомлення: `Follow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.`

Для першого (послідовне додавання натуральних чисел) методу генерації нових повідомлень:

initial iteration message: `b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw"`

iteration	message	hash hexdigest
0	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw0"	a89e6ddf
1	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw1"	b3a57b51
2	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw2"	950eecba
3	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw3"	9ddb2eb1
4	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw4"	c6994660
5	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw5"	f3432c2f
6	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw6"	0875dcaa
7	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw7"	916464a0
8	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw8"	ab8386a4
9	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw9"	d9fbf1a3
10	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw10"	69701c25
11	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw11"	e642d795
12	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw12"	7dbbbfe7
13	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw13"	d314315f
14	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw14"	ce2d16b4
15	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw15"	eca90cf2
16	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw16"	50bd9add
17	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw17"	f49dbb3e

iteration	message	hash hexdigest
18	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw18"	760268dc
19	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw19"	2115254b
20	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw20"	5945b00f
21	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw21"	8e4f9da1
22	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw22"	003f83cf
23	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw23"	46bae7d4
24	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw24"	d6206b6a
25	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw25"	cf65f189
26	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw26"	3d034070
27	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw27"	1a38cff8
28	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw28"	444a67cc
29	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw29"	2c60a8da
48497	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw48497"	a2e1118e

Отримали колізію на повідомленнях з індексом

number	message
48497	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw48497"
18310	b"xa@TEFq\x0cFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.>\x0cz';Nsw18310"

Для другого (внесення випадкових змін) методу генерації нових повідомлень

intial message: `b'~JAF\r*JTFollow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.+J5_"gbw'`

iteration	message	hash hexdigest
0	b')xH:1aZ?Follow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.!%ikjhS)'	8c78c349
1	b')xH:1aZ?Follow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.!%ikjhB)'	3e49e8cf
2	b')xH:1aZ?Follow the white rabbit.\nKnock, knock, Prikhodko Yuriy Oleksandrovych.!%[kjhB)'	03169ab7
3	b')xH:1aZ?Follow the white rabbit.\nKnock, knrck, Prikhodko Yuriy Oleksandrovych.!%[kjhB)'	093389df
4	b')xH:1aZ?Follow the white rabbit.\nKnock, knrck, Prikhodko Yuriy Oleksandrovych.!%[k/hB)'	90264948
5	b')xH:1aZ?Follow the white rabbit.\nKLock, knrck, Prikhodko Yuriy Oleksandrovych.!%[k/hB)'	68f202c7
6	b')xH:1aZ?Follow the white rabbit.\nKLock, knrck, Prikhodko YAriy Oleksandrovych.!%[k/hB)'	8b10f821
7	b')xH:1aZ?Follow the white rabbit.\nKLock, knrck, Prikhokko YAriy Oleksandrovych.!%[k/hB)'	a2452249
8	b')xH:1aZ?Follow the white rabbit.\nKLock, knrck, Prikhokko YAriy Oleksandrovych\!%[k/hB)'	bb1c671e
9	b')xH:1aZ?Follow the white rabb\nt.\nKLock, knrck, Prikhokko YAriy Oleksandrovych\!%[k/hB)'	0ab109e6
10	b')xH:1aZ?Follow the white rabb\nt.\nKLoMk, knrck, Prikhokko YAriy Oleksandrovych\!%[k/hB)'	f8d65848
11	b')xH:1aZ?Follow the white rabb\nt.\nKLoik, knrck, Prikhokko YAriy Oleksandrovych\!%[k/hB)'	45269b16
12	b')xH:1aZ?Follow the white rabb\nt.\nKLoik, knrck, Prikhokko\YAriy Oleksandrovych\!%[k/hB)'	e42db607
13	b')xH:1aZ?Follow the white rabb\nt.\nKL/ik, knrck, Prikhokko\YAriy Oleksandrovych\!%[k/hB)'	298ed6fd
14	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrck, Prikhokko\YAriy Oleksandrovych\!%[k/hB)'	636b5d5d

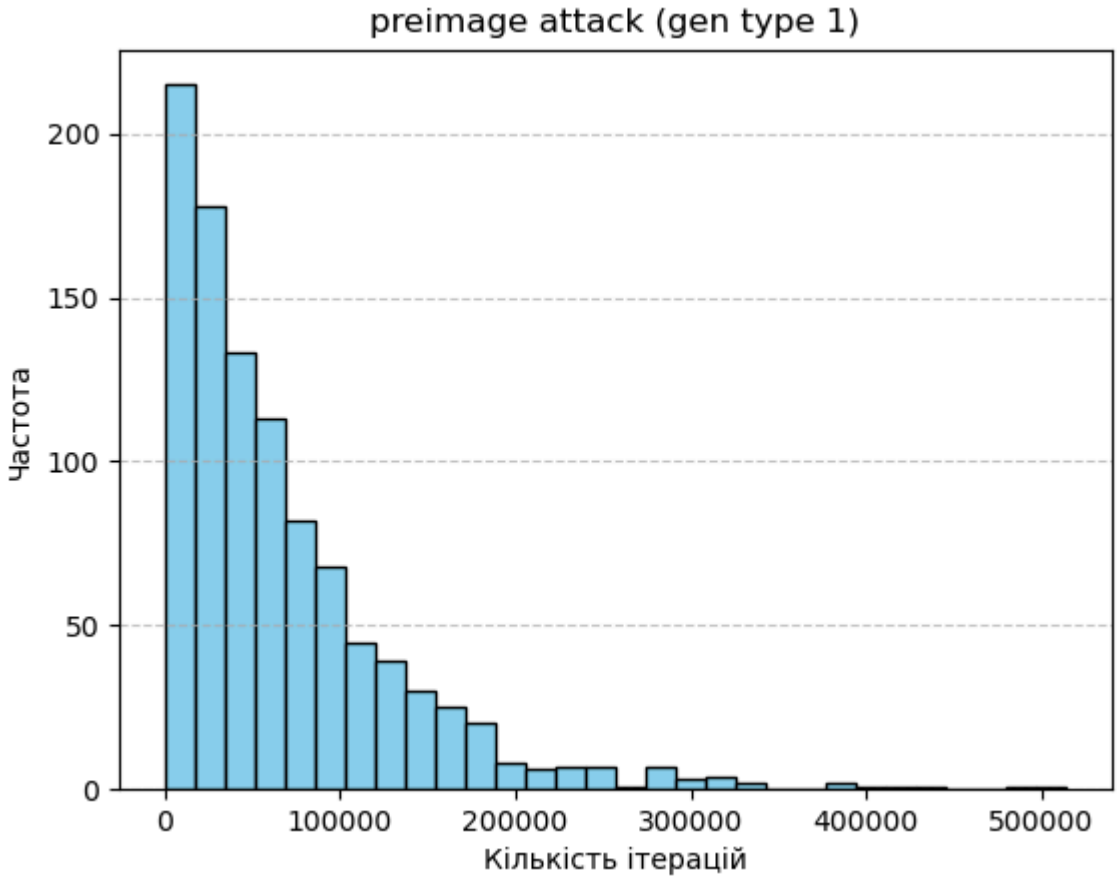
iteration	message	hash hexdigest
15	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrck, PriIhokko\YAriy Oleksandrovych\!%[k/hB)'	ddedfa2e
16	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriIhokko\YAriy Oleksandrovych\!%[k/hB)'	01f3c395
17	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriIhokko\YAriy Oleksyndrovych\!%[k/hB)'	af960af9
18	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriIhokko\YAriy OleksQndrovych\!%[k/hB)'	e7b3b5f9
19	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriI7okko\YAriy OleksQndrovych\!%[k/hB)'	e175fc19
20	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriI7okko\YAriy OlekYQndrovych\!%[k/hB)'	716c3d35
21	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, PriI7okko\YAriy OcekYQndrovych\!%[k/hB)'	35c491a9
22	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, Priy7okko\YAriy OcekYQndrovych\!%[k/hB)'	15e45a65
23	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, Priy7okko\YAriy OcekYQndrovych\!%[s/hB)'	7817b95d
24	b')xH:1aZ?Follow _he white rabb\nt.\nKL/ik, knrCk, Priy`okko\YAriy OcekYQndrovych\!%[s/hB)'	32a2117d
25	b')xH:1aZ?Follow _he w*ite rabb\nt.\nKL/ik, knrCk, Priy`okko\YAriy OcekYQndrovych\!%[s/hB)'	f12632b4
26	b')xH:1aZ?Follow _he w*ite rabb\nt.\nKL/ik, knrCk, Priy`okko\YAriy OcekYQndrorych\!%[s/hB)'	bfc7a332
27	b')xH:1aZ?Follow _he w*ite rabb\nt.\nKL/ik, kHrCk, Priy`okko\YAriy OcekYQndrorych\!%[s/hB)'	04515f3a
28	b')xH:1aZ?Follow _he w*ite rabb\nt.~KL/ik, kHrCk, Priy`okko\YAriy OcekYQndrorych\!%[s/hB)'	b20f97ac
29	b')xH:1aZ?Follow _he w*ite rabb\nt.~KL/ik, kHrCk, Priy`okko\YAriy OcekYQndrorGch\!%[s/hB)'	be3c0a58
138084	b'^n(\x0cyHJN#X24h+)-[[*.v|t0A/lgrT\rnO)b\n\nu2"3Tx>; {2SLWOrDu\taWKFM\t-1A)d5{e*Ap\vJ$q_zvO{)zmK'	02a9c6ff

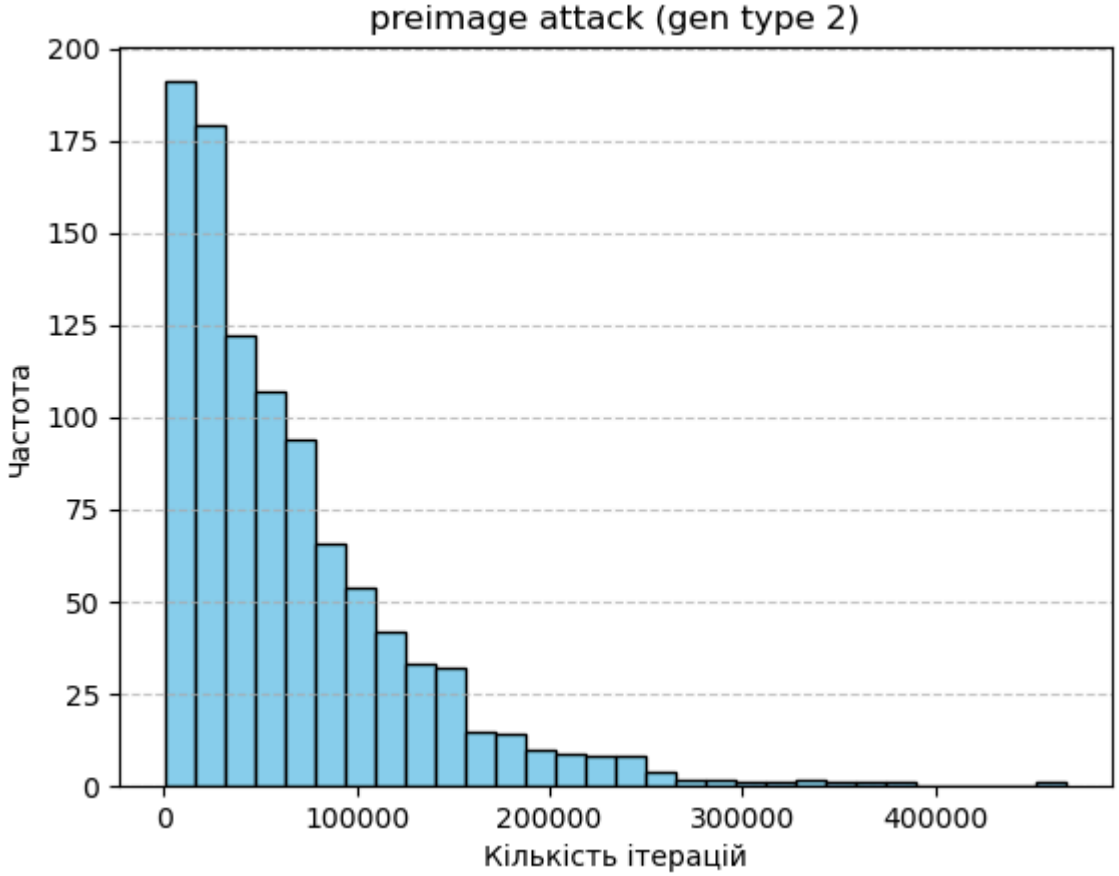
Отримали колізію на повідомленнях 67876 і 138084

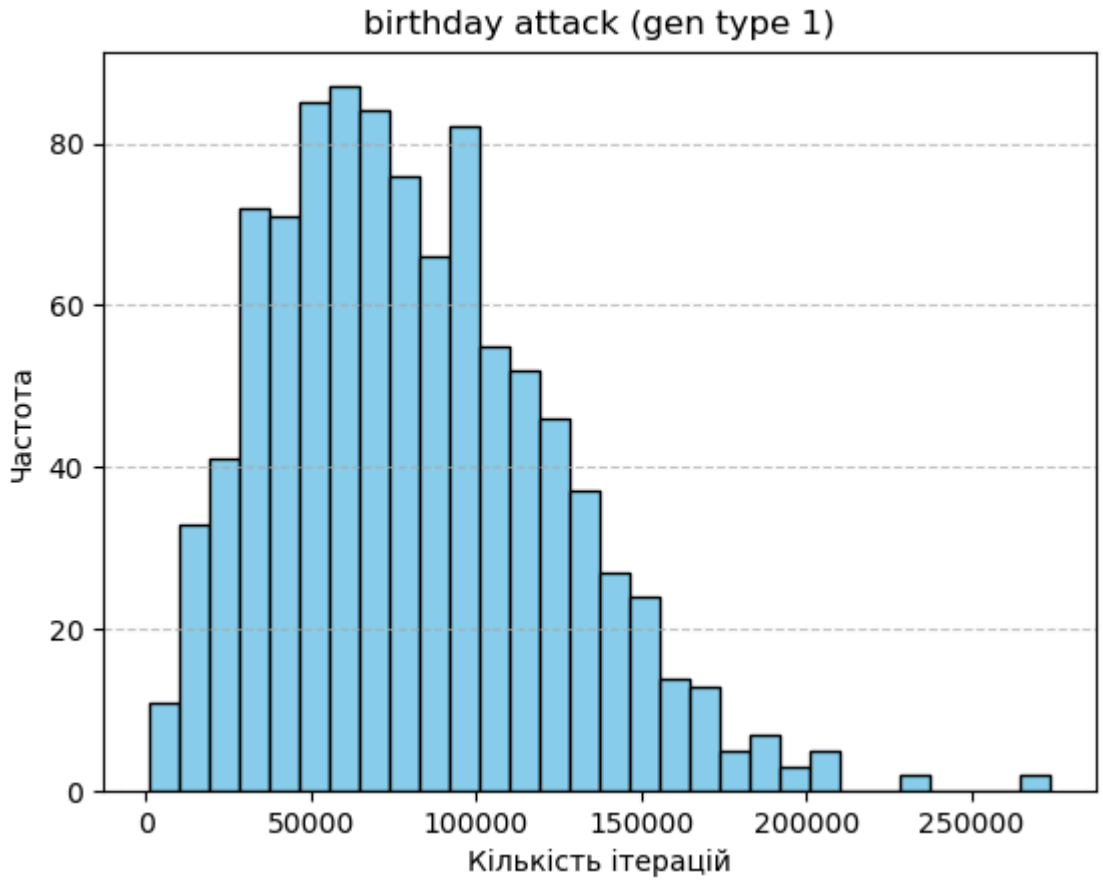
Опрацювання результатів

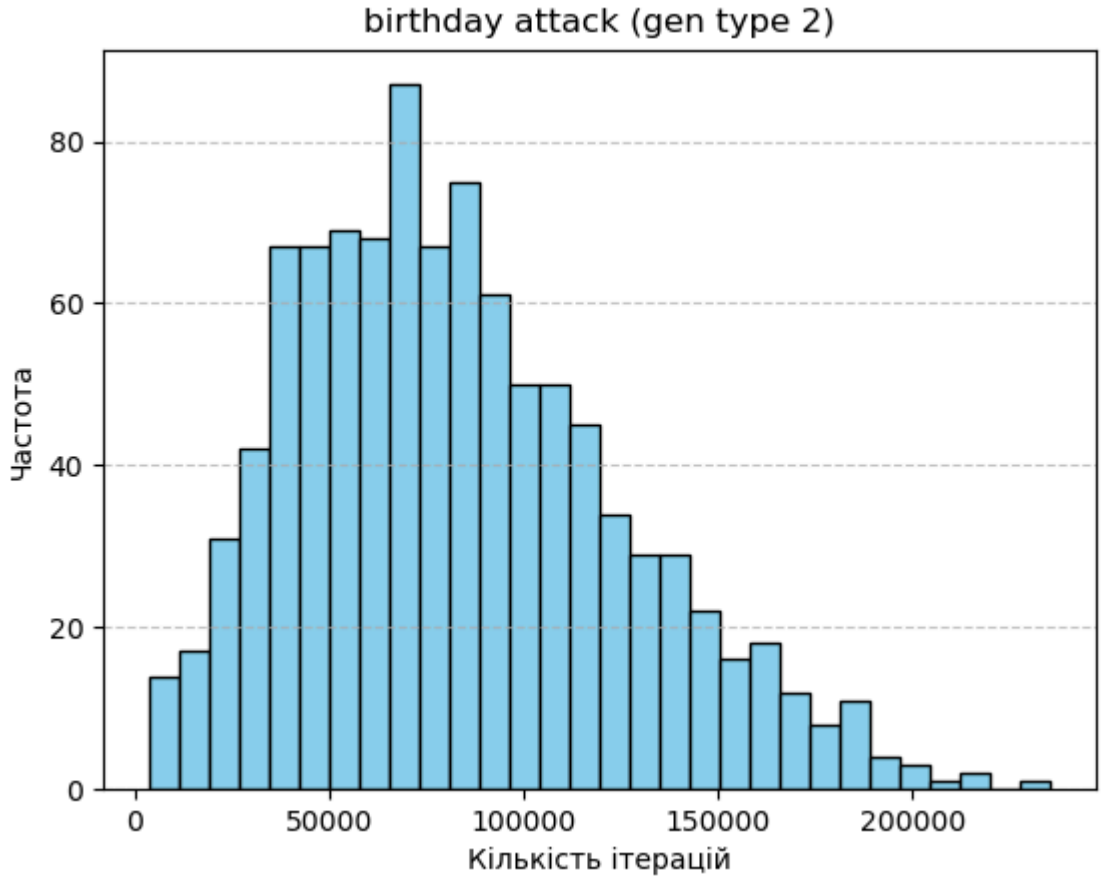
Після отримання результатів з 1000 ітерацій кожного типу генерації для кожної атаки ми можемо узагальнити результати та структурувати їх за допомогою гістограм.

type	mean	variance	confidence interval
preimage attack (gen type 1)	67796.845	4695150530.096	(63549.937, 72043.752)
preimage attack (gen type 2)	65427.447	3805006284.455	(61604.257, 69250.636)
birthday attack (gen type 1)	80751.176	1815979230.875	(78109.962, 83392.389)
birthday attack (gen type 2)	82931.820	1752060016.665	(80337.505, 85526.134)


preimage attack (gen type 1)
Частота
Кількість ітерацій
0
50
100
150
200
0
100000
200000
300000
400000
500000


preimage attack (gen type 2)
Частота
Кількість ітерацій
0
25
50
75
100
125
150
175
200
0
100000
200000
300000
400000





Порівняння одержаних результатів та висновки до роботи.

В результаті виконання роботи ми перевірили на практиці теоретичні оцінки складності атак загального виду, та отримали результати близькі до теоретичних. Отримані гістограми залежності кількості атак від кількості ітерацій чудового показує відхилення від теоретичного значення, що зумовлене випадковістю значень отриманих на практиці. Ймовірнісна оцінка розподілу зберігається на практиці.